



National Protective
Security Authority

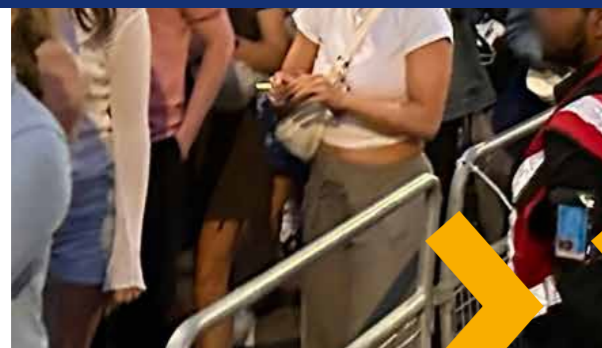
Mitigation of Terrorist Threats at Venues during **Ingress** and **Egress**



Introduction

This guidance aims to highlight the primary security concerns arising during the ingress and egress phases of venue operations. It will subsequently outline various strategies for mitigating the related risks. Recognising vulnerabilities in these situations and striving to reduce them is a fundamental part of protective security planning and an essential task for those with responsibility for ensuring the safety and security of staff and visitors.

The terms ingress and egress are used in this document as they are phases or periods of time. To some extent these words are interchangeable with 'entry and exit', however, the intention is to look at the vulnerabilities that arise, particularly as a consequence of crowds forming, during the build-up, arrival, departure and dispersion stages of a venue's operation. Ingress and egress may not always be linear and can occur concurrently for example during multiple event days or at large shows operating over extended periods. This does not detract from the purpose of this guidance which is to help identify vulnerabilities during ingress and egress and propose potential control measures.



¹ [ProtectUK | Home](#)

² [Guide to Safety at Sports Grounds 'Green Guide' - Sports Grounds Safety Authority \(sgsa.org.uk\)](#)

³ [Introduction \(thepurpleguide.co.uk\)](#)

⁴ [Safer Crowds Safer Venues](#)

Scope

Who is this guidance for

This guidance can be applied to any venue where crowds are likely to form during ingress and egress. The sort of venues envisaged include stadia, concert venues, exhibition centres, theatres, nightclubs, shopping malls, theme parks and temporary sites that are set up for short periods or single events such as festivals.

It will be most useful for people with responsibility for the design or operational security at venues or events including: venue owners and operators, event management and security companies, agencies and their planning teams, security co-ordinators, safety officers, security advisors (in the public and private sectors), risk assessors, security managers and duty or operational managers.

Some of the measures mentioned in this document are for advanced security regimes at higher risk venues that have the capacity and budget to put them in place. Many other measures mentioned are more elementary and emphasise design, communication, operational or procedural measures that can cost very little but still enhance a venue's security posture regardless of its size or budget.

What this guidance covers

This guidance outlines potential vulnerabilities during ingress and egress and then provides a scalable approach to security regimes, from a basic design to more complex solutions. It covers:

- **Crowding during ingress and egress.**
- **Key components of reducing risk.**
- **Understanding potential threats.**
- **Identifying vulnerabilities during ingress and egress.**
- **Control measures to be considered when looking to reduce risk.**
- **The importance of recording security processes, testing, reviewing and revising.**
- **Through an example, shows how control measures may be applied at a venue.**

What this guidance does not cover

During ingress and egress there are potential safety issues, through overcrowding, which could lead to crushing, trampling or other potentially life-threatening consequences. These concerns are hugely important to the management of events and should be considered as part of the overall planning and risk assessment process. This issue is not covered in this guidance, but further information can be found on the ProtectUK website¹ and within the Sports Grounds Safety Authority (SGSA) Green Guide² and Supplementary Guidance 03 'Event Safety Management'. Also, the Purple Guide³ is a comprehensive document outlining safe standards for the running of outdoor events. Lastly, for small to medium size venues, there is a good practice guide called 'safer crowds safer venues'⁴, that focuses on crowd management in UK performance and licensed spaces.

Crowding during ingress and egress

What is a crowd?

A crowd is a group of people who are gathered together in a specific location or area. The term 'crowd' typically implies a large number of individuals but can vary in size dependant on the environment or setting.

Crowds can have a diverse composition of individuals with different backgrounds, beliefs and motivations. When attending a particular venue, they may be united by a common interest, goal or purpose.

In a crowd, people often interact with one another, and the resulting dynamics can range from peaceful and cooperative, to energetic and enthusiastic, or even disorderly and unpredictable, depending on the circumstances and the behaviour of the individuals involved.

A crowd can sometimes exhibit certain characteristics that differ from individual behaviour. Factors such as anonymity, lack of individual responsibility and group influence can change the actions and decision-making of individuals within a crowd.

Crowds often act in a socially coherent manner and their actions can act as an early warning. For example, there may be a mass movement when a crowd responds to a perceived threat.

Why are crowds potential targets?

Crowds are potential terrorist targets for reasons including:

Exposure

Crowded areas, such as those that form during ingress and egress, are often accessible areas where there is little protection, which makes them vulnerable to an attack.

Soft targets

Crowds going to venues often consist of people who are excited, relaxed, chatting or otherwise distracted and may not have security awareness.

Demographic

Certain events may attract sector(s) of the population that makes them an attractive target for certain threat actors.

High profile and impact

Terrorist groups aim to generate maximum impact by targeting locations where a large number of people are gathered. Attacks on crowds can result in high numbers of casualties, widespread fear, and disruption of everyday activities.

Psychological impact

Terrorist attacks on crowds can create fear, anxiety and a sense of insecurity among the general population. By targeting crowded places, terrorists aim to create a climate of fear and disrupt social harmony, potentially influencing public opinion and causing socio-political ramifications. Media attention amplifies the impact of their actions.



The threat during ingress and egress

The start and finish times of events are usually predictable, as are the areas where there will be increased crowd density during ingress and egress. This increases vulnerability at these times and locations and must be taken into consideration as part of the security planning process.

During ingress, venues can create potential target areas as crowds form. This could be during the approach to the venue, at gates or restrictions on the outer perimeter, at a ticket check area, search area or point of entry. Clearly, safety is an important consideration in all of these areas, and safety and security should be considered together.

The threat during egress differs, in that crowds may form whilst leaving a controlled environment and entering an uncontrolled area where they can become a potential target. A site can become particularly vulnerable at this stage as exits are opened and people flow out into public areas. The people leaving may be exposed to risk, as well as those still in the venue where control measures may have been lifted to facilitate egress, thereby affording opportunity to a threat actor to enter the site or proximity of the site unhindered.

In both cases the problem centres around the congregation of people who are vulnerable to attack where there are limited security measures in place. This is particularly relevant in areas that may be outside the curtilage or direct control of the venue.



Example

Manchester Arena

Manchester: 22nd May 2017, a lone attacker waited in a large foyer area adjacent to the Manchester Arena. When the pop concert finished, people were making their way out of the event while others had come from outside the venue into the foyer area to meet up with or collect friends or family members (children). When the foyer was full of people, the attacker detonated his suicide explosive device. Twenty-three people died, including the attacker, and hundreds of others suffered physical injury.

There are many lessons to be learned from this incident including the vulnerability of crowds during egress and the need to make sure that risk is identified, understood, and effectively managed by the parties concerned. This will require effective communication and collaborative working. Full details of the Manchester arena inquiry are available online.⁵



Grey Space and Zone Ex

Grey Space is the area outside a site and may be either a public or private space. It is the area in the vicinity of a venue and impacted by the activity of the venue, but not under the direct control of the venue.

The Sports Grounds Safety Authority (SGSA), responsible for regulating sports ground safety, do not use the term 'Grey Space' but instead refer to Zone Ex (the External Zone).

In their guidance document, known as the Green Guide, it states that, 'clearly, Zone Ex is key to the safe and secure arrival and departure of spectators. It is, therefore, vital that planning for the movement of people through Zone Ex involves the input of all relevant external organisations and stakeholders, such as the police, local authorities, highway agencies and, where applicable, the owners of private property'⁶

Grey Space and Zone Ex are interchangeable terms when used to describe the area that is outside the immediate control of a venue, where responsibility for security is shared, uncertain or even disputed.

Grey Space/Zone Ex should be considered when planning security and safety for events. One of the concerns is that such areas may be crowded, with high vulnerability. It could also be the area where terrorists make their final preparations for an attack. If there is a lack of clear responsibility and/or accountability, the area may be undefended by measures such as vehicle bollards, CCTV, or security patrols, which might otherwise be considered if it was entirely under the control of the venue.

Grey Space/Zone Ex may also be significant when there are connected or adjacent public or private buildings that have separate emergency facilities such as alarms or public address systems that if triggered during an incident may affect the response to a venue or event. Understanding these facilities and who controls them should be part of comprehensive operational planning.

