Design Manual
NR/GN/CIV/300/02

Security at Stations

YING
COTSMAN
0
16:03:05
43060

Document Verification

Authorisation

Name	Department or Role
Anthony Dewar	Professional Head Buildings & Architecture, Technical Authority
Frank Anatole	Professional Head Buildings & Architecture, Technical Authority

Standard Change Lead

Name	Department or Role
Boaz Yariv	Senior Architect Buildings & Architecture, Technical Authority
Wayne Watson	Head of Security Governance Technical Authority

Revision Information

Version:	1.0
Date issued:	June 2023

Description of changes:
First issue

Disclaimer

In issuing this standard/control document for its stated purpose, Network Rail Infrastructure Limited makes no warranties, expressed or implied, that compliance with all or any standards/ control documents it issues is sufficient on its own to provide safety or compliance with legislation. Users are reminded of their own duties under legislation.

Compliance with a Network Rail standard/control document does not, of itself, confer immunity from legal obligations. Where Network Rail Infrastructure Limited has granted permission to copy extracts from Network Rail standards or control documents, Network Rail Infrastructure Limited accepts no responsibility for, nor any liability in connection with, the use of such extracts, or any claims arising there from.

This disclaimer applies to all forms of media in which extracts from Network Rail standards and control documents might be reproduced.

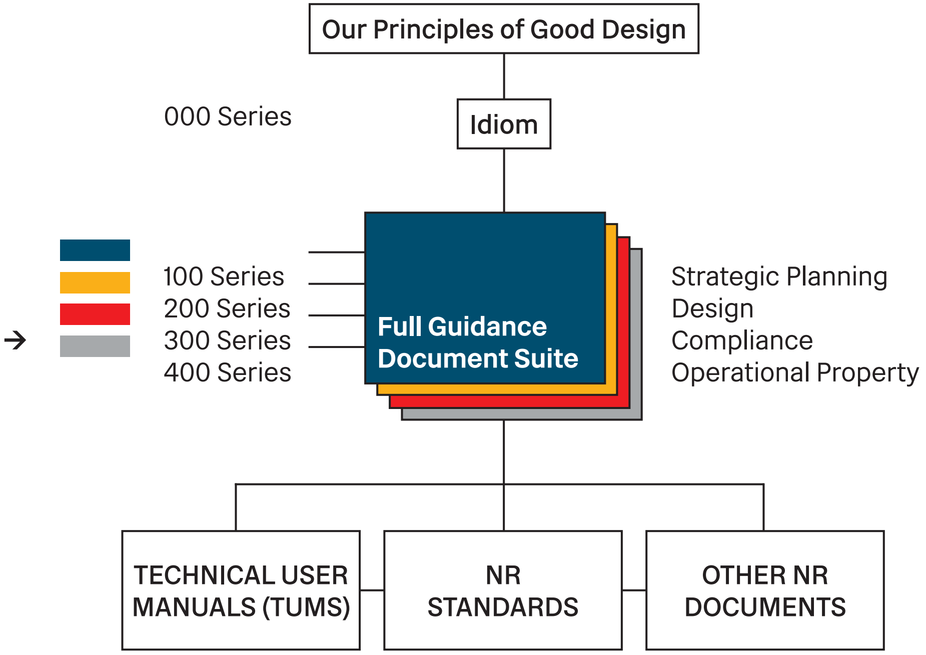
How to use the guidance suite

The Network Rail Document Suite

You are here

Security at Stations

DRAFT



References to other documents

🟨 Code of Practice Guidance
🟪 National Standard
⬜ Network Rail document
🟦 National Technical Specification Notice

Example:

National Technical Specification Notice

PRM NTSN
National Technical Specification Notice
Persons with Reduced Mobility (2021)

A full list of relevant documents, and other guidance suite documents is contained in the appendix.

Contents

Contents

Image 0.1
London Bridge station and the Shard

Security at Stations Design Guidance Manual

Introduction

1

Image 1.1
Birmingham New Street Station

1.1 Purpose

This guidance document provides advice to those working on rail station design projects, on how to assess, design and implement various forms of physical security measures at stations across the rail network.

This guidance sits within a suite of design manuals developed by Network Rail to help improve the quality and efficiency of all aspects of design at rail stations.

Security threats can take many forms, from simple anti-social behaviours through to criminality and terrorism. Detection can be natural or technical and a security response could take multiple effective forms. Physical security is the effective combination of measures to deter, delay, detect and respond to a security threat.

Successful implementation of physical security can result in a safer station environment, which in turn can improve the passenger experience and contribute to an improved rail network with decreased fear of crime.

The purpose of this design manual is to support those working in the station design sphere and offer clear advice which summarises and simplifies existing regulations, legislation and guidance from across the industry.

Image 1.2:Paddington Station Platform

1.2 Scope

Where applicable and appropriate this document uses examples and scenarios. These are not intended to encompass all options and alternatives and are used only to illustrate general concepts. It is the designer's responsibility to use their professional skills and judgement to apply any examples or scenarios suitably and to interpret and apply them correctly, seeking additional guidance from Network Rail wherever this might be required.

Those working on station design projects are expected to use the guide to inform the design process, applying the guidance appropriately to each project. Interpretation of any elements of this document is at the discretion of Network Rail or their appointed delegates. For any specific project, in the event of clarification being required, it is recommended that formal requests and queries are raised where needed, and that key security decisions and strategies are agreed and documented in line with established Network Rail processes.

The following material should be used on projects, in parallel with this design guide, for more information on given themes:

→ Primary Topic Guidance including Land Transport Security Compliance, Security in Design of Stations (SIDOS) and Protecting Crowded Places;

→ Useful Additional or Related Guidance including The Building Regulations, DfT Design Standards for Accessible Railway Stations and Rail Industry Standard for Station Infrastructure;

→ Publicly available or commercial standards including Loss Prevention Certification Board, British and European (EN) Standards and Publicly Available Specification (PAS) and International Workshop Agreement (IWA) Standards;

→ Legal Obligations including the Equality Act and the Construction and Design Management Regulations.

Other references will be found in the References Section which can be found in the Appendices of this Design Guide.

For projects that are likely to have a high security significance, it is recommended that Project Teams obtain specialist expert guidance from relevant partner organisations and consultants to check that security threats and risks are understood, and to inform the design process with the most relevant and appropriate security guidance. This might include members of the Register of Security Engineers and Specialists or equivalently qualified professionals.

1.3 Strategic Planning

Security design consideration should start at the strategic planning stage of a project. When initially space planning a project, preference should be given to open, generous spaces with clear lines of sight, inviting levels of natural and artificial lighting and barriers which are effective, without feeling intimidating or creating a fortress environment. These concepts should be considered across all areas of the station, including on platforms, bridges and subways, waiting areas, ticket halls and also the public realm, including car parks, taxi ranks and perimeter access routes.

Technological security systems, such as video surveillance systems (VSS) or electronic access control, should be strategically positioned and calibrated for optimum efficiency.

Projects should be guided by the threat and vulnerability assessments (TVRAs) undertaken by the relevant security stakeholders (including partner organisations such as the British Transport Police). Projects should ask Network Rail for the output of the TVRA, or a summary of this if classified.

The Security Category of the station should be understood by the project team. This will drive some of the necessary security design interventions and measures required. Where relevant, projects should consider resistance to blast in the early stages of design. This is usually necessary at projects at stations which are in Security Category A and B, but should be confirmed by Network Rail as part of the TVRA output. As part of this undertaking, designers should consider using alternatives to glass, such as Ethylene tetrafluoroethylene (ETFE).

Technical security performance criteria should be agreed as early on in the design as possible, for key components such as doors, glazing, walls, shutters and fences.

Security design should be a collaborative endeavour, and through Network Rail, partner organisations (such as the British Transport Police) should be involved in projects for expert support and guidance.

Image 1.3: Glasgow Station concourse

Introduction
1.4 Information Security

Information security is a separate subject and is not within the scope of this document. However, it is useful to make reference here to some basic requirements for Project Teams to follow in relation to the information that is created as part of the design process.

Security of information, especially information related to security strategies could affect and impact:

→ Station and network reputation
→ Railway business continuity
→ Passenger experience

Failure to correctly secure information might incur costs to recover or redact information or to change security arrangements should the efficacy of the security strategy be jeopardised.

In serious cases, failure to correctly secure information could put passenger safety at risk, should the information be used with hostile intentions.

For further general guidance on information security see the Network Rail Security Assurance Framework, which confirms the security classification of different types of station design project information. For the security of Building Information Management (BIM) see BS EN ISO 19650.

Every document should have an owner who is responsible for setting the document security classification. The person commissioning a document, rather than the person writing the document, may well be the owner and should be consulted when the document setup is undertaken.

Seek to avoid aggregating too much information into one document or location.

NR Guidance Suite Reference

Network Rail Information Security Policy
NR/L1/INF/02232

Document authors should include the security classification and handle the document appropriately. All documents should have a classification, even if to state the document in publicly available or has no classification at all.

Split security information into different documents with links or references. For example it is good practise to have separate drawings for access control measures, CCTV equipment and secure boundary buildups.

Security of information is based on the principles of “need to know”. Consider the intended recipient of each document and what they are required to know vs what they do not need to know.

The owner of a specific document, and anyone handling it, should be mindful of how it is being transmitted and stored. Distribution records might be necessary, as might the use of secure transmission systems such as Egress.

Introduction

1.4 Information Security Continued

Be aware that Local Authority Planning Portals will place information within the public domain. There are processes in place with many planning authorities for the handling of security sensitive project and information which should be adopted early if necessary.

It is best to redact or omit room names or any security specific information on drawings uploaded to planning, or to make special arrangements with planning officers for certain types of information to not be made publicly available on the accessible portal.

It is important to note that once information is released it can rarely be retrieved. It is important then to consider what is acceptable to release before it leaves the control of a project.

Project information should be archived upon completion of the project. This might include physical and technological archiving of documents plus the implementation of access protocols and passwords should the information need to be retrieved in the future.

It may not be clear how information could be helpful to an adversary. If in doubt seek advice from qualified persons. The inclusion of all information might seem helpful, but when this is viewed by hostile persons this can have a security impact on both current and future projects.

From a project’s inception, the use of Common Data Environments may be useful for design coordination, information sharing and storage. Access permissions to such environments should be carefully managed and reviewed.

Be aware of long email chains which can aggregate information. Long email chains, especially where multiple parties contribute, can inadvertently contain significant amounts of information and will increase the possibility of breaking the “need to know” principle.

It is also good practise to check all recipients before sending information, to check that it is appropriate for all the recipients to receive the information being transmitted.

1.5 Getting Home Safe

Throughout this guide considerable information is provided on the technical processes, technical requirements and Standards related to security design at stations. As well as these, projects are reminded to consider the experiential qualities that help create a secure station environment which, crucially, helps to instil a feeling of safety for passengers.

Feeling safe when travelling is an important part of the journey experience for everyone, regardless of the journey distance, purpose, route, mode or timing. The need for safe public spaces is paramount and those involved in station projects should try to create services and public spaces that are safe for everyone; regardless of characteristics, such that everyone feels able to travel when and how they like, from first to final mile, in both daylight and after dark.

As well as the station and its immediate perimeter, where possible within the brief, projects should consider how the scheme sits as part of wider passenger journeys. This might mean reviewing street lighting on nearby pedestrian approach routes, checking local mobile phone and CCTV coverage or considering other transport infrastructure which rail passengers might require on route to the station.

Whilst the project might not be able to immediately deliver upgrade works to areas beyond the station boundary, conversations around such matters might stimulate local authorities and other public realm stakeholders to commission and undertake separate projects, with the station works acting as a catalyst for wider security focussed upgrades.

Security works aimed at improving passenger experience might take the form of low to the ground, well maintained landscaping, active street frontages creating a sense of movement and activity, digital interventions such as digital wayfinding, community focussed interventions or look and feel type aspects, such as considered material choices or public art work, to imbue a sense of personal security for passengers.

Introduction

1.5 Getting Home Safe Continued

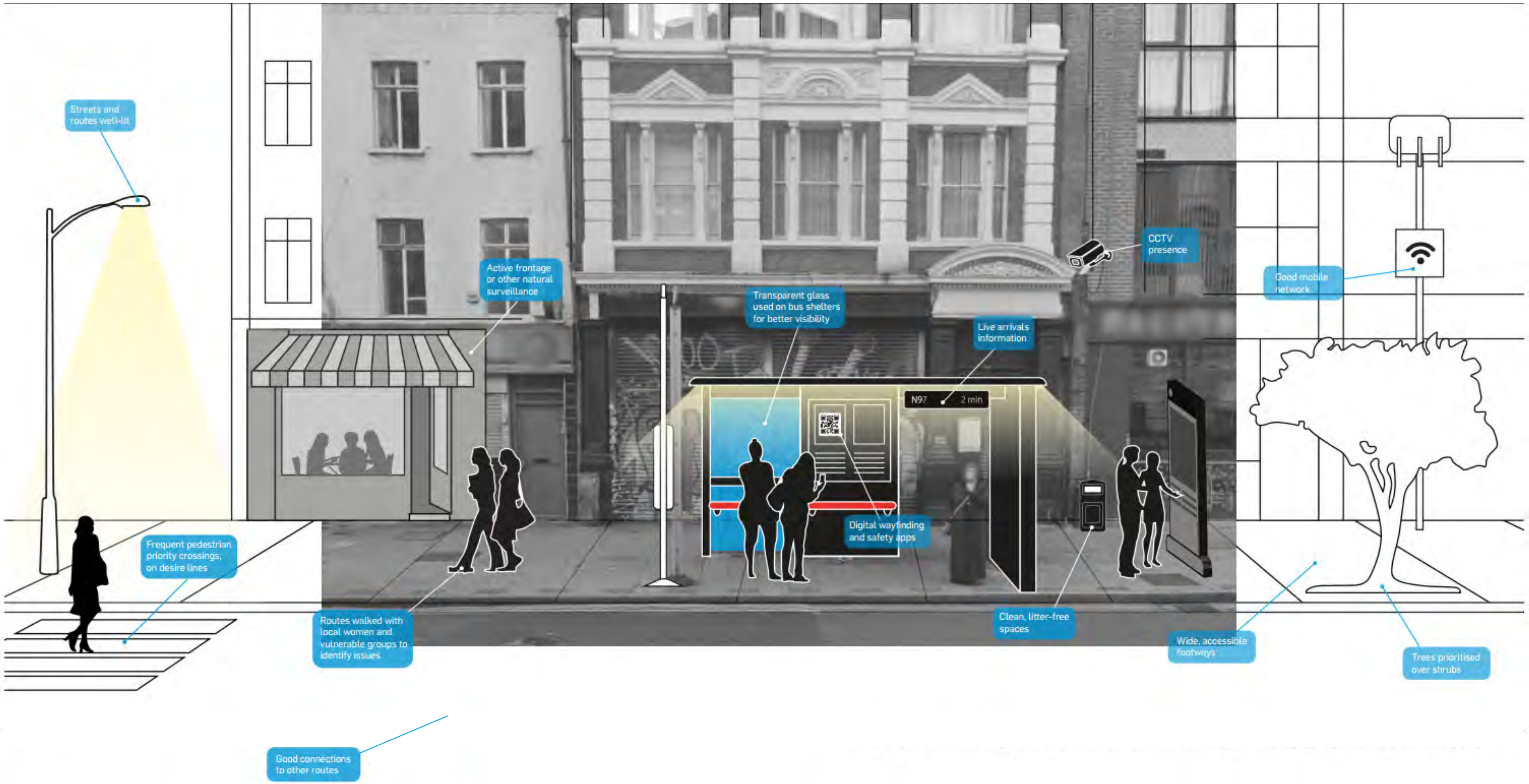

Streets and routes well-lit
Active frontage or other natural surveillance
Transparent glass used on bus shelters for better visibility
CCTV presence
Good mobile network
Live arrivals information
N97 2 min
Frequent pedestrian priority crossings, on desire lines
Digital wayfinding and safety apps
Routes walked with local women and vulnerable groups to identify issues
Clean, litter-free spaces
Wide, accessible footways
Trees prioritised over shrubs
Good connections to other routes