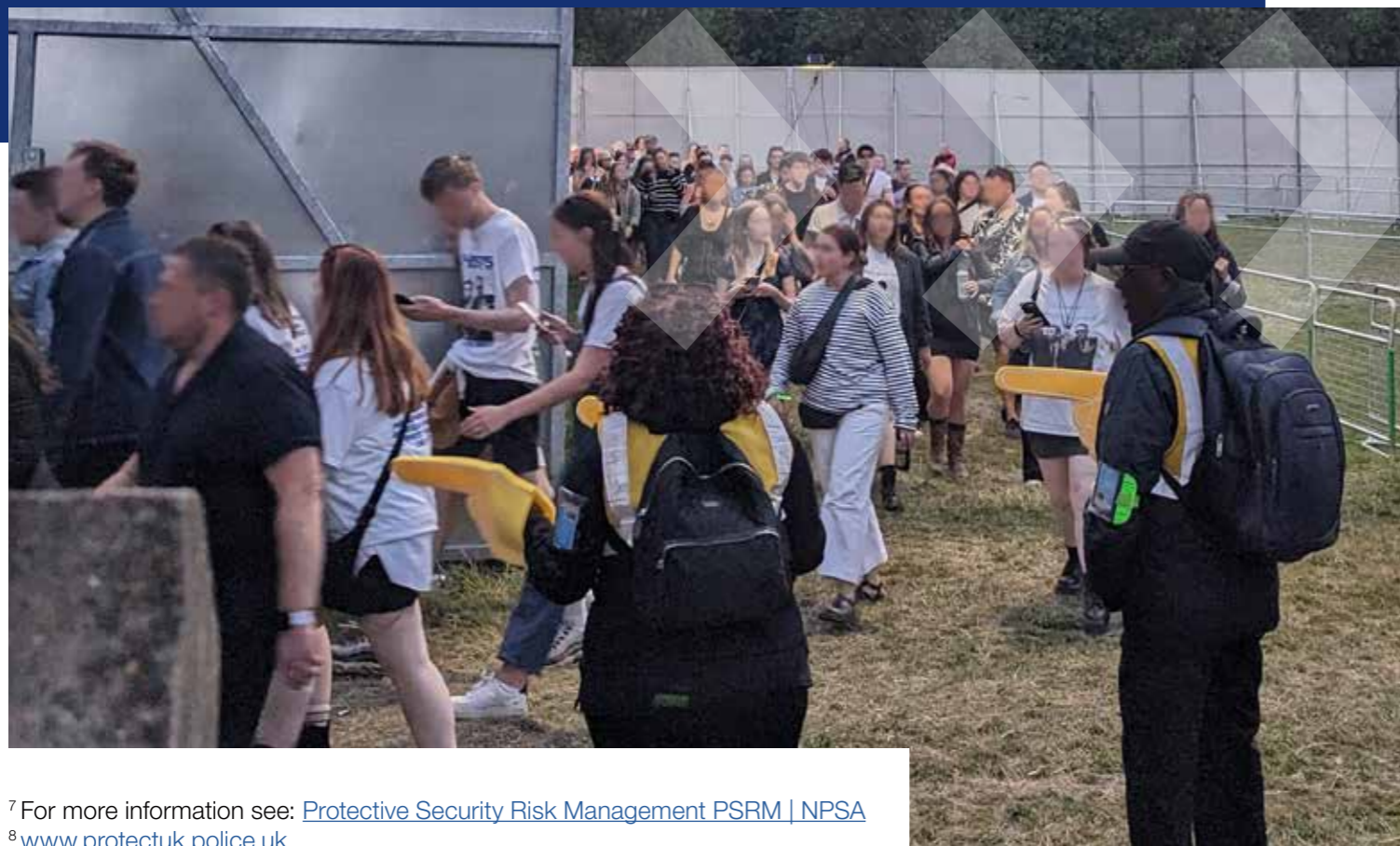


⁵ Manchester Arena Inquiry reports - GOV.UK (www.gov.uk)

⁶ Zone Ex - Sports Grounds Safety Authority Sports Grounds Safety Authority (sgsa.org.uk)

Key components of reducing risk






This guidance does not prescribe a risk assessment process (guidance can be found on the NPSA⁷ and ProtectUK⁸ websites). However, identifying and reducing vulnerabilities is a key component of any risk assessment process. When looking at ingress and egress the following steps makes it possible to identify the areas of concern and help prioritise any necessary mitigation measures.



⁷ For more information see: [Protective Security Risk Management PSRM | NPSA](#)
⁸ www.protectuk.police.uk

Understanding the potential threats

The key terrorist threat types relevant to crowded areas are shown in the table below. They are the most common attacks that have occurred in the UK in recent times.

Threat	Description
 Marauding Terror Attack (MTA)	The use of blades or other weapons, including guns, to attack people. Attacks can be fast moving and violent, as assailants move through a location aiming to find and kill or injure as many people as possible. There have been numerous incidents of this type in the UK with multiple fatalities.
 Vehicle as a Weapon (VAW)	Deliberately driving a vehicle at an individual or into a crowd to cause harm. Terrorists have used this attack type to cause multiple casualties in the UK and Europe. It is low complexity, low cost, requires little planning or skill and is less likely to be detected in the planning phase. There have been instances where a VAW attack has been followed by an MTA.
 Improvised Explosive Device (IED)	Devices can be carried, placed, posted or delivered by vehicle. Some expertise is required to make a home-made explosive device. Explosive devices of all types and delivered in various ways have been used in the UK.
 Fire as a Weapon (FAW)	Petrol or other flammable material used to start a fire, with the intent to cause harm to people. FAW is defined as being part of an MTA and can be used as a distraction tactic, as a means to augment another attack methodology, or as a disruption or deterrence to the emergency services' response. In several MTA attacks in the UK, FAW was an intended element of the attack.
 Hazardous Substances	Attacks can involve the use of corrosive or flammable chemicals, toxic or radioactive materials. The damage and injury caused by an attack depends on the material and the manner in which it is used. These attacks are rare but can have significant impact.

It is important to understand how these threats could apply to an identified venue whilst recognising that the threat has shifted from being target specific to consequence focussed (i.e. threat actors may target random crowded places if they can achieve their aims). This supports the need for additional security considerations around vulnerable crowded areas. Venue operators who consider they may be a low risk target should not ignore the fact that a hostile actor may identify the venue as a 'soft target', if security is poorly developed. An incident at any venue is likely to have a high impact.

Threats change over time, for example, drone technology and their use is rapidly evolving. To date drones have not been used as terrorist weapons in Europe or the UK. Currently, the advice is to understand how your venue might be vulnerable to a drone attack and, if necessary, explore how proportionate counter drone mitigations can be incorporated into your security plan to help mitigate the risk. Venues should refer to the NPSA and ProtectUK websites for counter drone guidance and keep their security stance under continuous review.



Identifying vulnerabilities during ingress and egress

In order to identify vulnerabilities during ingress and egress it is necessary to understand the way a venue operates - why, where and when crowds form and for how long.

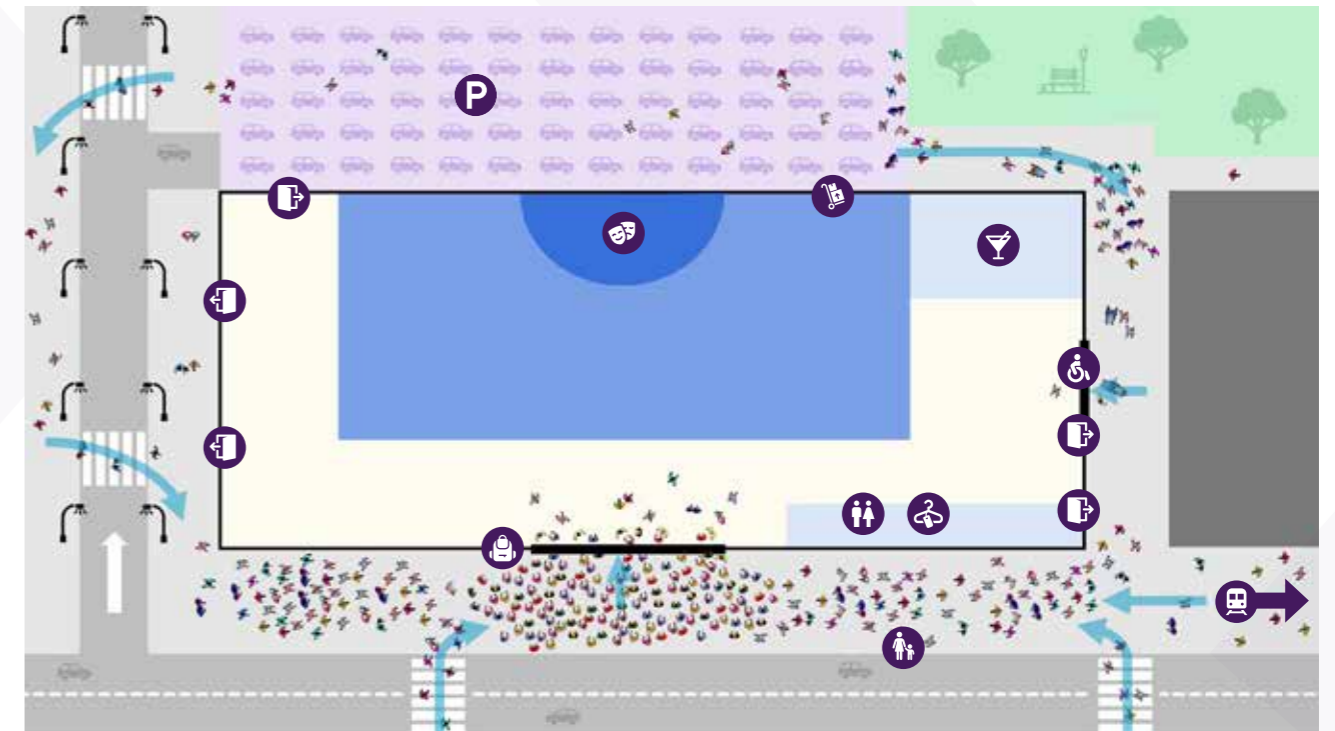
Below are two illustrative examples showing crowded areas during ingress and egress. The vulnerabilities are then identified.