Figure 1.4: Bus stop environment assessed according to 'Safe by Design by Women' principles

Image 1.5
NR Worker and BTP Officer

Security at Stations Design Guidance Manual

2

Station Security Categories

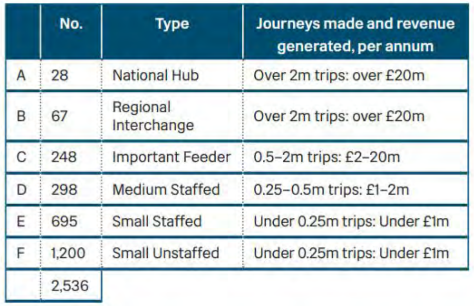
Waterloo East via escalator
GENERATING blue
LOW CARBON ELECTRICITY
FOR THE GAMES.
edf
official electricity supplier
of the Olympic and Paralympic Games
Boots
HELPING
SHIN
Information
12
13 13
14

Image 2.1
New Balcony at Waterloo Station

2.1 Types of Stations

Stations are categorised into six types by the Department for Transport (DfT). This categorisation is determined by the frequency of usage of the station plus complexity of interchange.
The largest, busiest Stations on the Network fall in to Category A with the smallest, least busy Stations falling in to Category F.

The NR Station Design Guide (ref. NR/GN/CIV/100/02) gives further information on these six different types of station classification which are most likely to have differing security requirements



	No.	Type	Journeys made and revenue generated, per annum
A	28	National Hub	Over 2m trips: over £20m
B	67	Regional Interchange	Over 2m trips: over £20m
C	248	Important Feeder	0.5–2m trips: £2–20m
D	298	Medium Staffed	0.25–0.5m trips: £1–2m
E	695	Small Staffed	Under 0.25m trips: Under £1m
F	1,200	Small Unstaffed	Under 0.25m trips: Under £1m
	2,536		

Network Rail Guidance Suite Reference

Network Rail Document Station Capacity Planning. NR/GN/CIV/100/03

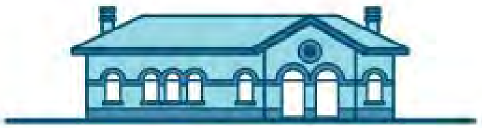
Table 2.2: Different category of stations and their attributes

Category A - National Hub

The largest stations, these are major termini or interchanges. Examples include Birmingham New Street, London King's Cross and Cardiff Central.

Category B - Regional Interchange

These stations are key hubs on the network, serving cities and major towns, or acting as interchanges. Examples include Cambridge, Derby and Clapham Junction.



Category D- Medium Staffed

These stations serve inter-urban business or a particularly high volume of urban commuting.

Category F - Small Unstaffed

These amount to almost half of the stations on the network. These stations serve local communities and can vary widely in terms of size and facilities provided. They often have a surprisingly large station building as part of a historic legacy, with a civic presence that defines the character of the immediate area.

Figure 2.3: DfT Station Categorisation A-F

2.2 Security Categories

Further to the six DfT station categories, the National Railway Security Programme (NRSP) categorises Stations in to four different security categories, from A through to D. The NRSP station security categories are specifically about categorising stations in order to apply appropriate controls to protect from Terrorism. Passenger footfall represents the core categorisation criteria, but other factors are included, and these are weighted to determine the overall classification of the Station.

This security categorisation is the responsibility of the Station Facilities Operator (SFO) and categorisation decisions are then shared with DfT Land Transport Security who control the station security category list. This categorisation may change over time and is reviewed by the SFO annually or when a significant change to the station is happening.

Those involved in station design projects should consult with the SFO, Network Rail Region or Route Security Team, or Group Security in the Network Rail Technical Authority, to ascertain the security category of the station where work is proposed, such that proportionate security measures can be considered and implemented in accordance with the Network Rail Security Assurance Framework.

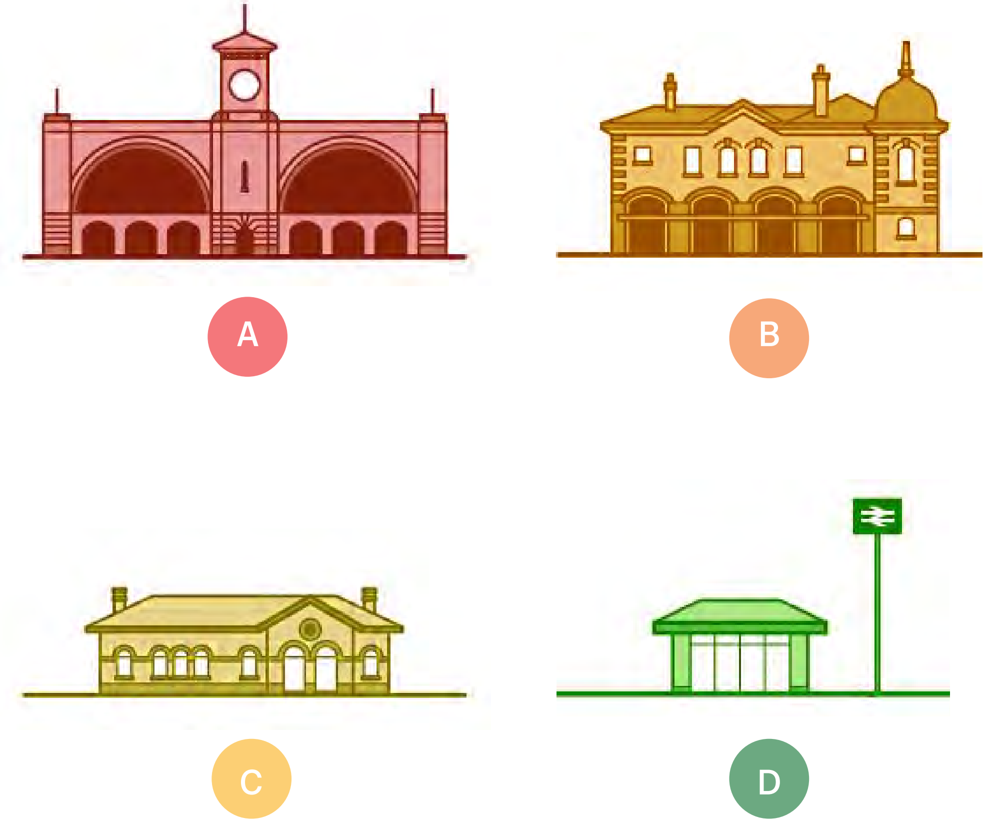


Figure 2.4: NRSP Station Categorisation A-D

National Standard

National Railway Security Programme (NRSP)

2.3 Security Requirements (per Security Category)

Deliverables, Processes & Guidance	Security Category A Station	Security Category B Station	Security Category C Station	Security Category D Station
Conduct a physical security triage for the proposed works	■	■	■	■
Notify the station nominated security contact (NSC)	■	■	■	■
Inform Station Security Committee of the proposed project	■	■		
Establish a Security Working Group for the project	■	■	■	■
Prepare a Station Security Plan and Station Security Incident Response Plan	■	■	Optional	Optional
Undertake a localised Threat Risk and Vulnerability Assessment	■	Optional		
Prepare a Station Security Zoning Plan	■	■	■	■
Undertake a Threat Risk and Vulnerability Assessment (focussing on counter terrorism)	■	■	Optional	Optional
Undertake a BTP Crime Reduction Risk and Vulnerability Assessment	■	■	■	■
Follow the guidance set out in Security in the Design of Stations (SIDOS)	■	■	■	■
Review the need for Hostile Vehicle Mitigation (HVM) measures	■	■		
Undertake a blast assessment and design	■	■		
Undertake a Station Categorisation Assessment	■	■	■	■
Prepare a Security Assurance Plan	■	■	■	■

Table 2.5: Table of deliverables, processes, and guidance that is needed for each category of stations

This table sets out high level security processes and measures which may be required depending on the security category of the station where work is proposed. This is not exhaustive and is offered as a guide only - the Network Rail Security Teams should be contacted for further information on specific station applications and the Network Rail Security Assurance Framework (NR-SAF) consulted for further information.

Table Key:

■ Activity Required

░ Suggested/ Optional

National Standard

National Railway Security Programme (NRSP)

Station Security Categories
2.3 Security Requirements Continued

Asset in Station	Security Category A	Security Category B	Security Category C	Security Category D
Provide a Station Control Room	■	Optional - Suggested	Optional - Suggested	
Provide a British Transport Police Office *	■	Optional - Suggested	Optional - Suggested	
Provide lost property and left luggage security scanning facilities	■	Optional - Suggested		
Provide evacuation rendezvous points	■	■	■	■
Provide emergency evacuation signage and wayfinding	■	■	■	■
Provide a public address system	■	■	■	■
Provide a CCTV system	■	■	■	■
Provide electronic access controls to relevant assets and areas	■	■	■	■
Provide an intruder detection system to relevant areas	■	■	■	Optional - Suggested
Provide a secure, identifiable station boundaries	■	■	■	■
Provide secure cycle storage	■	■	■	■
Provide security awareness posters and or signage	■	■	■	■
Provide passenger help points	■	■	■	■

Table 2.6: A table of assets that are required in different categories of stations

Table Key:

■ Activity Required

▒ Suggested/ Optional

* BTP Facilities to be discussed on a station by station basis

2.4 Station Zoning

Every station should have a security zoning plan. This is the responsiblity of the Station Facilities Operator (SFO) to prepare, review and share with relevant stakeholders as an output from a local risk and vulnerability review. Different security measures may be required in different zones of the station. These zones should be considered during the security risk assessment to check that any measures are proportionate to the identified risk.

The security zoning of the station sits above the general security rating which does not take into account specific areas of the station.

Areas that may be subject to security zoning may include:

→ Perimeter (the whole station footprint)
→ Car parks
→ Cycle parking
→ Entrances and exits (both foot and vehicle)
→ Forecourts / dropping off and picking up areas (including taxi ranks and bus stops)
→ Booking hall
→ Ticket barriers
→ Ticket offices
→ Ticket vending machines
→ Platforms
→ Waiting rooms
→ Back of house staff areas
→ Passageways and footbridges
→ Lifts
→ Escalators and stairs
→ Retail outlets (including licensed premises)
→ Waste and refuse areas
→ Rendezvous Points (RVPs) and evacuation routes