Example 1 Medium sized theatre (950 seat) located in town centre

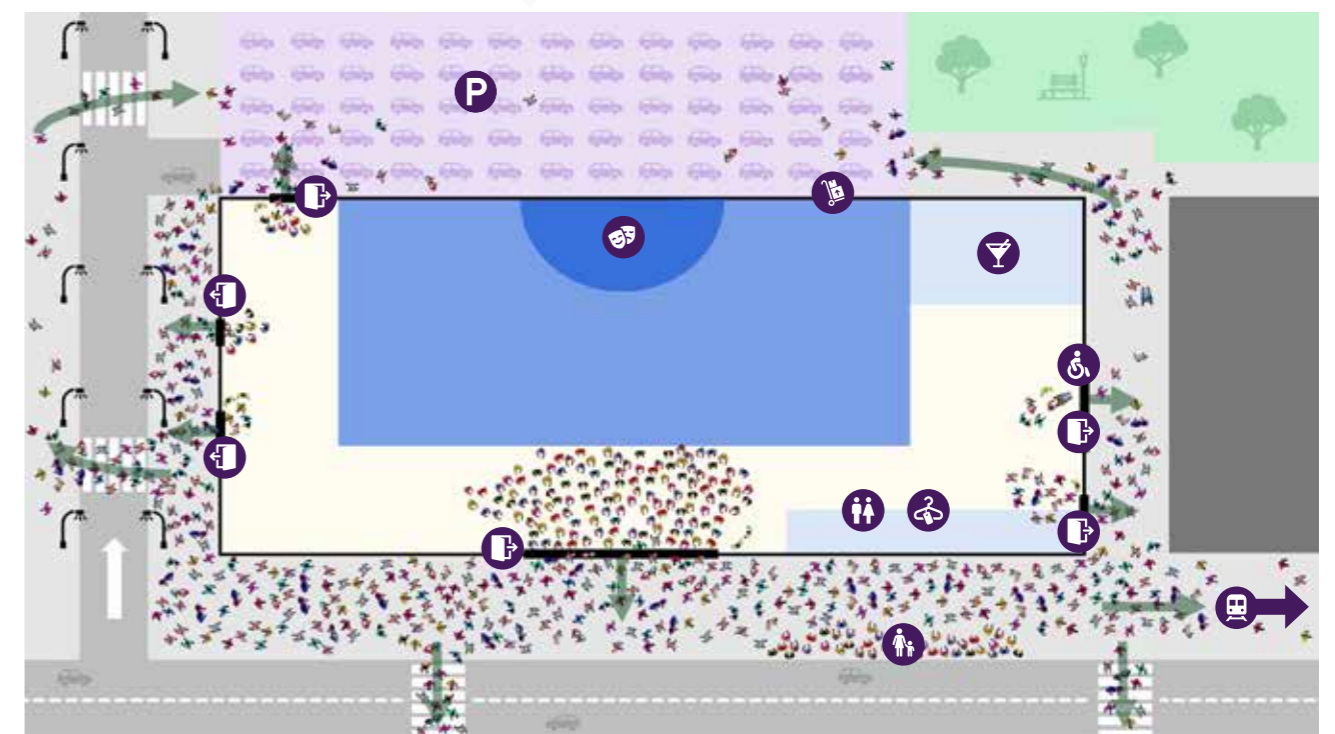
In these illustrations the following vulnerabilities are highlighted:

- Because of its confined urban setting, the theatre will have crowded places on the pavement outside the theatre and in the entrance lobby as visitors queue to go through the search regime. These crowds are exposed and vulnerable.
- When the show is sold out or near full capacity, these crowded areas are predictable and will last for a measurable amount of time whilst loading takes place. This pattern can be observed and considered by any threat actor undertaking hostile reconnaissance as part of their attack planning.
- Anything that causes a delay to the smooth ingress of visitors adds to vulnerability; this may include people bringing larger bags that need to be deposited before entry.
- When the show closes, the main entrance will again be very busy as many people will automatically leave by the same point at which they entered. Additional exit points may be opened to speed up egress but because everyone is leaving at the same time, crowded areas form throughout most of the perimeter and on the pavement towards the railway station.
- At certain events, particularly where young people attend, parents or guardians may congregate at the egress areas to collect them. This creates a slight inflow toward the event at the time when most people are exiting. Apart from adding to the general congestion, it also gives ideal cover to a threat actor heading towards an event when everyone is leaving.
- In this example, during both ingress and egress, the crowded areas adjacent to the road are vulnerable to hostile vehicles.

> Ingress phase



< Egress phase



Key

- | | | | |
|---------------------|--------------|---------------------------|---------------|
| Train Station | Exit | Bar | Cloakroom |
| Car Park | Stages | Toilets | Back of House |
| Accessible Entrance | Pickup Point | Bag Search / Ticket Check | |

Example 2

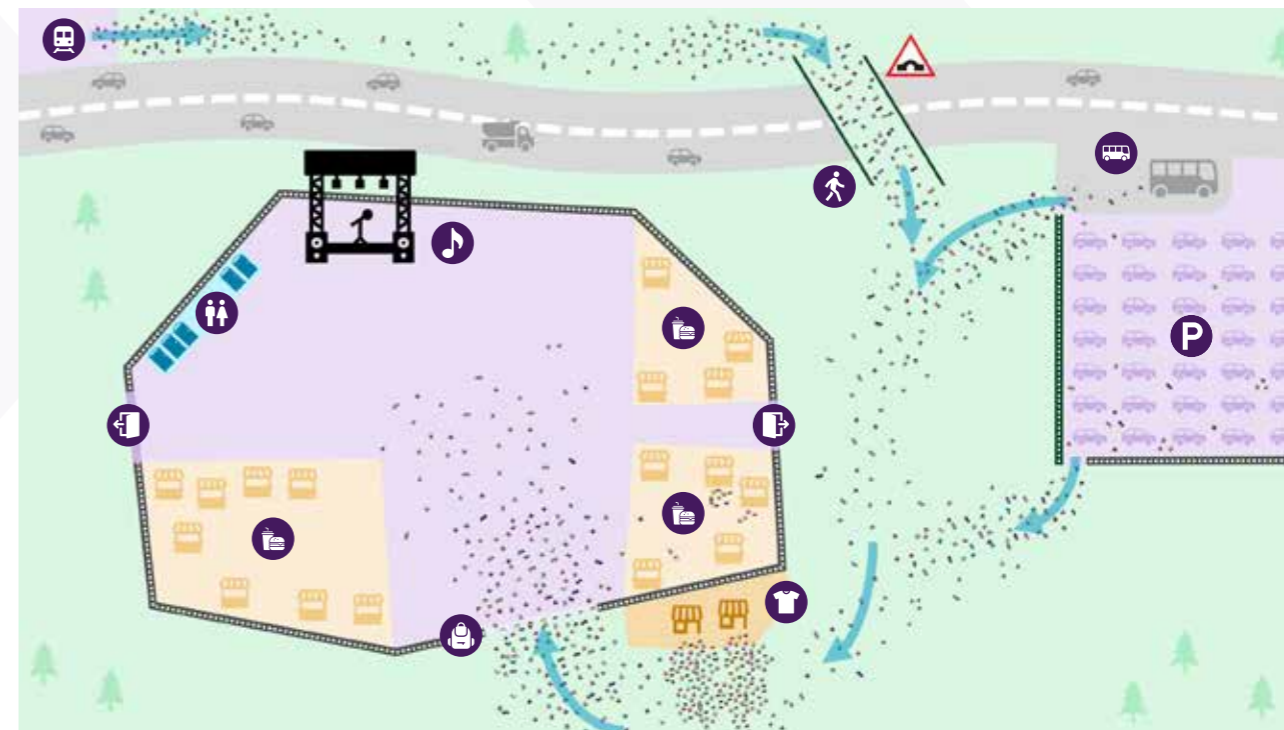
Music festival, multiple day event (10,000 ticket capacity per day) near rural village

In Example 2 the following points are highlighted:

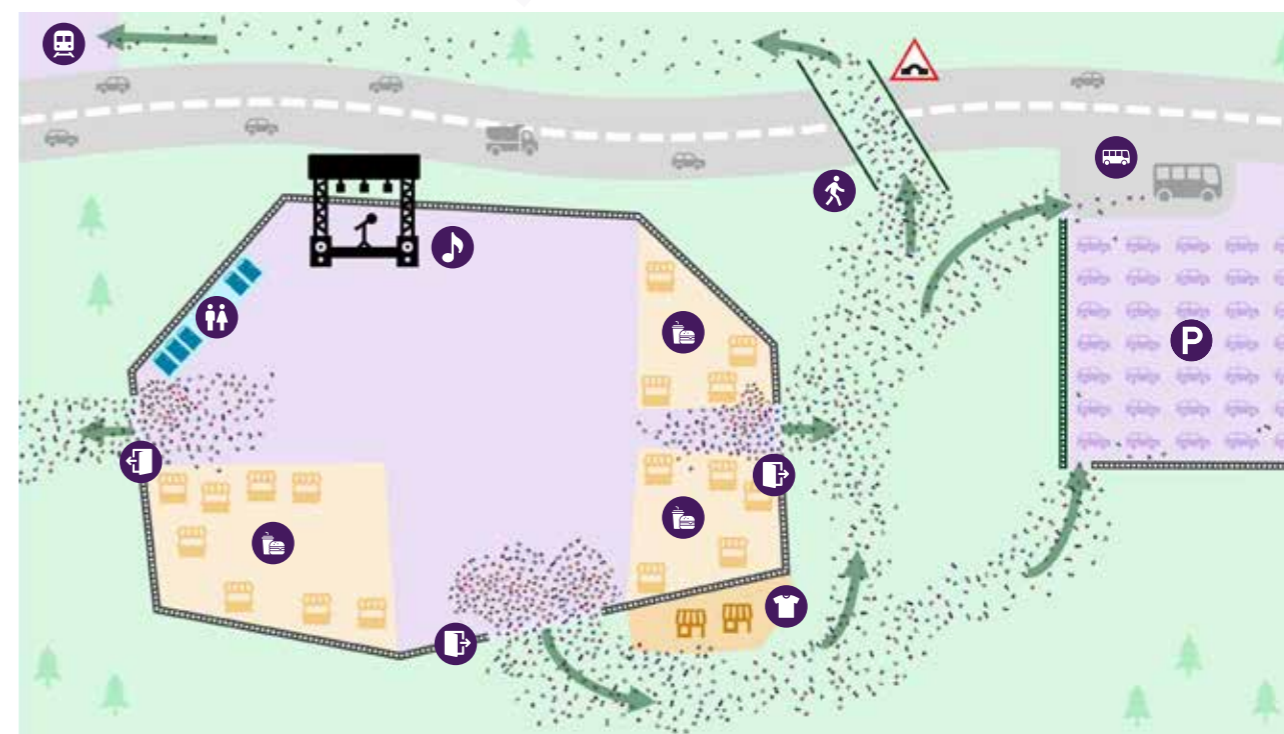
- The event is temporary and accordingly security vulnerabilities have to be anticipated and planned for in advance by those running it. Venue design will play an important part in minimising crowded areas at ingress and egress, as will the way the operation is conducted.
 - Health and safety requirements, including site safety, crowd management, emergency preparedness and stakeholder co-ordination, will form a big part of the considerations. The Purple Guide⁹ published by the Events Industry Forum gives comprehensive guidance on relevant legislation, regulations, and industry standards.
 - In this example, the principal areas of risk in terms of vulnerable crowds are the bridge and the main entrance before the search is conducted.
 - In this scenario there could be a question over responsibility for the bridge, for both security and health and safety. Ownership and responsibility should be clearly defined and agreed as part of the licensing process. Regardless, it should be flagged in any risk assessment and control measures will undoubtedly be required.
 - The conflict between vehicles and pedestrians needs to be understood. Clearly, it is undesirable to have cars near crowds because of safety and security concerns. The road, drop off point and car park need to be
- viewed in this context and suitable physical and/or operational measures put in place.
 - During ingress the main entrance would be busy, but because this point is some distance from the transport link areas, it is unlikely to be congested, particularly if the search regime is well planned and resourced.
 - Careful thought should be given to the location of facilities that may cause congestion before the 'secure area' of a site. In some venues this may include a baggage drop; in this example, the sighting of a merchandise store selling T-shirts and memorabilia outside of the site perimeter could cause a crowded area. Consideration should be made to the placement of the store and the possibility of moving it within the secure perimeter.
 - Venue design would need to take into consideration the danger from the road. It is likely that some form of barrier and marshalling would be needed to stop crowds attempting to cross the road rather than using the bridge. This could enhance perimeter protection.
 - In the scenario described the event is held over several days, giving a threat actor an opportunity to observe the site and identify areas of weakness. Hostile reconnaissance could start well in advance of the event by researching online information. Mitigation for these vulnerabilities is explored below.

⁹ [The Purple Guide](#)

➤ Ingress phase



◀ Egress phase



- Key**
- Train Station
 - Car Park
 - Coach Drop-off
 - Exit
 - Main Stage
 - Footbridge
 - Merchandise
 - Toilets
 - Bag Search / Ticket Check
 - Food and Beverage

Control or mitigate risks

An effective risk assessment will identify vulnerable areas. The most significant risk reduction occurs when well-structured security measures are put in place to mitigate these vulnerabilities. However, as outlined in the St Denis convention¹⁰, security must not be considered in isolation. It should form part of a co-ordinated plan that includes safety, security and service.

The following sections detail security measures that are relevant to decreasing risk during the ingress and egress phases of a venue's operation. It should be recognised that some of these measures will not be suitable for all venues. It is important to ensure that those security measures that are considered relevant and necessary are highlighted and recorded in relevant documentation (i.e. risk assessment/security plan).

Security measures



Safe and secure environment

Throughout a venue's operation, there needs to be a level of management that makes it as safe as practicable from terrorist threats. Measures that help create a safe and secure environment include:

- Considering security within the vicinity of the venue (Grey Space/Zone Ex). What measures are required and who has responsibility and/or accountability for putting them in place?

Communication with relevant agencies and stakeholders, including the emergency services, local authority, businesses, neighbours, local transport providers etc. is essential to agree appropriate and proportional measures. **If there is denial or obstruction by those who have a role to play the facts must be recorded and other solutions explored.**

- Creating a clear, effective, security cordon within which there is a good level of control and situational awareness.
- The deployment of barriers and fencing should be carefully considered and integrated with other safety and security measures. **It is fundamental that type and placement of barriers and fencing do not present greater risks than those they are intended to control.**
- Operational practice and procedures to create and maintain a safe environment, such as appropriate defensive searching of vulnerable areas and maintaining sterility through security tagging of sealable areas, CCTV and or regular checks and patrols.
- Site design that minimises pinch points and has considered measures, such as:
 - landscaping that restricts vehicle movement and allows efficient unobstructed pedestrian flow.
 - long 'walk up' areas to spread crowd out (this may not be appropriate for all sites).
 - expansion or release areas for contingency operations, for example to accommodate more arrivals than expected or to redirect crowds where necessary.
 - consider having 'soft ticket' and/or 'soft security' checks (e.g. asking people to show their tickets and redirecting people with bags) at advanced locations away from the entry points of the venue.
- if practical, have more than one entry point.
- entry and exit areas being uncluttered and free from fragmenting materials.
- minimising areas for concealment of prohibited articles such as weapons or explosive devices.
- removing any unnecessary clutter so that anything out of place can be readily seen, (this includes bags, coats etc. belonging to stewards and security staff).
- good line of sight and lighting for visual and optical surveillance.
- eliminating CCTV and radio signal blind spots.
- egress layout with multiple exits allowing rapid dispersal.
- consideration of the impact on those with accessibility issues and provide suitable workarounds where necessary.
- Advance messaging on your website and tickets and by using social media to warn attendees about the security regime and in particular items that are prohibited (e.g. large bags, knives, bottles, fireworks, etc). See NPSA guidance on Security Minded Communications¹¹ (SMC).
- Dealing quickly and decisively with any prohibited behaviour such as unauthorised vendors or ticketless visitors.