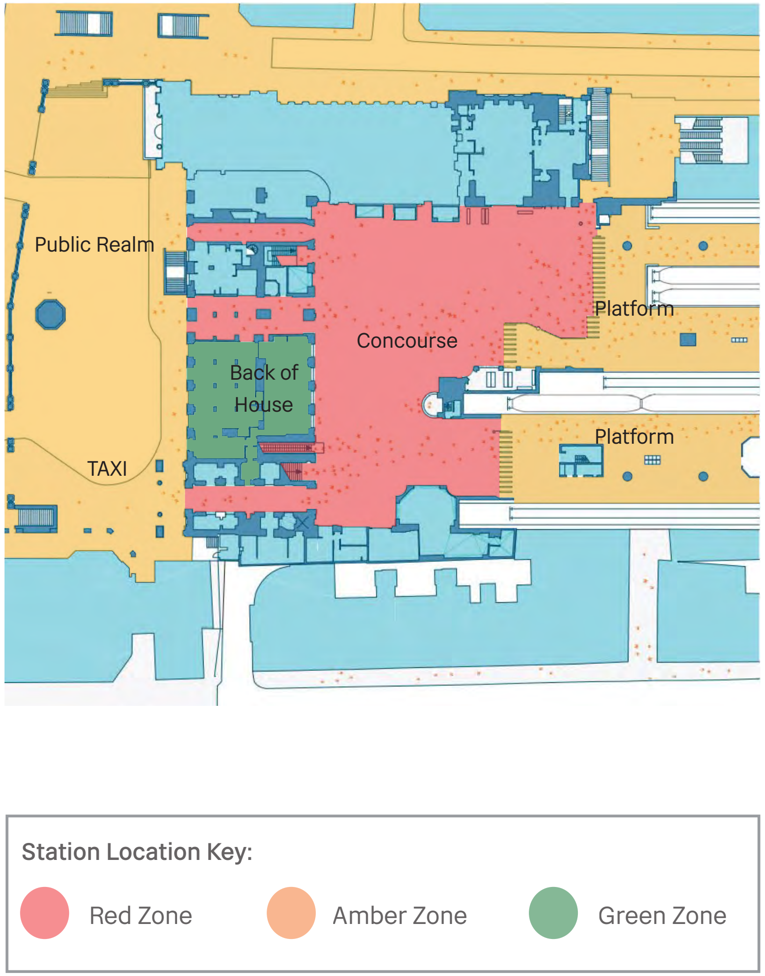


Figure 2.7: Indicative plan of Charing Cross station zoning

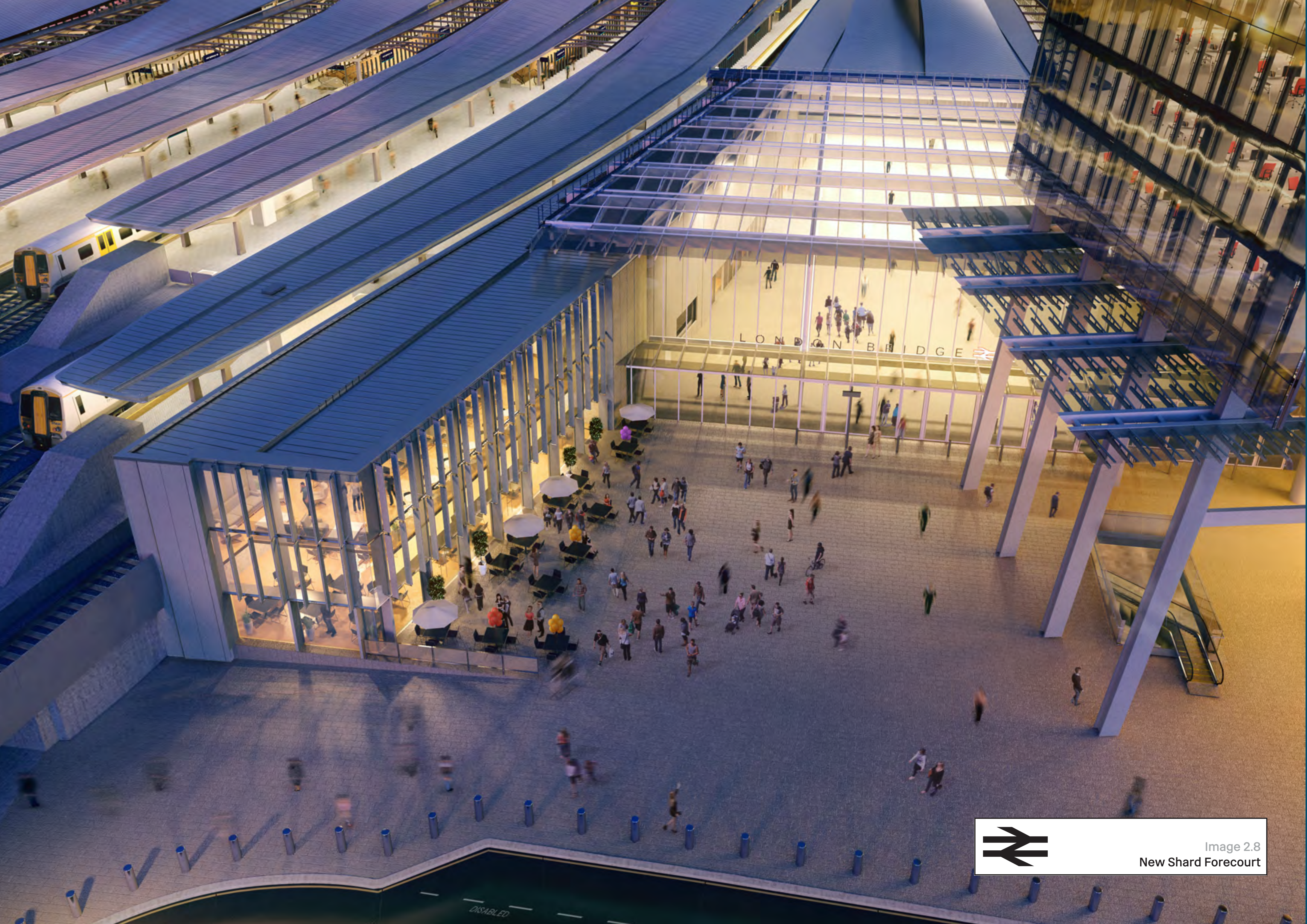


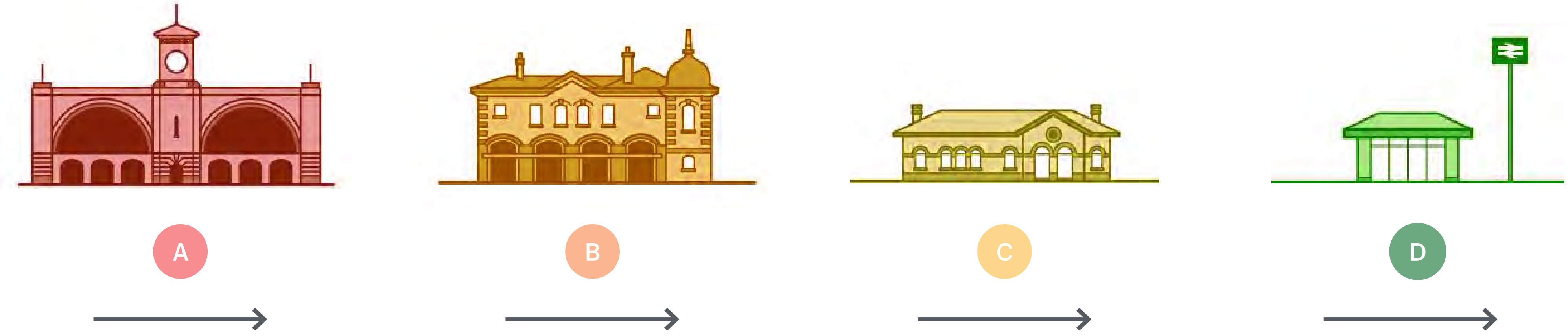
Image 2.8
New Shard Forecourt

3

Security at Stations Design Guide Manual

Security Risk Management

3.1 The Security Risk Review Process



When a project has confirmation of a Station's security category (A-D), the security review process should begin to identify different types of security threats which might inhibit the station, the likelihood of these threats happening, the severity, should they occur, plus ways in which these could be mitigated and security risks lowered.

The extent to which different members of a project team are involved in the project security review process will vary, depending on the team and the project.

The method for assessing, communicating, and managing security risk and assurance activities in projects and in operation across Network Rail station projects is defined in the Network Rail Security Assurance Framework (NR-SAF).

The NR-SAF defines different 'streams' of security review and assurance work for different types of Network Rail projects. Physical security is most relevant to station projects and it's generally this stream of the NR-SAF which should be followed for station design projects.

National Standard

National Railway Security Programme (NRSP) Section 7 Station Security (Official Sensitive)

Figure 3.1: NRSP Station Categorisation A-D Severity

3.2 Security Assurance Framework

The Network Rail NR-SAF Physical Stream requires all projects to undertake an initial 'security triage' to determine which further actions from the NR-SAF should be followed. This involves two high level questions and the workflow illustrated opposite.

This triage will generally be led by the Network Rail Security Team but Designers and external Security Consultants may be called upon to provide input and support depending on the project and team.

For support in conducting an initial security triage, refer to Network Rail Group Security or the Route or Regional Security Team relevant to the Project.

National Standard

National Railway Security Programme (NRSP) Section 7 Station Security (Restricted)

NR Guidance Suite Reference

Security Assurance Framework (NR-SAF)

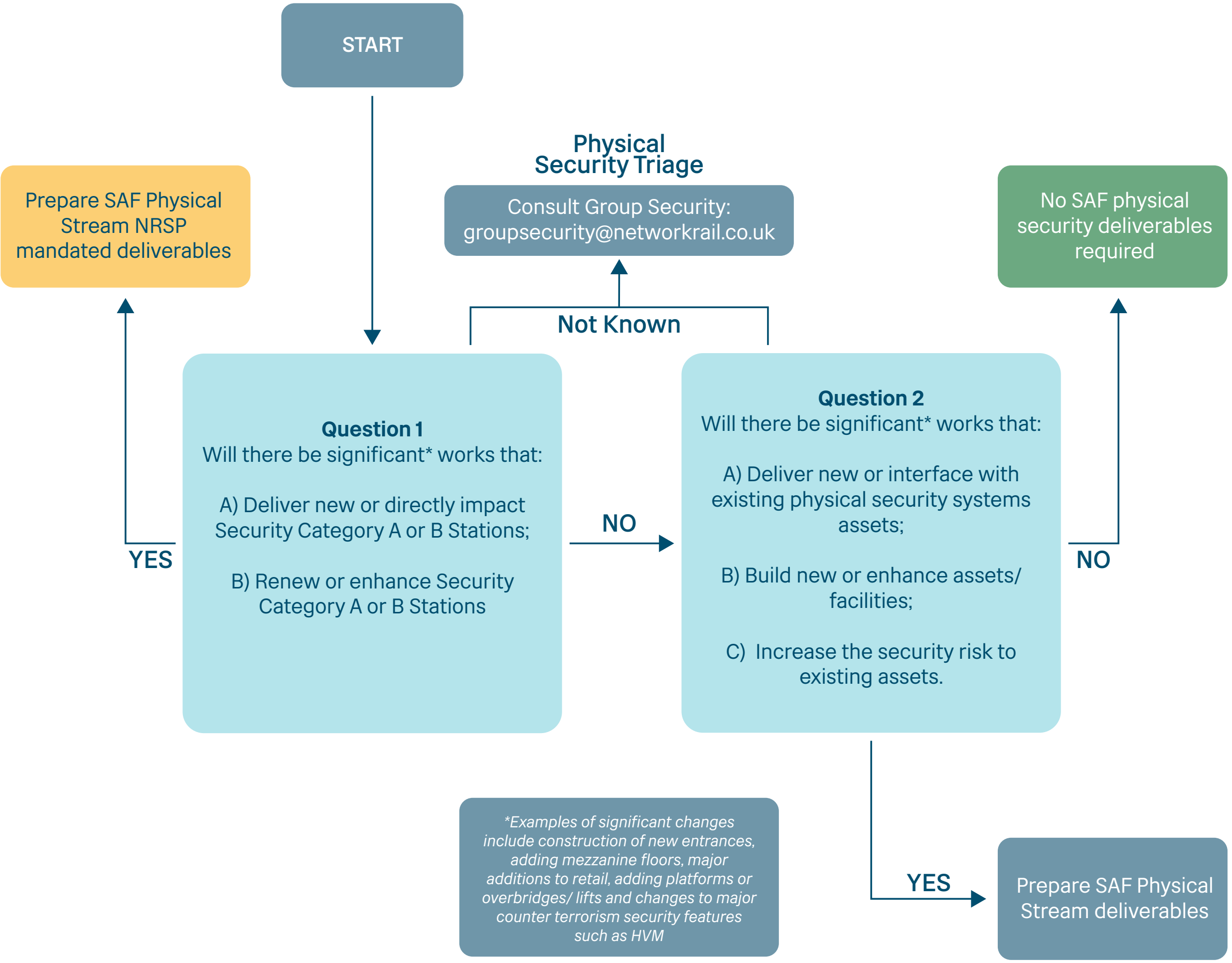

START
Physical Security Triage
Consult Group Security: groupsecurity@networkrail.co.uk
Not Known
Prepare SAF Physical Stream NRSP mandated deliverables
No SAF physical security deliverables required
YES
Question 1
Will there be significant* works that:
A) Deliver new or directly impact Security Category A or B Stations;
B) Renew or enhance Security Category A or B Stations
NO
Question 2
Will there be significant* works that:
A) Deliver new or interface with existing physical security systems assets;
B) Build new or enhance assets/ facilities;
C) Increase the security risk to existing assets.
NO
*Examples of significant changes include construction of new entrances, adding mezzanine floors, major additions to retail, adding platforms or overbridges/ lifts and changes to major counter terrorism security features such as HVM
YES
Prepare SAF Physical Stream deliverables

Figure 3.2: A diagram explaining the Physical Security Triage

Security Risk Management

3.3 Conventional Security Threats

The following are common conventional security threats which should be considered in security risk assessments for projects in all Station Security Categories. This list is offered as a guide to projects and may not be exhaustive, suicide for example is excluded.

Table 3.3: Table of conventional security threats in stations

Protest and public order	→	Individuals have the right to peaceful protest; however, there is a risk that peaceful protest will cause disruptions and escalate
Criminal damage and sabotage	→	A person who without lawful excuse destroys or damages any property belonging to another, intending to destroy or damage any such property, or being reckless as to whether any such property would be destroyed or damaged, shall be guilty of an offence
Theft	→	The act of taking something that belongs to someone else and keeping it.
Antisocial behaviour	→	Behaviour by a person which causes, or is likely to cause, harassment, alarm or distress to persons.
Unauthorised access (including tresspass and persons in precarious positions (PIPP))	→	To enter a private property or protected area or structure without permission. This might include protesting in areas which cause disruption to the railway as well as accessing back of house areas with malicious intent.
Nuisance	→	Causing inconvenience or annoyance, perhaps acts such as loitering, nuisance driving and parking or flytipping.
Burglary	→	The act of illegally entering a building and stealing assets.
Graffiti	→	This is a form of visual communication, usually illegal, involving the unauthorised marking of public space by an individual or group.
Cycle Crime	→	This refers both to thefts of cycles and thefts from cycles. Thefts of cycles include thefts for transportation, thefts in which stolen cycles are traded in for cash or drugs, thefts of specific bikes to order and thefts to facilitate further crimes.

3.4 Terrorist Threats

The following are terrorist security threats which should be considered in security risk assessments for projects in Station Security Categories A and B. This list is offered as a guide to projects and may not be exhaustive or up to date. Projects should consult with the Network Rail Security Team in all cases where these threats might apply:

Table 3.4: Table of terrorist threats in stations

Vehicle Borne Improvised Explosive Device (VBIED) Including: Parked, Encroachment, Penetrative, Deception, Duress.	→	A VBIED is a vehicle which contains and delivers an improvised explosive device to a target. The vehicle may be old or new, inexpensive or valuable, liveried or plain, blend into most situations and / or be modified to prevent detection. VBIED size is defined by SIDOS.
Vehicle as a Weapon (VAW)	→	A vehicle by itself can also be used with hostile intent as a weapon to injure and kill people or breach a perimeter, ram and damage infrastructure.
Improvised Explosive Device (IED) - Left Package	→	An improvised explosive device (IED) is an explosive device intended to be detonated remotely from a package left on site. The explosives may be home made through to military grade and may contain fragments such as nails or shrapnel intended to cause additional injury and damage. The device may vary in size from apparent rubbish, to briefcase, to rucksack or larger.
Improvised Explosive Device (IED) - Hand Delivered / Mail	→	An improvised explosive device (IED) is a device constructed and deployed in ways other than in conventional military action. Carried out through hand delivery.
Person Bourne IED (PBIED), including suicide	→	Person-borne IED (PBIED) is an improvised explosive device often containing shrapnel worn, carried or housed by a person, either willingly or unwillingly.
Improvised Incendiary Devices	→	Improvised Incendiary Device An IID is a device designed to destroy, incapacitate, harass, or distract by creating intense heat and fire, rather than by exploding.
Stand-off attack (Projectile)	→	Standoff weapons are missiles or bombs which may be launched from a distance sufficient to allow attacking personnel to evade the effect of the weapon or defensive fire from the target area.
Shooting and close quarter attack	→	Close-quarters combat (CQC) is a close combat situation between multiple combatants involving ranged weapons, typically firearms.

Security Risk Management

3.4 Terrorist Threats Continued

Table 3.5: Table of terrorist threats in stations

Unmanned Aerial Systems (UAS) delivered attack, sometimes referred to as drone or Unmanned Aerial Vehicle (UAV)	→	A UAS can be used to cause danger and disruption, furthermore, they can be used to carry out remote attacks and pose risk to national infrastructure sites, sensitive sites, crowded places, and major events.
Marauding Terrorist Attack (MTBA) - Bladed and blunt forced weapon	→	Marauding terrorist attacks (MTA) are fast-moving, violent incidents where assailants move through a location aiming to find and kill or injure as many people as possible; in this circumstance, using a bladed or blunt force weapon.
Marauding Terrorist Attack (MTFA) - Firearm	→	Marauding terrorist attacks (MTFA) are fast-moving, violent incidents where assailants move through a location aiming to find and kill or injure as many people as possible; in this circumstance, using a firearm.
Chemical, Biological and Radiological attack (CBR)	→	‘CBR’ is used to describe the malicious use of Chemical, Biological, and Radiological materials or weapons with the intention to cause significant harm or disruption.
Fire as a Weapon (FAW)	→	Fire as a weapon (FAW) is the deliberate use of fire within a terrorist attack with the intent to cause harm. This may include causing harm to people, premeditated damage to property or be used as a means to cause evacuation of persons to a predefined location where further harm can be caused, potentially as part of a layered attack.
Insider threat	→	An insider threat is a malicious threat to an organisation that comes from people within the organisation, such as employees, contractors etc. who have inside information concerning the organisation’s security practices, data and computer systems.
Sabotage	→	Sabotage is deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information. This may come from disgruntled employees or otherwise.
Kidnapping	→	Kidnapping is the unlawful taking and carrying away of a person by force and detaining the person against their will.

3.5 TVRAs and Security Risk Assessments

Following an initial security triage, the Network Rail Security Assurance Framework (NR SAF) sets out routes for different types of Threat and Vulnerability Risk Assessments known as TVRAs.

Broadly, for significant station projects falling into Station Security Category A and B, National Railway Security Programme (NRSP) mandates that a terrorism TVRA should be undertaken, as well as a review considering conventional crime threats. This process should generally be led by the Network Rail Security Team and involve participants from British Transport Police (BTP), Centre for Protection of National Infrastructure (CPNI), the Station Facilities Operator (SFO) and at times the wider design team.

For significant projects involving stations falling into Station Security Categories C and D, the terrorism TVRA is not mandated, but a review of conventional crime threats should be undertaken. This type of review should generally be led by the Network Rail Security Team or BTP and might involve the SFO and wider design team.

The TVRA process employs a sequential methodology that results in a security mitigation solution that precisely aligns to the risks faced to the project. The TVRA methodology is designed to provide a repeatable and scalable, evidence driven process that logically flows from objective data, through specialist analysis to recommendations. The process is designed to be auditable, by rigorously maintaining the linkages between input and output and minimising subjectivity in favour of objective discovery and analysis.

The development of TVRAs should be project specific and relies on an understanding of the specific and credible threats posed to an organisation or site and of concern to the security stakeholders, and how vulnerable a site is to these threats.

Importantly, the extent to which the Project Team are involved in TVRAs will vary depending on the project and the team. Crucially, all projects should consult the Network Rail Security Team to check that a TVRA is has been undertaken for the project and that the right people within the Design Team are aware of what might need to be implemented.

Threat – A factor or event which could potentially cause the loss of or damage of assets.

Vulnerability – A weakness or a flaw in a security system or any business process that could conceivably be exploited by a threat.

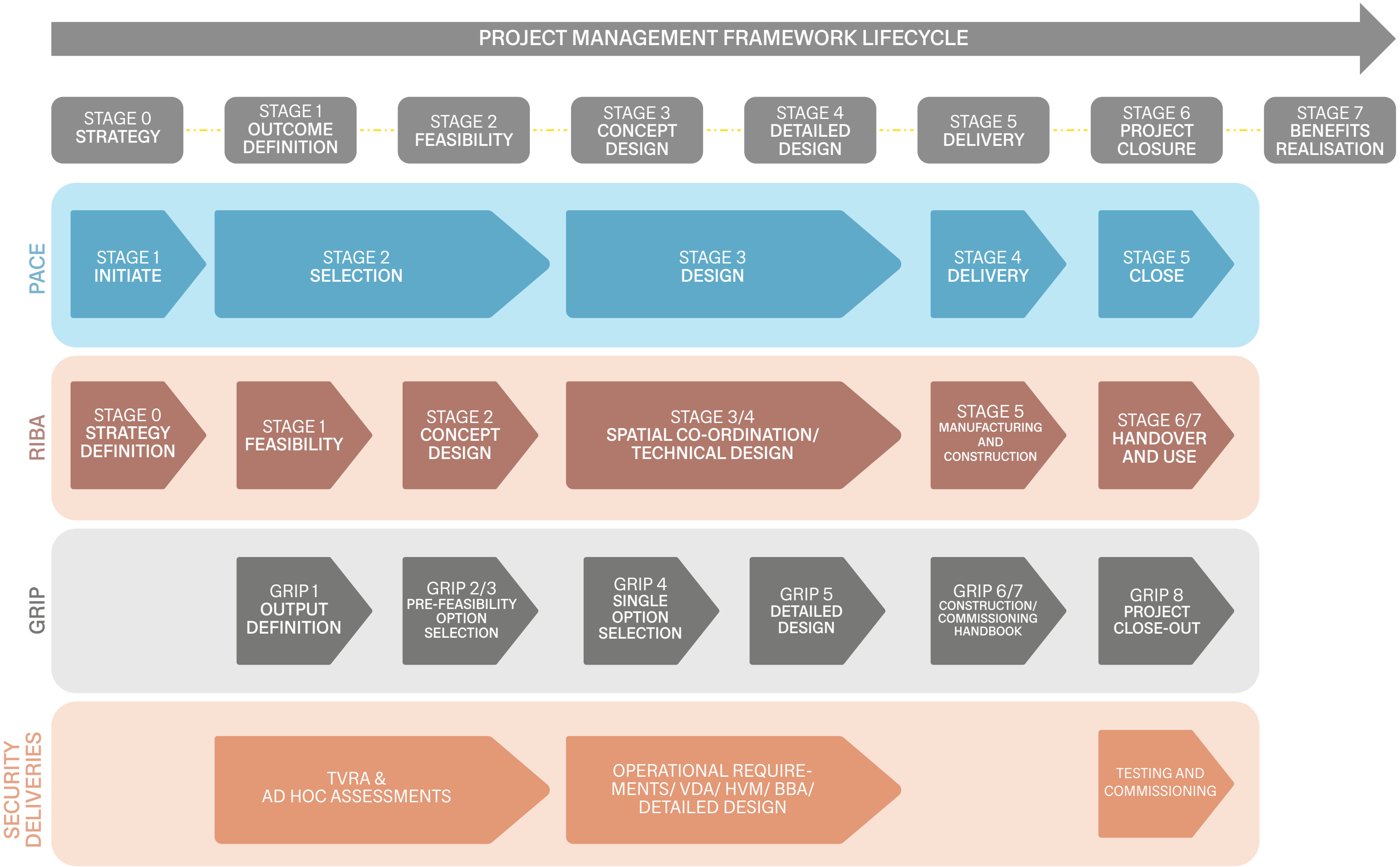
Risk – A potential event that will have foreseeable consequences for assets and impact on the success criteria.

Threat assessment – The analysis of threat inherent in the environment, assessing threat sources, methods, capability, intent, targets and actions.

Risk assessment – The overall process of risk identification, risk analysis, and risk evaluation.

Figure 3.6: Definitions of what the Threat and VulnerabilityRisk Assessments mean in TVRA

3.6 Security Risk Management Timeline



PROJECT MANAGEMENT FRAMEWORK LIFECYCLE

STAGE 0 STRATEGY
STAGE 1 OUTCOME DEFINITION
STAGE 2 FEASIBILITY
STAGE 3 CONCEPT DESIGN
STAGE 4 DETAILED DESIGN
STAGE 5 DELIVERY
STAGE 6 PROJECT CLOSURE
STAGE 7 BENEFITS REALISATION

PACE

STAGE 1 INITIATE
STAGE 2 SELECTION
STAGE 3 DESIGN
STAGE 4 DELIVERY
STAGE 5 CLOSE

RIBA

STAGE 0 STRATEGY DEFINITION
STAGE 1 FEASIBILITY
STAGE 2 CONCEPT DESIGN
STAGE 3/4 SPATIAL CO-ORDINATION/ TECHNICAL DESIGN
STAGE 5 MANUFACTURING AND CONSTRUCTION
STAGE 6/7 HANDOVER AND USE

GRIP

GRIP 1 OUTPUT DEFINITION
GRIP 2/3 PRE-FEASIBILITY OPTION SELECTION
GRIP 4 SINGLE OPTION SELECTION
GRIP 5 DETAILED DESIGN
GRIP 6/7 CONSTRUCTION/ COMMISSIONING HANDBOOK
GRIP 8 PROJECT CLOSE-OUT

SECURITY DELIVERIES

TVRA & AD HOC ASSESSMENTS
OPERATIONAL REQUIREMENTS/ VDA/ HVM/ BBA/ DETAILED DESIGN
TESTING AND COMMISSIONING

Figure 3.7: Project management framework lifecycle

3.7 Operational Requirements

For some projects, further to the TVRA, the production of a series of Security Operational Requirements, or Operational Requirements may be required. The Network Rail Security Team can confirm this, during the initial Security Triage.

Operational Requirements are an analytical and systems based approach that strive to remove subjectivity and deliver transparent and repeatable results to security assessment. ORs provide a record of the performance requirement decisions and enable the design to be assured in relation to security considerations. Operational Requirements should outline the function of the possible solution, potential concerns (e.g., external and physical constraints), integration and interfaces, and the performance requirements.

Operational Requirements documents typically address the potential requirement for the following key security measures:

- Video Surveillance System
- Systems to control access
- Hostile Vehicle Mitigation
- Intruder Detection System / Intruder Alarm System
- Physical security (doors, windows, glazing, building, fences, and gates etc. in relation to physical attack and blast performance)
- Security lighting
- Perimeter Intrusion Detection System (PIDS)

When a security risk assessment is complete and a security design measure approved, it might be necessary to develop a Construction Phase Security Plan (CPSP). The Network Rail Security Team can confirm when this may be required.

Code of Practice Guidance

CPNI Operational Requirement Guidance

Image 3.8
London Marylebone Station

4

Security at Stations Design Guide Manual

Designing Out Crime

Image 4.1
Abbey Wood Station

Designing Out Crime

4.1 Overview

Good design of the station environment can reduce the opportunities for crime and thus help to reduce operating expenditure due to activities such as vandalism, theft, and disruption incidents. Good design can make it easier to spot vulnerable people who may need assistance, reducing the risk of potential harm. Good physical design and maintenance can also improve passenger perception and the overall feeling of safety and security, which in turn can increase passenger numbers and revenue.

The development of the security design process should include consultation with the local Designing Out Crime Officer (DOCO) and the British Transport Police (BTP), in order to enhance the value of the project outputs, and to meet the unique requirements of the security design.

This section sets out some good general principles for station design and facilities, contact ‘design-outcrime@btp.police.uk’ for more information.

Figure 4.2: British Transport Police Logo

Image 4.3: BTP officers and Network Rail woker

4.2 Secure Stations

The Secure Stations Scheme is an accreditation opportunity for station operators to demonstrate how they are working with partners to reduce crime and play a greater role in safeguarding vulnerable people who might be at stations. An accredited station provides reassurance to passengers and staff that the station is a safe and secure environment.

Secure Stations is a national scheme which covers all rail networks that are policed by the BTP. The scheme establishes good practice standards and accredits stations which have worked with the BTP and local partners to improve safety and security.

The Secure Stations Scheme is owned by the Department for Transport (DfT) and jointly managed and administered by the DfT and BTP. Designing Out Crime Officers (DOCO) within the BTP Designing Out Crime Unit (DOCU) work with operators to accredit stations. The accreditation lasts for two years.

The adjacent table outlines potential opportunities for creating safer stations.

Code of Practice Guidance

Department for Transport, Secure Stations Scheme

Code of Practice Guidance

Security In Design Of Stations (SIDOS) Guidance

Principle	Description
Visibility & Layout	• Visibility aids in reducing and deterring crime, providing opportunities to observe/be observed, and informing passenger perceptions of a station. - The built environment should be conductive to allowing maximum sightlines. This should be reflected in the overall design. • Lighting should be uniform in coverage and intensity, well-maintained, and of sufficient brightness to allow signage and information to be easily read.
Passenger Information and Signage	• Provide appropriate navigation and wayfinding signage which is accessible. Crime prevention advice and safeguarding organisations contact information should be provided. • Systems for information delivery should be working and communicating accurate and timely information. Passengers should also have the means to always call for assistance - such assistance should be relevant, timely, and accurate. • Station staff should be a visible, helpful, and reassuring presence. Staff should be discouraged from remaining in areas that are not accessible, or less visible to, station users.
Surveillance	• CCTV should be sited to maximise coverage and visability of the station. CCTV systems should be registered with the Information Comissioner's Office. • Opportunities for informal surveillance should be sought through using 'open' fencing and barriers, using maximised staff presence, and using transparent surfaces over opaque ones.
Station Management	• A security and safeguarding strategy with a statement of intent which confirms a commitment to setting and monitoring standards of security and safeguarding, and working with partner agencies within them. • A trained and aware presence at the station, including staff who can effectively deal with conflict and respond to incidents and engagements with community and volunteer groups. • Consideration of and participation with local organisation around safe journeys to/from the station (including cycling). • Having well-maintained facilities and secure storage for passenger property, such as vehicle parking, cycle storage, and left luggage.