¹⁰ [St Denis convention](#)

¹¹ [Security-Minded Communications guidance | NPSA](#)

Keep the big threats away

The big threats include hostile vehicles and large bags or objects (e.g. equipment boxes etc.) that may contain explosives or weapons. These items have potential to cause the most damage or have the biggest impact, and as far as possible should be kept away from crowded places at or in the vicinity of the site. Some measures to consider are:

- Ideally create a zone around the venue where traffic is isolated and prevented from gaining access to any crowded place or critical structure.
- Hostile Vehicle Mitigation (HVM) measures such as vehicle security barriers, bollards or landscape design are optimum. However, there are many options and innovative solutions available; see public realm design guidance for further information¹².
- Always consider the entire ingress and egress route to ensure crowds associated with your venue are protected as far as is practicable. Keep pedestrian and vehicle interaction to an absolute minimum. For example, move drop-off and pick-up points away from crowded pedestrian areas, reorganise entry queues to form in an adjacent side street instead of at the front entrance, and close nearby car parks during the peak egress period to allow pedestrians to get away from the area.
- The provision of separate bag search lanes is good practice, especially at venues where there is a high visitor return rate (e.g. football) as it is an effective way of changing behaviour because people do not like the delay and inconvenience, resulting in fewer bags being brought to the venue.

- Restrictions forbidding large bags being taken into venues is a widely used measure because they are an obstruction or encumbrance and they could be used to conceal weapons or explosives.
- If it is anticipated that large bags or suitcases are likely to be brought to a venue, they should be deposited at a dedicated offsite location and away from vulnerable crowded areas. They should be searched before they are stored.



Understand crowds

It is important to understand how the venue operates in terms of crowd formation and audience profile.

- Understanding where crowds form at the site and why. This may be achieved by data collection (observation or manual/automatic counts) or by calculation (static analysis or crowd modelling).
- Clear data can help with operational decisions e.g. the number/type of search lanes required, etc. It could also capture variations applicable dependant on type of event, demographics and even weather conditions.
- Consider the audience profile and likely behaviours. Identify what is 'normal' behaviour for your site, so that you are able to recognise those that are behaving differently.
- Where possible, research and collate information from other venues that may have hosted the same artist or held a similar event. Open source material can also be useful.

Ensure a safe ingress

There are many things that will help reduce vulnerability and ensure a safe ingress. These may include:

- Coordinating and understanding the roles and responsibilities of all agencies and stakeholders involved. This is particularly the case for large events where there maybe a number of agencies and stakeholders involved with independent systems and protocols.
- Changing the arrival profile of visitors by timed entries or messaging regarding pre-event entertainment to encourage people to arrive early.
- Considering how the risk to gathering spectators can be minimised. Suggestions include search and screening of people looking to enter queue space, queuing within HVM barriers, or increased presence of staff.
- Maximising the number of entry points so that there is less congestion. Having an efficient entry process where ticket checks and search and screen procedures are well resourced, managed and co-ordinated. Consider 'high footfall screening' to speed up throughput (see glossary for details).
- Where possible and appropriate having a long run up to the entry gates with early ticket checks to create a steady flow and deter ticketless people trying to put pressure on the system to gain entry.
- Ensuring crowd flow is maintained by having good visual awareness of the site, e.g. through raised viewing platforms for security/stewards, good use of CCTV and efficient marshalling.
- Concentrate monitoring effort on areas that are particularly vulnerable and locations that a threat actor is more likely to select in order to carry out hostile reconnaissance.
- Deploying specialist resources such as explosive detection dogs and Behavioural Detection Officers (BDOs) to identify prohibited items being brought into the area and to spot suspicious behaviour of those planning or seeking to undertake malicious acts (it is important these resources are appropriately trained, see National Canine Training and Accreditation Scheme¹³ and NPSA Behavioural Detection Guidance¹⁴).
- Using an element of randomness when selecting people and bags to undergo a more thorough search.
- Having the ability to communicate with the whole crowd, both audio and visual (signage), particularly in emergency situations.
- Ensuring plans consider exceptional circumstances, for example identifying where crowds and queues might extend if there are issues on the surrounding train/tube lines.

¹² [Public Realm Design for Hostile Vehicle Mitigation | NPSA](#)

¹³ [National Canine Training and Accreditation Scheme \(NCTAS\) – Private Security Industry \(NCTAS-P\) | ProtectUK](#)

¹⁴ [Behavioural Detection | NPSA](#)

Ensure a safe egress

It should be recognised that egress is a time of vulnerability for a crowded event. The following will help reduce risk:

- Before people start leaving, check all egress routes for any obstructions, suspicious people or articles.
- Reduce the volume of people leaving at the same time by having after show events or activities.
- Have good signage and use staff to direct attendees to the correct exit points.
- Use the optimum number of exit points to encourage continual safe crowd flow and rapid dispersion.
- If there are likely to be people meeting/collecting attendees, identify areas where this can happen that are not obstructive to egress crowd flow and where they will not become crowded areas. If possible, the meeting points should be located within areas covered by protective measures (e.g. within an area protected by HVM). Information about such meeting points could be restricted to ticket holders (i.e. just available on issue of tickets) so that it is not generally known.
- Do not open the exits too early unless there are stewards on hand to prevent unauthorised entry by unsearched people into the event space.
- As the end of the event approaches monitor the outside area using CCTV and consider using trained Behavioural Detection Officers (BDOs) or stewards to look for any suspicious activity or people loitering or coming toward the crowded area or event space.



Security awareness

Minimise the opportunity for threat actors to complete reconnaissance and prepare for an attack. Create and promote proactive security awareness by introducing measures that may include:

- Use Security Minded Communications (SMC)¹⁵. This can help limit the amount of useful information available to a threat actor, show that you take security seriously and have a deterrent effect on them early in their planning.
- Staff being properly briefed about the terrorist threat.
- Training and awareness to help staff understand what hostile reconnaissance is, what it looks like and how and when to report suspicious activity. (ACT training and SCaN training¹⁶ – for information see ProtectUK¹⁷)
- SCaN training can help staff use 'The Power of Hello' to challenge suspicious activity and to increase customer service.
- Identify any areas that may be useful to threat actors if they were preparing to attack the site (final preparation points FPPs – see glossary). This may include toilets or areas that give good cover. Take steps to minimise this possibility through design or operational measures such as regular but unpredictable patrols.
- As illustrated by this guidance, ingress and egress are key times of vulnerability. Staff should be particularly alert at these times. Where feasible, CCTV cameras focusing on key areas should be monitored by trained staff.
- Information obtained about any suspicious activity or hostile reconnaissance must, where appropriate, be forwarded to police and should also be passed between teams and at the end of shifts in case it reoccurs.
- Suitable and appropriate staff handovers both during and at the conclusion of shifts creates continuity and heightens security awareness.

¹⁵ [Security-Minded Communications guidance | NPSA](#)

¹⁶ [ACT Awareness and ACT Security e-Learning are now available in one place on ProtectUK | ProtectUK](#)

¹⁷ [See, Check and Notify \(SCaN\) | ProtectUK](#)



Response planning

A planned and co-ordinated response will mitigate the impact of an attack should an incident occur. Preparations and procedures for responding to incidents are part of the planning process and should focus on how to get people away from danger. The following are response planning considerations:

- The ability to communicate effectively and to co-ordinate an effective response to an incident is essential. This may involve a dedicated Security Control Room (SCR) or Control Point (see glossary). Ideally, for larger venues, an incident management room should also be identified.
- Develop a communications plan detailing how your site communicates, what is communicated, when and by whom. This should include steady state comms as well as what should happen in an emergency.
- Staff that are equipped with radios must be appropriately trained in their use. For further information on communications see NPSA guidance on command and control¹⁸.
- Rapid and effective reporting is critical. Staff must be able to report suspicious incidents, this could be by radio, telephone or reporting directly to a supervisor who is close by and has a radio.
- The public should also be encouraged to report suspicious incidents to any member of staff who must then know how to respond. A venue should have practical response plans in place and staff must be aware of their roles within these plans (for example, what to do if they or a member of the public find a suspect package).
- When an incident occurs, at or nearby a venue where there are high numbers of people, mobile telephone communications often become overloaded. Accordingly, venues should not be exclusively reliant on this means of communication.
- Evacuation plans are required for all venues to meet fire safety standards. Evacuation in the case of a terrorist attack may differ from fire evacuation; for example, if certain routes cause people to move toward danger. The escape plan may need to be adapted for different threat types and could include a full evacuation, a partial (phased) evacuation or an invacuation. The development of an exceptional egress plan is outlined in the Green Guide¹⁹. It highlights that in some circumstances evacuation will involve the use of unfamiliar alternative routes, necessitating a very controlled approach.
- Considering the impact on crowd safety and security if a decision to evacuate is made. Test, exercise and rehearse your response to the attacks considered to be the highest risk. There needs to be clear leadership to initiate and ensure safe crowd movement away from danger in emergencies. For further information see NPSA guidance on command and control²⁰.
- Lockdown may not be suitable for all sites or all forms of attack. However, it can be a lifesaving response and, where appropriate, should be developed, tested, rehearsed and refined. The type of lockdown used should be adapted to respond to the unique circumstance of the site and the unfolding scenario.