Table 4.4: Table of potential station design and facilities and what they mean for safer stations

4.3 Crime Prevention Through Environmental Design

Crime Prevention Through Environmental Design (CPTED) is a sustainable security concept, based on the problem-solving approach that assesses environmental conditions and the opportunities they offer for crime or other undesirable behaviours.

The key concept of CPTED is:

Crime is more likely to occur where it can happen.

Making an environmental less conducive to criminal activity will reduce the likelihood of crimes being committed in that area.

CPTED attempts to reduce or eliminate these opportunities by using elements of the environment to control access; providing designs that enable a see and be seen philosophy; it also serves to define ownership and encourage maintenance and good housekeeping. CPTED is different to other security measures in that it focuses on the beneficial aspects of non-security design to provide security benefit instead of simply hardening.

CPTED is outlined in ISO 22341:2021 – Guidelines for crime prevention through environmental design.

The CPTED philosophy is well practised and many CPTED solutions appear logical and intuitive to designers. No single CPTED principle could result in a reduction of all crime; instead, they should be applied in conjunction with one another, based on a thorough analysis of the local context.

As the examples in the table overleaf show, CPTED encourages prevention through exploitation of the design and location.

Code of Practice Guidance

Department for Transport, Secure Stations Scheme

Code of Practice Guidance

Security In Design Of Stations (SIDOS) Guidance

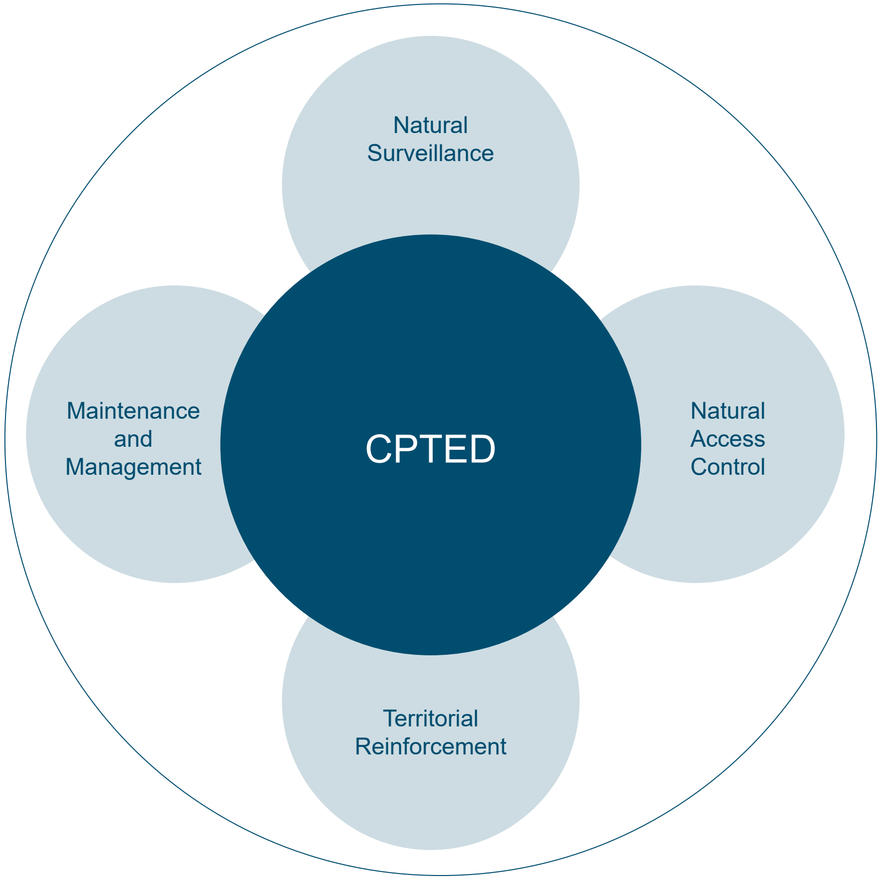


Figure 4.5: Diagram showing the CPTED principles

4.3 Crime Prevention Through Environmental Design

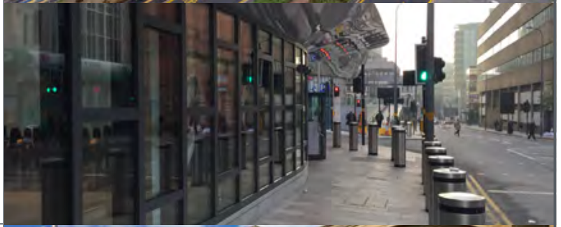
CPTED Principle	Description	Achieved By	Examples
Natural Surveilance	Develops opportunities to see from adjacencies or the station external areas onto the building, and potentially to see parking areas, deliveries, public realm and other various locations inside the station.	Windows, lighting, and the removal of obstructions can be placed to improve sight lines from within stations infrastructure.	
Natural Access Control	Creates both real and psychological barriers to entry and movement.	Physical elements to delay access such as: doors, fences, shrubs, and others. Use of adequate locks, doors, and window barriers. For public areas, use of non-physical or psychological barriers - these may appear in the form of signs, paving textures, nature strips, or anything that announces the integrity and uniqueness of an area.	
Territorial Reinforcement	Creates a sense of ownership, designing signals of who belongs in a place and what they are allowed to do. Additionally, it will emphasise the individuals that do not belong in that space.	Use of physical elements such as fences, pavement treatment, art, signs, landscaping to express ownership.	
Maintainance and Management	The maintenance and 'image' of an area can have a major impact on whether it becomes targeted. Maintenance and management need to be considered at the design stage, as the selection of materials and finishes impact on the types of maintenance regimes that can be sustained over time.	Use clear spatial definitions such as the subdivision of space into different degrees of public / semi-public / private areas. Raise standards and expectations of an area. Lighting, paint, signage, public realm etc. are kept in good order.	

Table 4.6: Examples of CPTED Principles and their descriptions

4.3.1 The 'Three Ds' Approach

CPTED involves the design of the physical space in the context of the normal and expected use of that space by the users as well as the predictable behaviour of people around the space. Conceptually, the CPTED principles are applied through the three Ds approach:

→ Designation.
→ Definition.
→ Design

The three Ds approach helps the user in determining the appropriateness of how a space is designed and used. By using the three Ds as a guide, spaces can be evaluated by asking the questions outlined previously.

Consideration of these questions may reveal areas that require changes or improvements. Once these questions have been considered, the information received may be used as a means of guiding decisions about the design / modification of the space so that the objectives of space utilisation as well as natural surveillance, natural access control, territorial reinforcement and maintenance and management can be better achieved. Refer also to the International CPTED Association (ICA).

'Three D' Spaces	Description
Designation	· What is the designated purpose of this space? · For what purpose was it originally intended? · How well does the space support its current use or its intended use? · Is there a conflict?
Definition	· How is space defined? · Is it clear who owns it? · Where are its borders? · Are there social or cultural definitions that affect how space is used? · Are legal or administrative rules clearly set out and reinforced in policy? · Are there signs? · Is there conflict or confusion between purpose and definition?
Design	· How well does the physical design support the intended function? · How well does the physical design support the desired or accepted behaviours? · Does the physical design conflict or impede the productive use of the space or the proper functioning of the intended activity? · Is there confusion or conflict in the way physical design is intended to control behaviour?

Table 4.7: A table with the 'Three D's' and their descriptions

4.4 Secured By Design

Secured by Design (SBD) is the official police security initiative with the specific aim to improve the security of buildings and their immediate surroundings to provide safe places to live, work, shop, and visit, not just rail stations. The scheme seeks to improve physical security by using products such as doors, windows and locks that meet SBD security requirements.

In addition, SBD includes proven crime prevention techniques and measures into the layout and landscaping of new developments – such as utilising CPTED principles. This is achieved by working closely with developers, project teams, Architects, and local authorities to incorporate police crime prevention standards from initial design through to construction and completion. This is delivered by specially trained Designing Out Crime Officers (DOCOs) within Police forces throughout the UK, who offer designing out crime advice free of charge.

SBD offers:

→ An SBD product-based accreditation scheme, 'the Police Preferred Specification' which provides a recognised standard for all security products that can deter and reduce crime.

→ Several authorative Design Guides to assist building design to incorporate security into developments and crime prevention and security advice. Whilst SBD is specific for commercial and domestic sites, (although some rail developments might be relevant for SBD commercial developments) its principles still represent best practice and reflects the established principles of designing out crime.

→ Guidance and SBD awards (for relevant sites) can be gained by working with SBD's trained national network of police personnel who specialise in designing out crime.

More information can be found on the SBD website securedbydesign.com. The website also contains a directory of all regional DOCOs.

For all railway related developments projects can contact the BTP Designing Out Crime Unit (DOCU) via Design-OutCrime@btp.police.uk

Image 4.8: Bristol Temple Meads

4.5 Protect Duty

In February of 2021 the Home Office consulted on new legislation known as the Protect Duty.

This consultation sought opinions from industry and members of the public on new legislation aimed primarily at public venues (such as shopping centres, sports venues and tourist attractions, large organisations (such as retail or entertainment chains) and public spaces (such as public parks, beaches and town squares).

The consultation seeks opinion on the notion that greater responsibility should be placed on facility operators and owners to protect those members of the public visiting their spaces.

At the time of publication the Protect Duty remains in the consultation phase and is not yet binding legislation. It is understood however, that the National Railway Security Programme (NRSP) will remain the governing programme for rail stations but where larger public venues, such as shopping centres and cinemas, are situated adjoining rail stations, the Protect Duty might also apply.

Image 4.9: Birmingham Grand Central - John Lewis outside shot

Image 4.10
Waterloo Ticket Gates

5

Security at Stations Design Guide Manual

Physical Security

Image 5.1
Birmingham New Street Station
Departure Board

5.1 Security Barriers

Security barriers are intended to stop or delay entry for the required time period, and to deter crime and intruders from the network. Physical security often takes the form of different types of barriers, which are intended to delay adversaries from reaching an objective. Physical barriers alone cannot be wholly effective without detection and response measures, but an effective system of security should start with one or more physical barriers to delay access.

Different types of barrier should be used in stations to segregate and protect passengers, staff and assets and may take the form of the following:

→ Walls and fences
→ Doors and gates
→ Balustrading and screens
→ Gate lines

Security barriers are intended to stop or delay entry for the required time period. As such, the performance criteria of any barrier should be considered carefully and defined as an output of the TVRA.

Key considerations for barriers include the following:

→ Location
→ Height
→ Security rating
→ Materiality

Barriers should provide effective protection to suit their purpose, but do so without feeling overly intimidating or obstructing to passengers. For example, the use of transparent glazed screening, of an appropriate height and rating, may be more conducive of a secure environment than an opaque wall of the same height and rating.

It is important to note that although stations are open to passage most of the time it is operationaly important to have the ability to shut them for whatever reason.

Image 5.2: Wood Lane Underground Station Glazed Screens

Image 5.3: Glasgow Station Front Doors

Image 5.4: Victoria Underground Station

5.2 Assets, Attention, Adversary

When determining what type of barrier should be designed, consideration should be given to the following:

5.2.1 Assets

The TVRA should identify which assets need to be protected. This assessment will consider the criticality of the asset and impact should it become attacked, damaged or destroyed. Some barriers might be required to protect just one specific asset, perhaps key building services equipment or the station control room, whereas other barriers might be intended to protect a larger group of assets or an area such as a station concourse or platform.

5.2.2 Attention

After identifying the asset or group of assets to protect, the TVRA should consider the type of attention that the asset requires protection against. This might result in providing a barrier intending to prevent trespass, theft, vandalism or sabotage, or a barrier intended to prevent an errant or hostile vehicle incursion. The purpose of any barrier should be clearly defined and designs developed in response to specific threat types and scenarios.

5.2.3 Adversary

The capability of an adversary requires due consideration. The TVRA will identify various credible threat scenarios, which might vary from a vandal, aspiring to spray graffiti on a station wall (armed with paint) or a saboteur aspiring to close down a major station (armed with powerful equipment).

The time for which a barrier is designed to resist the attacker will vary as will the complexity and financial cost of procuring, installing, and maintaining the barrier. These considerations should be proportionate to the adversary's conceivable attack methods, which should be set out in the TVRA.

5.3 Deter, Detect, Delay, Respond

When a physical security design response is being conceived, to a threat set out in the TVRA, the principles of deter, detect, delay and respond should be considered.

Deter: physical security measures should create the impression of a secure station environment, which will help to deter crime.

Detect: technological security measures will play a key role in detecting criminality but physical security measures also have a role to play - by providing clear lines of sight, minimising concealment opportunities and by providing adequate lighting, station staff can detect criminality swiftly.

Delay: physical security measures, barriers, delay the adversary to varying extents, depending on their performance criteria.

Respond: physical security measures should support a swift and efficient operational response. This might take the form of strategically placed access points such as doors and gates.

The principles of CPTED, which are discussed further in Section 4.3, should play an important role in the design of physical security barriers, as should more numerical performance criteria, set out in the project's TVRA and other industry standards, regulations and guidance.

Standards Reference

Enhanced security for doorsets and windows, PAS 24:2022

Security attack classifications, BS EN 1627-30

Security technical schedule 202, STS 202

Image 5.5: Victoria station concourse

5.4 Publicly Available Standards

There are a number of publicly available standards for physical security including PAS 24, STS202 and BS EN1627- 30.

The updated STS202 standard is a requirement for burglary resistance on a range of products, such as door sets, windows, curtain walling, etc. STS202 specifies the use of a range of attack tools that would ordinarily be used by "professional" criminals attempting to gain entry.