- It is important that those in command and control of venues consider the impact of their lockdown/evacuation decisions. Communicating those decisions using the most suitable means (public address systems, social media, trained staff) should then direct public movement. An event log should be used to record and provide context for any operational decisions made. (See NPSA command and control guidance in footnote 20 below).
- There must be sufficient medical equipment and medically trained personnel on site. Guidance on the requirement is available through HSE²¹ (search - planning for incidents and emergencies).
- Public Access Trauma (PACT) first aid kits will significantly enhance a venue's first aid preparedness and if a serious incident occurred could be used to improve the survivability of a person with life threatening injuries (see ProtectUK for CT First Aid awareness²²).

There are a number of agencies, professional bodies and stakeholders, including where appropriate: the police (Counter Terrorism Security Advisors – CTsAs), Local Resilience Forums, and local businesses, that can assist with the development and maintenance of security and response plans. The emphasis being on joint working to maximise safety and security.



¹⁸ [Incident Response and Command and Control | NPSA](#)

¹⁹ [Guide to Safety at Sports Grounds 'Green Guide' - Sports Grounds Safety Authority Sports Grounds Safety Authority \(sgsa.org.uk\)](#)

²⁰ [Incident Response and Command and Control | NPSA](#)

²¹ [HSE: Information about health and safety at work](#)

²² [Counter terrorism first aid awareness | ProtectUK](#)

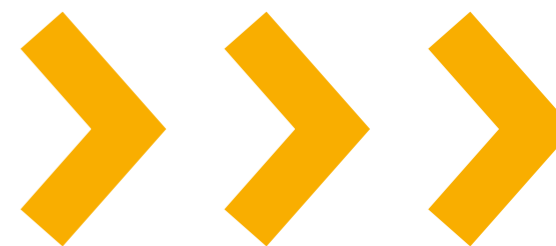




Use the right people

When planning or operating a site it is important that the right people with the appropriate skills are identified or deployed to the relevant jobs. Event organisers have responsibility for making sure those providing security have the time and opportunity to properly prepare for the event. The following apply:

- All staff, particularly security staff, should be properly briefed. The briefing should include the threat and response levels and reminders about roles and responsibilities in both prevention and response if an incident takes place (see ProtectUK for further information about briefing content²³).
- Organisers and managers must make sure there are enough staff available to do the tasks required.
- Use personnel who have plenty of first-hand knowledge, skills and experience in planning for and managing crowd events. Senior safety and security managers should have experience and knowledge of the venue.
- Ensure personnel in all event locations, including those from agencies, are suitably qualified, screened, trained and briefed for their deployment in both normal and emergency situations. This includes ensuring the medical training staff receive is suitable for the type of event and the potential risks (e.g. first aid and trauma response).
- Employ appropriate personnel for appropriate roles e.g. Community Safety Accreditation Scheme²² (CSAS) for traffic management, stewards with relevant spectator safety qualifications or Security Industry Authority (SIA) Door Supervisors, for searching (see glossary).
- Training courses and certification is not sufficient of itself, staff need specific venue instruction for crowd management, safety and security before carrying out their roles.
- Good supervision is essential to make sure staff are doing what they are meant to. Supervisors should ensure that staff are appropriately trained for the job they are doing and competent at doing it. Staff rotation is important to keep people alert and effective throughout the course of the event.
- All staff, whether or not their primary role is safety or security, have a responsibility to keep each other and visitors safe by reporting suspicious items and behaviour. Most people have a sense about things that do not look or feel right, and they should have the confidence to report it to their supervisors and be taken seriously. SCan for All Staff can be used to increase awareness about this subject.



²³ [Tactic IB1: Ensure that staff are briefed on Threat and Response Levels | ProtectUK](#)

²⁴ [Community safety accreditation scheme powers - GOV.UK \(www.gov.uk\)](#)

Record, test, review and revise

A venue or event should have a written security plan that outlines how all aspects of security are conducted at the site. Where applicable this should include the Counter Terrorism measures described in this guidance. The security plan may be part of a wider operational document but should nevertheless contain the policies and procedures relating to all aspects of the security of the venue, including those concerned with ingress and egress.

Operationally, things may not always go as anticipated and the plans should be reviewed, revised and updated as shortcomings are identified and as the venue develops or changes. Certain emergency procedures, for example, lockdown or evacuation, should be tested and exercised to ensure that they work operationally. This should feed into a continuous improvement cycle and changes made as necessary.

When response testing is completed, especially if it is done during a live event, use your communication channels to amplify your effective security plans. For example, using social media to thank customers and staff when the emergency evacuation procedures are tested, explaining it is a vital part of ensuring that the site is ready to respond in the event of an emergency. This will indicate your venues preparedness to any hostile actors.

It is important to keep written records of all matters concerning security including plans, policies, procedures, risk assessments, tests and exercises. Written evidence of the security arrangements will be an essential part of post incident procedures or inquiry.



Conclusion

This guidance is about planning and preparation to ensure the safe and secure operation of venues, with emphasis on situations of heightened vulnerability, notably during ingress and egress.

To address these security concerns, organisations and event planners need to implement a combination of operational and physical security measures, personnel training and security protocols. They also need to have measures in place to ensure a suitable response to an incident should it occur.

The proposed measures in this document are intentionally comprehensive. Not all of them apply to all sites, but where appropriate they should be considered as part of a thorough, coordinated security plan.

During research for this guidance a number of venues were visited. At one of them a security briefing was observed. At the end of the briefing the person conducting said, 'let's hear it' and the security staff actively responded by chanting 'not here, not today'. This venue had excellent security infrastructure and its staff were positively engaged in the key areas of protective security.

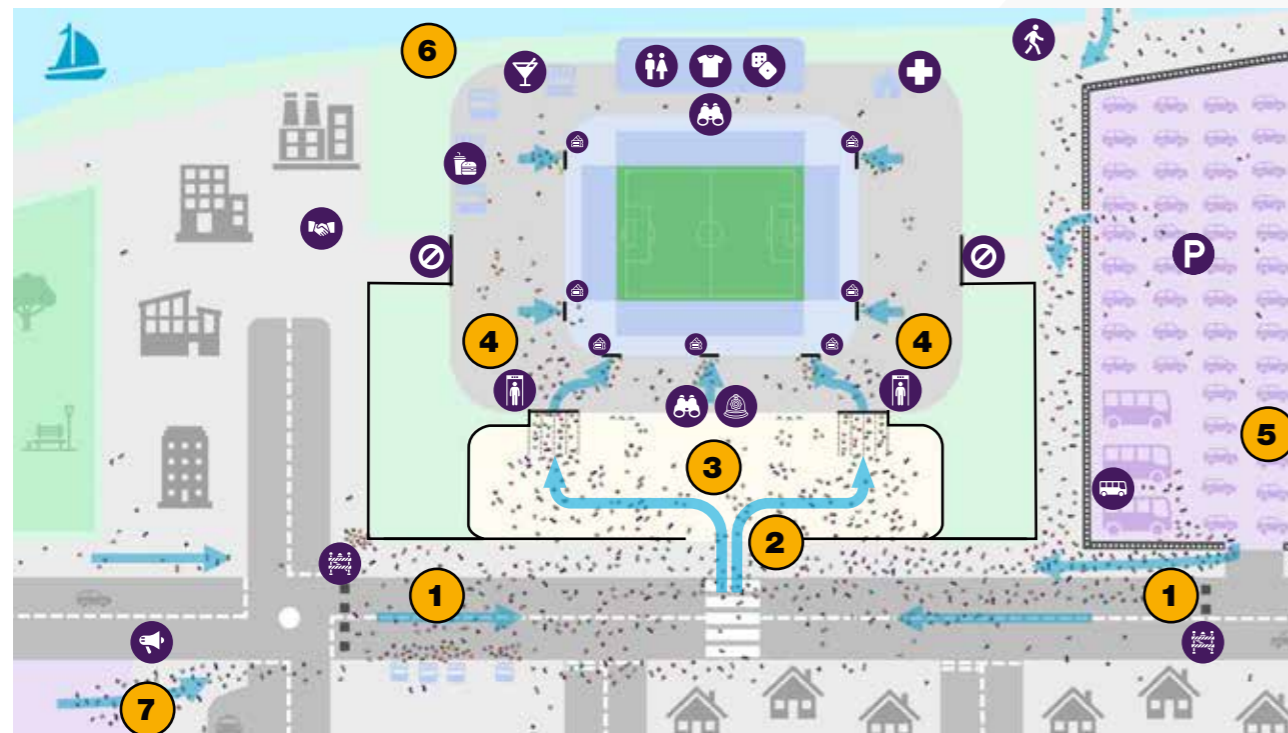
Appendix A

Good practice example

Below is an illustration that helps identify the issues that are relevant during ingress and egress at a fictional venue. The accompanying table details some of the key control measures that could be used to reduce risk in these areas.