For "general" security the adoption of LPS 1175 (Loss Protection Standard) and LPS 1270 is recommended because this provides the most uniform approach and includes independent certification. LPS 1175 is focussed on doors/openings and LPS 1270 is associated with glass and glazing (windows, skylights etc). The application of LPS1175 is based on the time for an attacker to gain access through a barrier with a set of tools. The tool set is aligned between LPS1175 and LPS1270 for uniformity of approach. There is a further element in the use of LPS1270 in that it comes with differing designations, so the stated performance is 1270:X.Y.Z. X is the rating (time and toolset) to produce a small hole (big enough to insert tools like rods or loops), Y is the rating (time and toolset) to produce a larger hole (big enough to get a fist/arm through) and Z is the rating (time and toolset) to create a hole big enough for a human to enter through. For the Z hole there is a standard torso test piece which defines the opening size.

For LPS 1270 the design should take account of the lower delay designations in relation to any opening mechanisms (for example for openable windows). Where the glazing is simply fixed and not openable there is no issue but if the glazing is openable or a glass panel is close to an opening mechanism the design should consider that the attacker could create a small hole and use a tool to release the locking/closing system from the secure side. If the attacker enters within the delay time period the system fails the requirements. There is a consideration with LPS1270 in that it applies to the glass element of a door (vision panels to whole glazing) and windows – not to the framing or fixing of the frames. There is therefore the possibility of a combination of LPS1175 for the frames for windows and LPS1270 for the glass elements to create a fully secure line.

EN356 can also be used to set standards for glass. This standard uses a different approach and does not combine tools and time but uses instead a single tool and a number of blows to create an opening through which an attacker could gain access. Where EN356 is used the minimum grade of protection of glass considered applicable to intrusion resistance is P6B.

PAS 24 products are generally considered suitable to household and domestic security. While many PAS 24 certified products may provide additional security when compared to products not certified to the standards the level of protection is not as great as the lower levels of LPS 1175 or EN1627. Accordingly, PAS 24 products are not recommended for security at stations although, with asystem of layering of physical security there may be some justification for use at the fringe layers.

The Centre for Protection of National Infrastructure (CPNI) produce guides representing industry best practise in physical security. These range from guidance papers on specific items, such as fencing or doors, through to more general guidance on physical security measures which might respond to specific threat types or scenarios. As well as guides, CPNI maintain a library of approved products which meet the various accreditation standards mentioned. As with some of the CPNI guidance papers, some aspects of the library are restricted to vetted security professionals, but other aspects are publicly available on the CPNI website.

Standards Reference

Loss Prevention Certification Board's force test standard – LPS 1175

Loss Prevention Certification Board's force test standard – LPS 1270

Security technical schedule 202, STS 202

5.5 LPS 1175 and BS5234

5.5.1 LPS 1175

Loss Protection Standard (LPS) 1175 has recently been revised from Issue 7 to Issue 8. Issue 7 uses the SR designation while issue 8 uses the toolset and time delay combination as the designator. This creates some issues of interpretation:

- → The new, issue 8, designations are not aligned with matched standards such LPS 1270
- → There are few if any products that refer to the revised issue 8 designations
- → The market and supply chain is more familiar with the issue 7 designations

Accordingly, where designations are provided, where there are equivalent or matching designations, these will be given in the format of both standards, for example “C5 (SR3)”.

5.5.2 BS5234

BS 5234 Specification for performance requirements for strength and robustness including methods of test of partitions. BS 5234 is predominantly used for the specification of internal walls and partitions.

It is used in hotels, catering areas and back of house areas subject to extensive and heavier than normal use and is expressed in “duty” ratings. The duty ratings are associated with normal use in the environment and the durability of the wall or surface treatment.

Intruder delay is not a normal condition. Duty ratings, even at the high end of the options (Heavy and Severe) do not equate to any level of intrusion resistance.

No BS 5234 ratings are suitable for use as intruder delay measures – however if surfaces need to be duty rated in accordance with BS 5234 then additional layers to this standard can be applied to the security wall structure.

	LPS1175	EN1627-30
Threat	Burglar, criminal terrorist, activist or protestor	Burglar
Tool Set	Wider range of more powerful tools 8 toolesets, 48 combinations	Fewer tools, less powerful tools, 6 toolsets
Treatment of glazing/noise	Noise permitted. Attacking glass allowed at all levels	Limited noise permitted- stealth. Avoid attacking glass due to noise
Product Scope	Attacking physical aspects of product & electrics/electronic components	Attacking physical aspects of product
Attack Ready	Rated in all lock conditions e.g. day or night	Rated with all locks engaged e.g. night mode
Certification	Third party tested & certified annual surveillance audits. Centralised verification database	Self certification No surveillance audits No centralised verification database
Revision	2019	2011

Table 5.6: A table indicating the key differences between LPS1175 and EN1627-30

5.6 Layering

Layering of physical security lines is a tactic to both enhance the overall protection of a critical asset and reduce the delay and massing of each layer.

No critical asset should normally be immediately adjacent to or accessible from fully publicly accessible locations. If this cannot be avoided, the physical protection against attack would need to account for the ease of access.

In a layered solution, the external initial layer, for example, between the public concourse and the initial back of house areas, could reasonably be BS 5234 Severe duty walls with PAS 24 doorsets. The introduction of lobbies might also help to create a layered security arrangement but in doing this, consideration should be given to how accessible and inclusive the resultant arrangement might end up.

Progressing further into what is now private space, there could be several doors and walls to navigate, comprising levels at, for example LPS 1175 (Issue 8) B2.

Access to secure comms rooms and electrical plant could be additionally bounded by walls and doors at, for example, C2 with any highly critical spaces formed with a higher rating.

The station control room and server room (and other critical operational spaces) should be afforded enhanced protection to at least, LPS 1175 C5 and additional physical measures such as air locked entry doors should be considered based on risk assessment.

In summary, the physical protection measures of any given space will depend on:

1. The security value of the space or asset
2. Where the space is in relation to the adversarial attack pathways
3. How many layers are in place to delay the progress of the attacker.
4. How quickly a response/intervention can be deployed to stop the progress of the attacker.

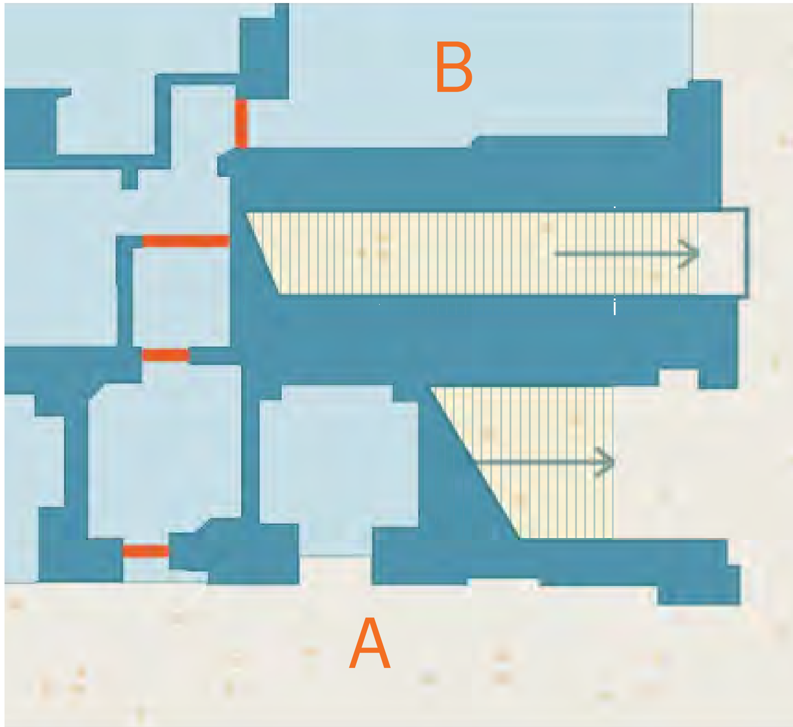


Figure 5.7: Layering plan illustration

Key

—	Barriers
A	Front of House
B	Area/Asset being protected

5.7 Walls and Floors

There are many different types of walls and floor systems that are used within station buildings, and together these elements play an important role in protecting occupants and assets from the effects of security threats. Walls and floors should be designed to meet the threats identified within a TVRA, which might include vandalism, an attack involving explosives, impact and / or fire.

When designing structural framing, walls and floors should incorporate physical security requirements from the outset as this will help to create efficiencies in the design process as well create integrated design solutions. Where it is necessary to retrofit or adapt existing structures, physical security needs should form a central part of the security risk review process for the enhancements - specific advice from the Network Rail Security Team should be sought, should the requirements of the TVRA be unclear.

In some instances, walls and floors may be required to resist onerous threat types such as ballistic attack or fire as a weapon type attacks. Where this is defined in the TVRA, projects should seek advice from a security professional on designing mitigations to these complex considerations.

Image 5.8: Security rated partitioning systems might suit other contexts.

Image 5.9: Masonry construction may be suited to some threat scenarios.

Image 5.10: Specialist advice may be required, should ballistic threats be identified.

5.8 Doors

5.8.1 Doors Generally

The location, type and size of doors should be considered in response to the TVRA. During the design process doors should be designated with a secure side and an unsecure side. This is in relation to whatever asset is being protected and the direction of attack by an adversary seeking to reach the protected asset. The design of doors should consider accessibility and inclusivity - power assisted opening devices may be required for larger, heavier doors with higher prescribed security ratings.

5.8.2 Door Controllers

It should not be possible to open a door by attacking a door controller – the door controller should be protected by the physical layers it is associated with. It is good practise to distribute door controllers. Door controllers that are centralised will all fail at the same time if an event (fire, flood, mains fail etc) occurs to or in the same area.

Distributing doors controllers reduces the likelihood of wide scale system failures (doors may be designed to 'fail safe' or otherwise, depending on the scenario).

Door controllers should be located out of normal reach. Door controllers should be located close to the door(s) they are controlling, however, door controllers should be located outside of the swing arc of the door and should be serviceable without having to fully close off access to the relevant door.

5.8.3 Security Doors

Security doors are normally purchased as door sets which incorporate the door, frame, locks, hinges, hinge bolts and other attributes. Security doors are typically tested and a certificate of successful passing the testing is issued. The certificate is predicated on the whole door set – any changes or modifications to the door may void or invalidate the test certificate and may result in a reduction of security.

5.8.4 Fire Doors

Fire doors tend to be robust in nature and while tested and certified for fire purposes they are not necessarily tested for security. Locks can therefore be specified for fire doors and should therefore be selected in accordance with this guidance – use locks where a handle acts directly on the bolting mechanism in the direction of escape.

Image 5.11: Security door examples

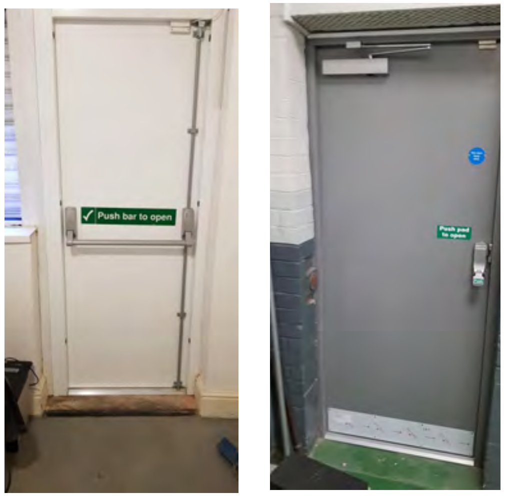


Image 5.12: Fire door examples

Physical Security

5.9 Mechanical Keys

In most mechanical and electromechanical locks the locking and bolting functions are combined. They are, however, distinctly different functions within the same device. The bolting component is the element that holds the door shut within the frame. The locking component is the element that locks the bolting mechanism preventing it from being unbolted without authorisation. For a mechanical lock, turning the key unlocks the lock which allows the bolting mechanism to be withdrawn after which the door can be opened. When interfaced with electronic control systems (EACS (Electronic Access Control System), digital keypads etc) the lock is held locked using an electrical connection (usually a solenoid) which is controlled by the EACS, digital keypad etc.

The use of locking which combines mechanical only exit (in the direction of escape) with powered to unlock entry (in the direction of attack) is recommended. These systems will fail locked in the direction of attack if mains power is lost, thus preserving security but will allow exit under all circumstances to maintain life safety requirements.

Any locking/bolting mechanisms should include emergency entry override methods

(typically in the form of a physical key or push bar) for entry. Mechanical or mechatronic (keys with an electronic component) locking should be used where electronic systems are unnecessary.

For physical key systems the Station will need operational procedures for the control and management of keys and particularly for the return of keys after use.

For new key systems it is wise to provide the supplier (and any contractor within the supply chain) with clear instructions on key management during construction. Designers should consider:

- → How are keys controlled?
- → Could a contractor take/make or obtain a copy of a key to be retained after handover with authority?
- → How are keys managed while in possession of the supplier?
- → Does the supplier hold all the keys during construction?
- → It is good practise for the owner to be given all keys on delivery.
- → How does the supplier/contractor manage the keys during construction?
- → All keys should be uniquely individually identified
- → A secure database should be maintained, identifying which keys are for which locks

Consider key suiting. Master and Grand master systems are common – but if implemented all the master and grand master keys need to be accounted for. Good practise would have the higher level keys handed to the Client on delivery and better still directly from the supplier.

Image 5.13: Mechanical key examples

5.10 Mechatronic Keys

Mechatronic keys should be physically managed in the same way as mechanical keys.

Designers should avoid the use of single code locks due to the following:

- Single code locks become compromised if someone unauthorised learns the code.
- Where there is only one code and multiple users it is not difficult to observe the code or code pattern being used
- With a single code, locks tend to wear on the code keys. This reduces the number of entry combinations which have to be tested
- If the code is compromised there is significant effort in going to each lock to change the code.
- If a code is compromised, changing the code becomes time bound (i.e. it is important to change the code quickly if not immediately putting pressure on operational staff)

Systems that use multiple codes one for each user are better but still suffer from someone having to manage codes, adding codes for new members of staff and removing codes for staff that leave.

Where a code based system is deployed, an online system that can be managed centrally is typically better, from a management and control perspective.