A major sporting stadium with a capacity of 30,000 people situated in a town centre.

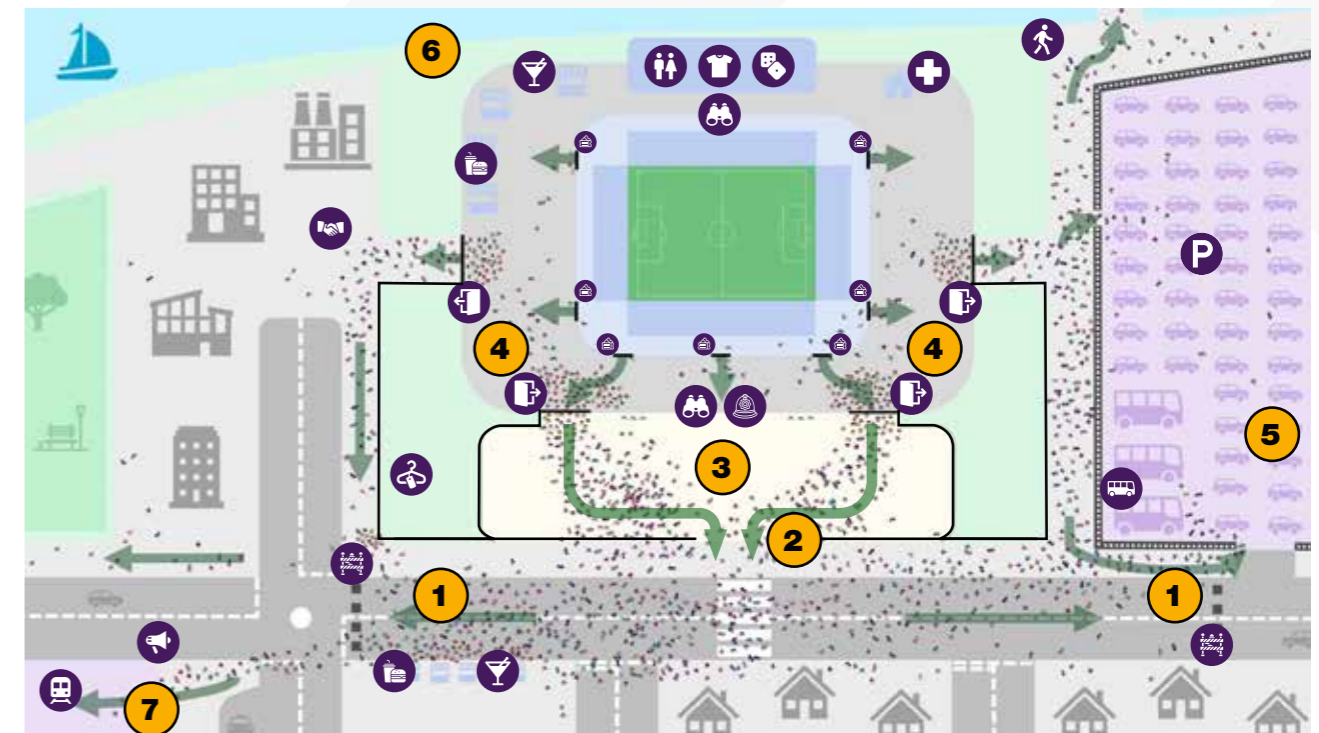
> Ingress phase



Areas

- 1** Grey Space/Zone Ex
- 2** The initial site entry point
- 3** The outer concourse
- 4** The inner concourse
- 5** Stadium car park
- 6** Riverside
- 7** Around the Railway Station


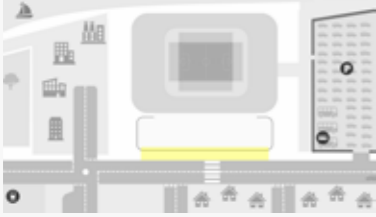

< Egress phase

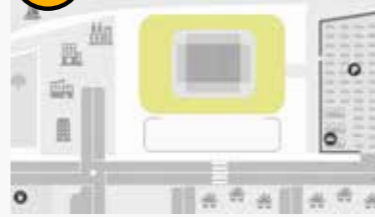
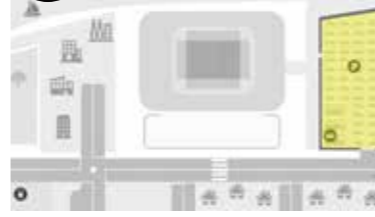
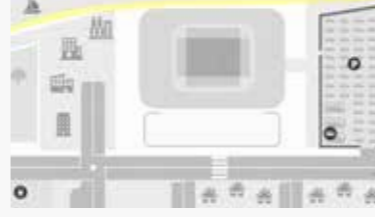


Key


- | | | | |
|----------------|---------------|---------------|------------------------|
| Train Station | Exit | Merchandise | Food and Beverage |
| Car Park | Bar | Toilets | No Access |
| Bus Stop | Footbridge | Ticket Check | Cloakroom |
| Police | Betting Booth | Loud Hailer | HVM |
| First Aid Area | Lookouts | Search Arches | Stakeholder Engagement |