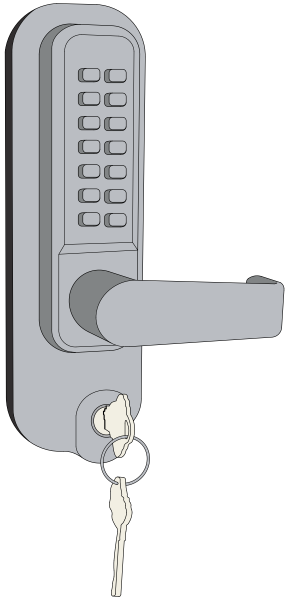


Figure 5.15: Alternative type of mechatronic key

Image 5.14: Mechatronic Keys in use

5.11 Relative Performance Specifications

The following are offered as indicative performance specifications for typical conditions and station elements. These are included as indicative only and should be confirmed as suitable by Network Rail on a case by case basis:

N.B Fire, blast resistance and other relevant performance criteria should be considered as well as those security criteria indicated.

Typical condition / Station element	Security Performance Requirement (Applicable to all constituent components: walls, doors, gates etc.)
Station control rooms	LPS 1175 SR3 or equivalent
Critical building service spaces	LPS 1175 SR3 or equivalent
Rooms where cash is stored, handled, or counted	LPS 1175 SR3 or equivalent
Station entrances (public)	LPS 1175 SR2 or equivalent
Front-of-house to back-of-house boundaries	LPS 1175 SR2 or equivalent
Retail units	Robust construction
Seating lounges	Robust construction
Public toilets	Robust construction
Station entrances (service and vehicles)	Varies, depending on context

Table 5.16: Table showing the relative performance specifications alongisde the station element

Image 5.17
Network Rail customer assistants

6

Security at Stations Design Guide

Technological Security

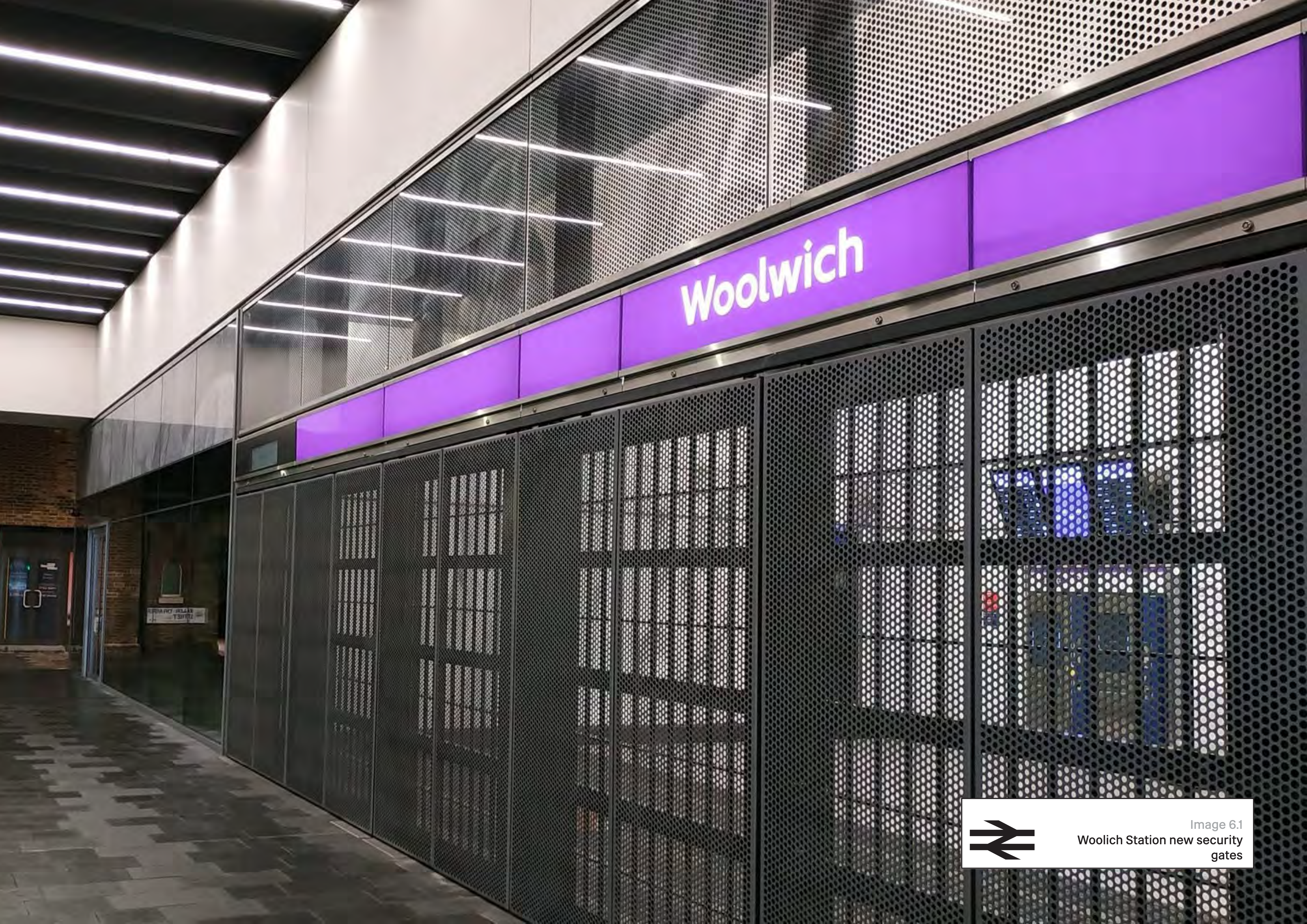


Image 6.1
Woolich Station new security gates

6.1 Technological Security Generally

6.1.1 Technological Security Generally

Technological security systems can provide a valuable means to detect a security event and raise the alarm in response to an event.

Perhaps the most critical technological security system is a station's CCTV system as this allows operations to be monitored and analysed remotely.

6.1.2 CCTV System Purpose

The purpose of the CCTV system should be established at design outset, in response to requirements set out in a TVRA and other Network Rail Standards.

Typically, the primary purpose will be for public safety and the prevention and detection of Crime. CCTV systems will have secondary purposes and functions, for example:

- Monitoring crowd movement
- Post incident analysis, learning, evidence and prosecution
- Monitoring fire events
- Control and situation awareness in extreme events
- Capturing statistical data for further analysis

6.1.3 Product Viability

Products and systems used in security need to be reliable and need to function consistently and persistently to the required specifications set out in the TVRA. Products selected should therefore be mature and tested, in real life scenarios and conditions for at least 12 months.

Refer also to National Cyber Security Centre guidance on the use of non-British technological security systems.

Refer to Section 9:
Section 9 includes guidance on technical integration of systems

Image 6.2: Kings cross platform

6.2 Purpose and Terminology

Closed Circuit TeleVision (CCTV) is a colloquial and genericised term that has been used for many years. Originally systems were closed, with no direct connection to other systems. Current systems are often based around computer systems and are more accurately termed 'Video Surveillance Systems' (VSS), partly because they are no longer closed circuit.

Video Surveillance Systems are common place in the UK and extensively used in all forms of transport, to such a point where there is almost an expectation that VSS/CCTV will be provided, proving coverage as defined in NR/L2/TEL/30135 and British Transport Police BTP CCTV Output requirements.

While not exclusively the case, older style systems are unusual. For the purposes of this guide the newer Internet Protocol (IP) based systems will be assumed. Under certain circumstances (for example legacy systems or systems with specific electrical or cyber resistant requirements) older style communication methods and system architecture may be appropriate.

In addition, there are hybrid designs which allow high definition cameras in conjunction with older style cabling systems (i.e. coaxial cables or unscreened twisted pair) connected as analogue signals (not IP protocols) to digital recorders.

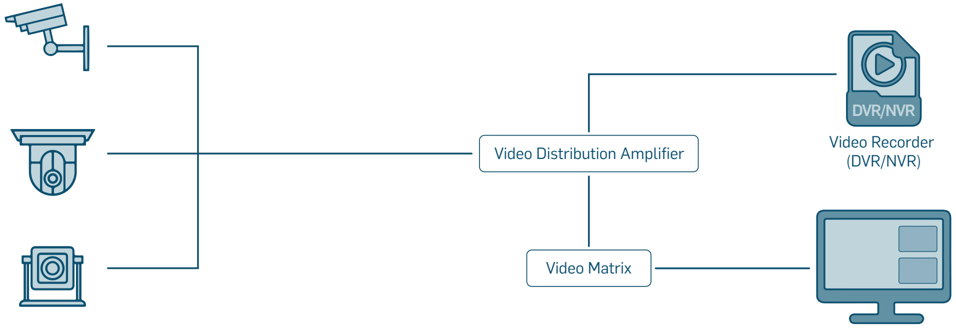


Figure 6.3: Typical CCTV (analogue)

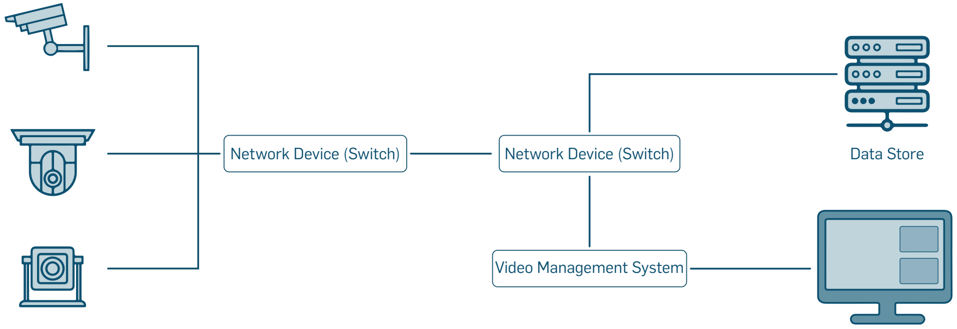


Figure 6.4: Typical IP Video Surveillance

6.3 CCTV Systems

6.3.1 Primary Design and Performance standards to be adopted for CCTV systems

For detailed requirements of system the following documents should be consulted:

NR/L2/TEL/ 30135 – Network Rail Video Level 2 Specification: Video Surveillance Systems

British Transport Police BTP CCTV Output requirements

BS EN 62676 - Video surveillance systems for use in security applications (Suite).

6.3.2 Cloud or On Premises

The current recommendation is for On Premises systems. Cloud based systems, including any component or function that is Cloud based may only be considered with specific permissions from Network Rail Security

6.3.3 Remote Systems

It is possible that smaller stations or parts of larger stations may operate as satellites to larger stations. In such cases the cameras are located at the smaller facility while the recording, command and control is located

elsewhere. Provided the communication path for these situations is managed from within the Network Rail domain this is an acceptable solution and is not the same as a Cloud based system.

6.3.4 Opportunities for product development

While core products and systems should be mature, field tested and proven there may be opportunites to trial new and emerging technologies in a station environment.

Provided there are commercial and operational benefits both to Network Rail and to a Vendor/System manufacturer, a busy station could be used as an environment to test and develop CCTV technologies, particularly in the Artificial Intelligence space.
A key element however is the separation of any test environment with the live operational systems such that the live systems cannot be affected by the test system/equipment.

6.3.5 Operator Requirements

CCTV systems should be designed to satisfy the requirements of the operator. In this context the “operator” is both the controlling/responsible body and the individuals who are using/operating the systems, noting that in the future some or all user functions could be replaced by computers/Artificial Intelligence(AI).

Figure 6.5:CCTV illustration

6.4 Resolution & Lenses

6.4.1 Resolution

Camera resolution is described through the use of pixels. There are numerous standards and representations of camera resolution: 720p, 1080p, 4K etc. are often quoted. There are also different ways of expressing the same values (i.e 2Mp, 5Mp, 12Mp etc.) together with different formats or aspect ratios (4:3, 16:9, 21:9 etc.)

It is the designer's responsibility to select the optimum camera parameters for the purpose of the camera, the view required and the needs of the operator/user of the camera information.

6.4.2 Lenses

Lenses are a critical component of any camera whether integrated with the camera or as a separate item.

Lenses should be specifically chosen to be suitable for the camera definition. The output from high resolution cameras may be adversely affected by lenses not specifically designed for the camera. Similarly lenses should be designed to work with infrared(IR) where IR lighting is used.

Varifocal lenses allow flexibility of both design and installation to accommodate changes in camera position and view. A general rule for varifocal lenses is that they should not be used at the extremities of their range.

Typically a varifocal lens should be selected that provides the designed image within the mid 60% of the available range. The design should not use the far distant 20% or the close range 20% of the overall range of the lens.

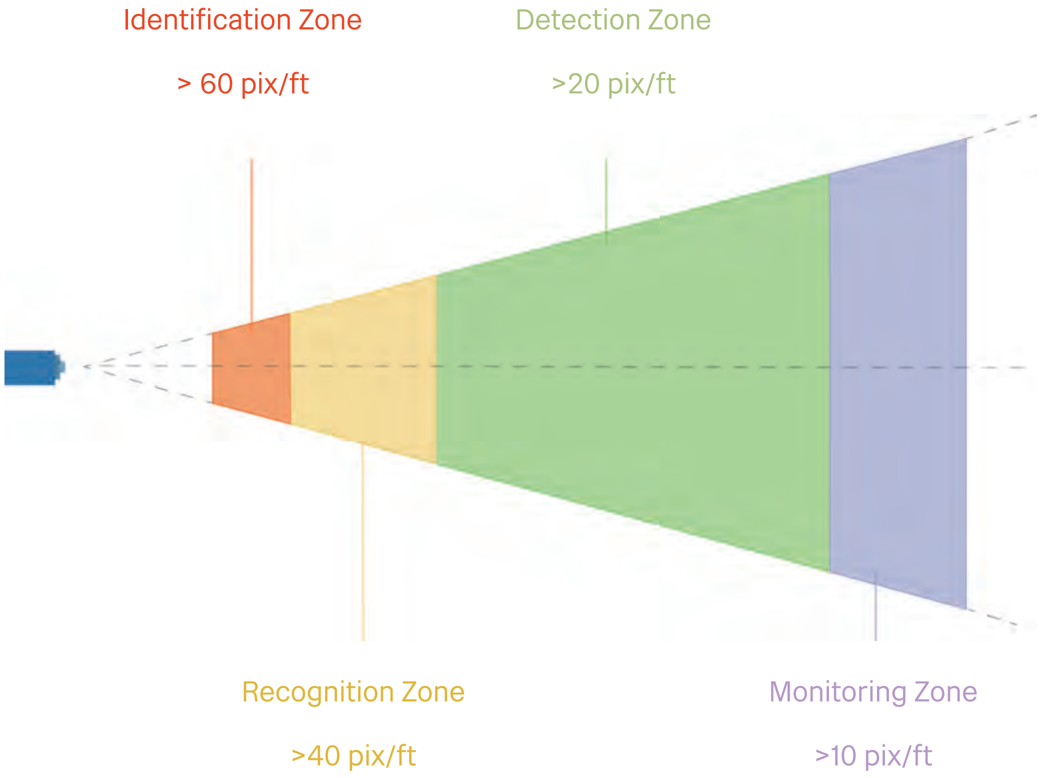


Figure 6.6: CCTV resolution diagram

Technological Security

6.5 CCTV Signage

The Data Protection Act (DPA) requires that people entering areas of surveillance are warned as they do so. Typically this is provided by signage. Signs should be clear and reasonably obvious and should meet the requirements of the Data Protection Act.