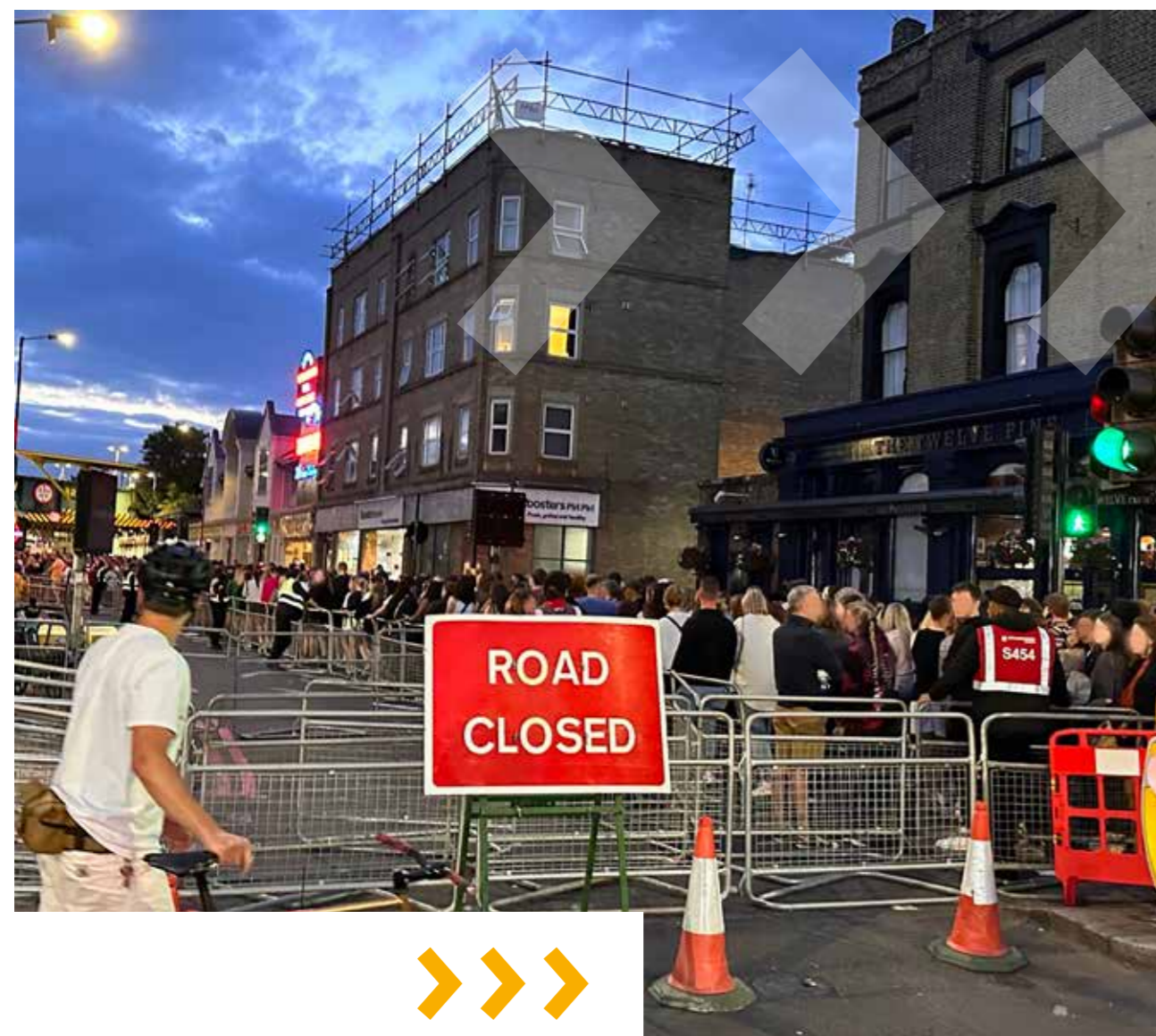
Control Measures for example overleaf

Area	Risk	Control measures
<p>1 Grey Space/Zone Ex</p>  <p>This is a crowded place outside the curtilage of the venue. It is the main access road. Both before and after the event this area is likely to have a medium to high density crowd.</p>	<p>People who are not attending the event can mingle with the event crowd. Without control measures, moving vehicles and parked vehicles could be in this space.</p> <p>Vulnerable to all main threats: VBIED VAW PBIED IED MTA (see glossary for acronym definition).</p>	<p>This space is not within the direct control of the venue. Working with partners (e.g. Local Authority and Police) will be necessary.</p> <p>Without any control measures this area is vulnerable to the threats identified.</p> <p>Ideally the road should be closed to traffic during peak ingress/egress period and suitable HVM measures put in place. In addition to physical measures, active measures should be considered such as security patrols to identify and deal with anything suspicious. BDOs would be useful in this space.</p> <p>Increase situational awareness of what is happening. This can be achieved through the use of CCTV or using stewards or security officers to observe the movement of people and identify suspicious behaviour.</p>
<p>2 The initial site entry point</p>  <p>The first pinch point for the crowd.</p>	<p>This is an area that is likely to have a medium density crowd during entry, and a high-density crowd as people leave following the event. Assuming vehicles are prohibited at this point the key threat is from an IED or MTA.</p>	<p>Vulnerability can be reduced as the venue can control access at this point. Vehicles can be prevented from accessing the site by bollards or other restrictions.</p> <p>The free flow of pedestrians is important to prevent crowd build up. Marshall's should be deployed to encourage this. Their deployment in these areas will also act as a 'high viz' deterrence and help to identify suspicious behaviour.</p> <p>High footfall screening could be desirable if manageable.</p> <p>CCTV coverage of this main access point will afford good situational awareness.</p>
<p>3 The outer concourse</p>  <p>Often a meeting point or point where people gather before entering the stadium. A reasonably high crowd density for an extended period before the event and a high density for a shorter period post event.</p>	<p>A concourse such as this is typically an area where unrestricted, unsearched crowds form before the event. Post event most people will be hurriedly leaving, but others may arrive to meet family or friends.</p> <p>There is opportunity for a threat actor to identify crowded areas for potential attack both pre and post event.</p>	<p>Areas such as this, where crowds can form - particularly towards the event start time and upon egress - have increased vulnerability. They should be checked for any suspicious articles both before the start of the event and before egress.</p> <p>Operational efficiency, i.e. having enough gates staffed and open to ensure rapid inflow is a primary control measure. Also, event staff preparing people for the search processes by advising people of where to go and what they need to do.</p> <p>As above, CCTV at all entry points is useful to monitor crowd movement.</p>

<p>4 The inner concourse</p>  <p>This can be the area used to search and screen spectators. Clearly, this causes congestion and could be a risk area, especially if it is the first occasion a person is likely to encounter some form of security challenge.</p>	<p>Wherever the search regime is located there is an element of additional risk because it is at this point the threat actor could be exposed if he/she has a weapon or explosive device with them.</p> <p>It could be the primary attack location because it is a crowded place or it could become a secondary target if the device is discovered at this point.</p>	<p>Generally, search regimes delay pedestrian flow and cause crowded areas.</p> <p>Maximising the efficiency and effectiveness of search is the aim. This is achieved by having clear policies and procedures regarding what is being sought and why and how this is to be achieved.</p> <p>If just bags are being searched, separate lanes to enable this helps speed up the process.</p> <p>Sufficient trained and competent search staff, using suitable equipment, are also essential elements.</p> <p>New technology is helpful (e.g. high footfall screening).</p> <p>Effective and targeted communications to prepare people for the search regime.</p>
<p>5 Stadium car park</p>  <p>Without control measures, unsearched vehicles will be close to the stadium, particularly the east side of the main concourse.</p>	<p>In this illustration the car park creates opportunities for vehicles to get close to crowded areas on the concourse.</p>	<p>Barriers that prevent cars getting direct access onto the concourse should be a prerequisite for event days.</p> <p>Management of the car park could limit opportunity for any threat vehicles to get close to the vulnerable areas of the concourse (for example only allowing known members' or players' cars in these areas).</p> <p>A vehicle search regime could be put in place, but they are an expensive resource if they are to be effective.</p> <p>CCTV is a useful addition to monitor this area.</p>
<p>6 Riverside</p>  <p>The river runs along the North side of the stadium. A vessel could get within close proximity of crowds on the inner concourse and in the North stand. The most concentrated crowd using these areas is likely to occur during egress.</p>	<p>When completing a risk assessment all threats should be considered.</p> <p>In this illustration the threats from the riverside are very limited. A boat or other vessel could be used to house an explosive device, however, it is an unlikely scenario as the crowded area is likely to be less dense than other zones and the effectiveness of the device is likely to be substantially less.</p>	<p>The river is a good barrier protecting from most threats.</p> <p>If there is concern about the proximity of boats (although this may be assessed as a limited risk), one option is to prohibit mooring along the stadium flank. This could be enforced by using a physical floating barrier creating stand-off from the bank (as deployed at Palace of Westminster).</p> <p>Consideration should be given when developing incident response plans (in vacuation/evacuation) as the riverside restricts capacity and throughput of people.</p> <p>As the river is not owned or administered by the stadium any control measures are likely to need co-operation from other stakeholders, in this case it may be the relevant waterway authority.</p>

Control Measures for example overleaf

Area	Risk	Control measures
<p>7 Around the Railway Station</p>  <p>In this illustration the station is near to the stadium. There will be a constant stream of spectators from the station for an extended period before the event and a more concentrated crowd for a shorter period after the event.</p>	<p>This area is vulnerable as it is easily identifiable as a crowded place before and after all events that have high attendance numbers. Stations are separate sites and should have plans in place to limit vulnerability. The area outside the station to the stadium is a Grey Space that is exposed to all the main threats in the same context as Area 1 above.</p>	<p>The control measures for Area 7, outside the railway station and up to the stadium gates, need to tie in with the measures for Area 1. Again, there are other stakeholders involved and in this case the addition of the rail service provider and the British Transport Police. The whole question of Grey Space, where an area is impacted by an event and yet is outside the event's direct control, is one that causes difficulty. Communication, comprehension of the issues and workable solutions are required.</p>



Glossary of terms

Term used	Definition
ACT e-Learning	Action Counters Terrorism (ACT). ACT e-Learning provides counter terrorist training packages for all staff. There is also ACT Security e-Learning for SIA personnel and those wanting specific 'security role' information. The training is available free from the ProtectUK website.
BDOs	Behavioural Detection Officers (BDOs) are security personnel who are trained to identify and assess suspicious or unusual behaviour exhibited by individuals in settings such as crowded public areas. The primary role of BDOs is to detect potential threats to security by observing and analysing the behaviour and body language of individuals.
Control Point	A designated room or area within the venue from which the safety management structure is controlled and operated. Also known as an event control or control room.
CT	Counter Terrorism.
CSAS	Community Safety Accreditation Scheme (CSAS) is where some uniform roles, such as wardens and security guards, can contribute to maintaining and improving community safety by performing roles such as traffic management/pedestrian crossings for events.
Final preparation points (FPPs)	These are areas that may be used by a terrorist(s) to get ready just before they commit to an attack. For example, they could use a poorly lit, out of sight, refuse area to unpack weapons they have in a rucksack.
High Footfall Screening	Techniques for detecting mass casualty threat items, such as improvised explosive devices and firearms, in crowds entering a site without the delay caused by intrusive security processes.
HVM	Hostile Vehicle Mitigation. Measures that are designed to protect against hostile acts where vehicles could be used. Includes design, road layout and vehicle barriers.
IED	Improvised Explosive Device. A bomb.
MTA	Marauding Terrorist Attack. Could be with a knife or any other weapon(s).
NaCTSO	National Counter Terrorism Security Office.
NPSA	National Protective Security Authority (formerly the Centre for Protection of National Infrastructure CPNI).
ProtectUK	A website and App run by NaCTSO where information can be found about all aspects of protective security.
SCaN	See Check and Notify (SCaN) is a free training programme that aims to help venues maximise safety and security using their existing resources. It is found on the ProtectUK website.
SIA	Security Industry Authority.
SMC	Security Minded Communications. Guidance developed by NPSA that encourages organisations to use communications to help protect themselves, their staff and visitors from hostile acts.
VAW	Vehicle As a Weapon. Any type of vehicle deliberately used to cause injury.
VBIED	Vehicle Bourne Improvised Explosive Device. A bomb in a vehicle, could be a suicide attack where the driver detonates the IED whilst on board or a vehicle left unattended to be detonated by timer, remotely or by other means.



National Protective Security Authority

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer

This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2024

www.npsa.gov.uk