Signs should indicate the purpose of the system and provide the contact details of the operator of the system. Sizes and numbers of signs need to be sufficient to warn people they are entering an area of surveillance. Signs that are too small or too discrete or signs that blend too much into the background are to be avoided. Wayfinding and Directional signs should not block CCTV cameras.

While it is true that many people in the UK will be aware of CCTV cameras generally and might have an expectation of being under surveillance especially in a transport environment this is not the same for visitors and tourists. Signage should assume people do not know about CCTV cameras and are not aware of related legislation or their rights and should therefore be deployed to satisfy the purpose of warning people which might in turn positively enforce the feeling of a secure station.

NR Guidance Suite Reference

Network Rail Video Level 2 Specification: Video Surveillance Systems - NR/L2TEL/30135

Network Rail Visual Surveillance Systems Strategy

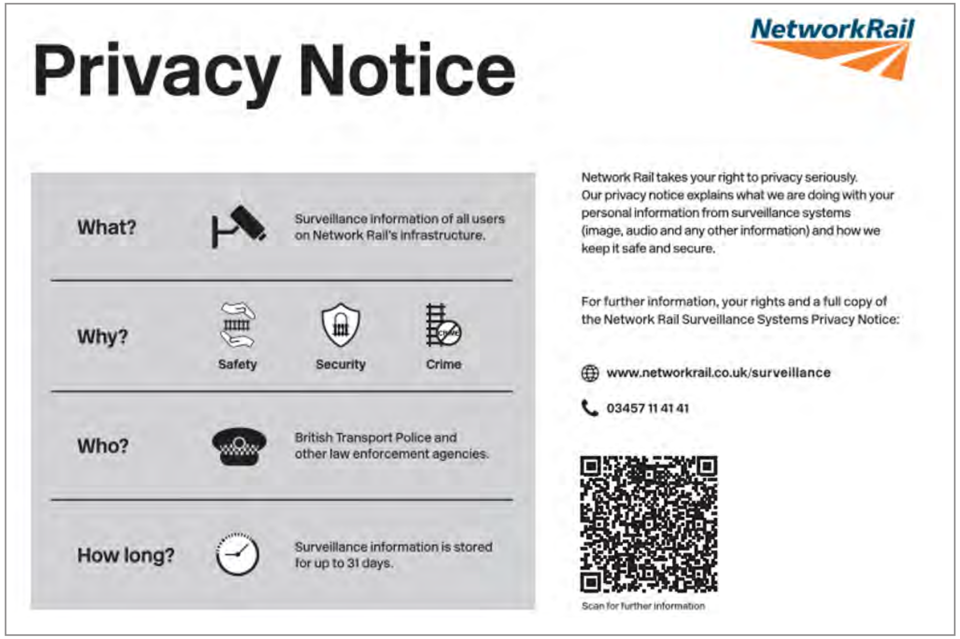
Standards Reference

Video surveillance systems for use in security applications (Suite)

BS EN 62676

Code of Practice Guidance

British Transport Police, CCTV Output requirements



Privacy Notice

NetworkRail

What? Surveillance information of all users on Network Rail's infrastructure.

Why? Safety Security Crime

Who? British Transport Police and other law enforcement agencies.

How long? Surveillance information is stored for up to 31 days.

Network Rail takes your right to privacy seriously. Our privacy notice explains what we are doing with your personal information from surveillance systems (image, audio and any other information) and how we keep it safe and secure.

For further information, your rights and a full copy of the Network Rail Surveillance Systems Privacy Notice:

www.networkrail.co.uk/surveillance

☎ 03457 11 41 41

Scan for further information

Image 6.7: Network Rail privacy notice sign

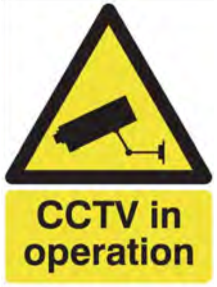


Figure 6.8: Typical CCTV warning sign

6.6 CCTV Review and Mounting

6.6.1 Pre and post alarm review

To assist operators in the verification of an alarm events, systems should provide pre alarm recording. The pre alarm recording needs to be long enough to see what occurred in the run up to the alarm but not so long as it detracts from the response to the alarm. This is typically 3 to 5 seconds. If the pre alarm reply is too long, then too much time will be expended in reviewing the information as opposed to handling the alarm.

6.6.2 Post Incident Playback

Facilities should be provided such that footage can be viewed by appropriate stakeholders (Network Rail or the Station Facilities Operator (SFO), British Transport Police (BTP) or the relevant Train Operating Company (TOC). These facilities should provide privacy to those reviewing footage which might include providing acoustically treated walls and blinds to windows and doors.

6.6.3 Mounting

Cameras used specifically for security need to be mounted so they provide stable images and do not move. In station environments there are multiple sources of movement including in response to train movements, environmental effects (wind). In some situations (for example very high ceilings) cameras may need to be suspended to obtain the required view.

Camera mounts should be robust and rigid to make the output image stable. This is especially important for cameras with optical or digital zoom capabilities as any movement of the camera is magnified when zoomed to a target to a point where the resulting output can be unusable.

Systems (standalone products and internal camera features) exist that can provide electronic image stabilisation. These systems should only be used as a last resort solution where suitable stable mountings are not possible to achieve. Where required in the National Railway Security Programme (NRSP), tethers should be provided to CCTV equipment. This might typically be in stations falling in to Security Category A and B - refer also to Section 7.3.1 of this Design Guide.

Image 6.9: Examples of elegant CCTV mounting in London's King Cross

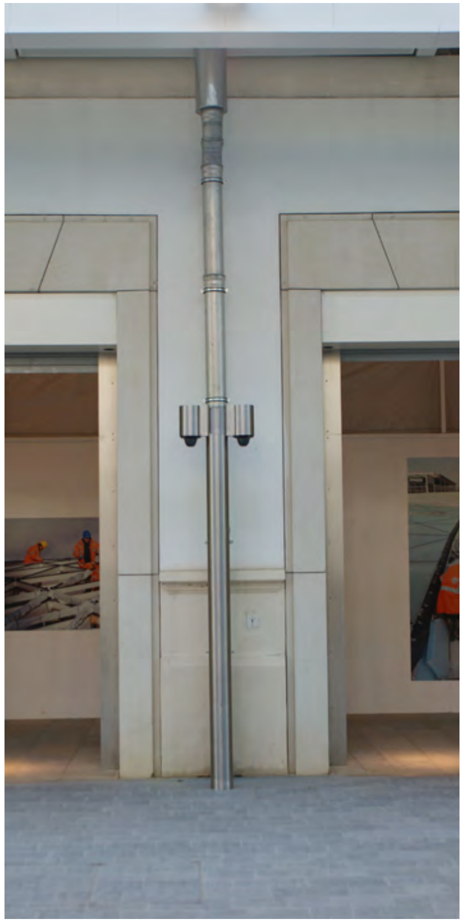


Image 6.10: Examples of elegant CCTV mounting in London's King Cross

6.7.1 Data Retention

Retention periods should be set in accordance with the system operator's GDPR/Data Protection Act compliance policy. Data should only be retained for as long as is necessary for the purpose of retaining the data. Often the default value for CCTV related data is 30/31 days, however this retention period may be excessive in certain situations, for certain cameras and may be inadequate for other locations/ cameras. The advice of this guide is to use 31 days as a base value and to discuss the retention for each camera with the system operator.

6.7.2 Data Storage

Data storage of information captured by the CCTV is critical for the post event forensic review of any incident. Data storage (including the data transmission paths) should be optimised for CCTV/video data.

Data storage should be resilient to hardware failures.

Data storage should be in a physically secure location. The location should be away from likely sources of damage from a critical event (security related or otherwise).Off site 3rd party storage of data may only be considered with agreements from the system operator/ owner. There are specific sensitivities about sending and storing security related information (including CCTV) to and on third party systems. There can also be costs to consider for adequate transmission paths for Cloud storage.

For smaller facilities it may be appropriate to store camera output at another NR premises/facility but this is subject to the capability of the communication channel, which should be discussed and agreed with NR before adopting this approach.

Data storage and CCTV control (and the communication path) should be resilient to mains electrical failure. Design of mains fail backups, including autonomy duration will depend on the existing electrical support systems.

The system should be designed to allow mass download of recorded data. This should be as fast as possible (hours not days) and should not impact normal operation (i.e. continued recording and continued use) of the system during the download. This is particularly important for larger systems and for systems installed in Category A and B premises, but also applies to systems which take in CCTV data from smaller stations.

Figure 6.11: Illustration of data storage

6.8 Artificial Intelligence

Cameras can act as the source for Analytics and Artificial Intelligence (AI) operations. To be effective, cameras should be specified and deployed to support analytics functions and AI. Standard analytics functions include (but are not limited to):

- → Left Item
- → Removed Item
- → Overcrowding
- → Trip Wire
- → Counting
- → Direction and counter direction of movement
- → Alarm Detection

More advanced detection which may be delivered through AI will include (but not limited to):

- → Violence
- → Pickpocketing
- → Body Language (unwilling accompaniment, coercion)
- → Physiological Biometric recognition Loitering
- → Pickpocketing
- → Loss or missing children /vulnerable people

True Artificial Intelligence is the development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making.

All systems should receive huge volumes of data and self learn, which is not the same process as being taught (by humans) what "good" looks like.

Critical to AI is the autonomous decision making process: the AI (computer) learns what "normal" looks like from data captured and identifies abnormal events. Over time the accuracy of what abnormal looks like is made more accurate and effective until a point where AI can be relied upon to report abnormal events and categorise the events according to the type of response required.

Figure 6.12: Illustration of monitoring a person over CCTV

6.9 Electronic Access Control

6.9.1 When To Consider Access Control

Electronic Access Control systems should be considered where the following is required:

- → Movement monitoring and historical recording
- → Immediacy of control, both granting and denying access
- → Compliance with Site standards
- → Dual authentication (e.g. Card and PIN or Card and Biometric)
- → Automated control (locking/unlocked / PIN enablement) on a timer schedule
- → Alarm monitoring and cause and effect switching

Typically this means that electronic access control should be provided to restricted access non-public areas. Systems that use a credential should be considered for electronic access control. Ideally the credential, in the form of a card, also provides a visual ID for staff and can incorporate a photograph of the holder, date information (such as expiry) and visual cues such as coloured objects indicating job role or rights of access. Where any existing electronic access control systems are in use, for example in an existing station being upgraded or in a development environment where assets with electronic access control are being retained, consideration should be given to compatibility between systems.

6.9.2 Access Control Credential - Type

A credential could be a card, token or fob but could equally be a personal biometric property. Biometrics for access control are categorised as physiological or behavioural. Physiological biometrics such as fingerprint, hand geometry and vein pattern are most commonly found in access control systems but other systems can be considered subject to reliability, security and maturity.

Credentials tend to be used in one of two modes:

Validation is the primary use of the credential. The credential is presented to the system, the system validates the credential and grants access if the rules for authorised access are passed. Verification is a process where the authorised use of the credential is verified using one or more additional process. This is frequently termed dual (can be more than two) factor authentication. The primary validation is the use of the credential and access is granted only after the verification process. Frequently the verification is based on an item of knowledge (such as a Personal Identification Number (PIN)). This is convenient for users but is less secure (it can be shared (deliberately or inadvertently)). Biometric property verification (for example card and fingerprint) is more secure, but the type of biometric should be selected to account for the types of job functions users have. For example, finger print based systems may not work very well where manual workers require frequent access. In this case hand geometry may provide better reliability of performance.

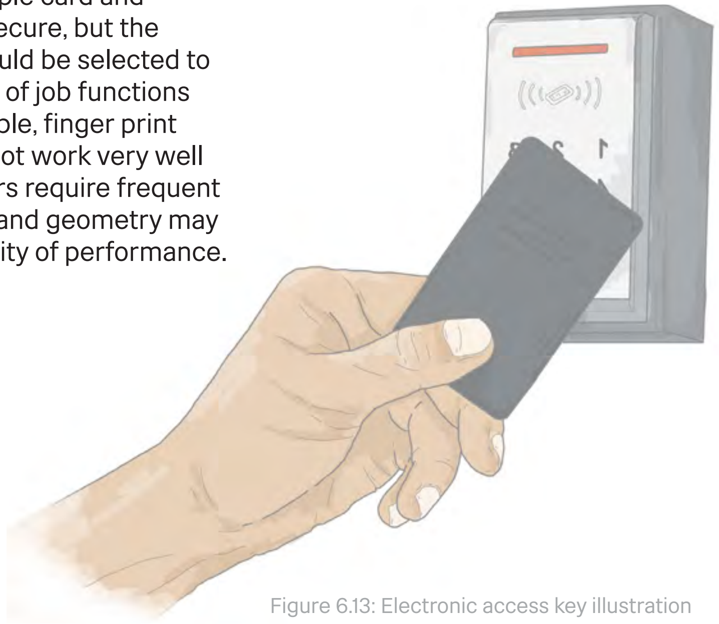


Figure 6.13: Electronic access key illustration

Technological Security

6.10 Help Points

Passenger help points offer an opportunity for passengers to call for assistance. These devices may be of particular importance at smaller, unstaffed stations where passengers may not have staff on hand to provide assistance.

Help points are useful to passengers in security scenarios, to raise the alarm when a security threat occurs. This might mean alerting Network Rail to suspicious activity, before a security event has taken place, flagging that an event is happening in real time or reporting an event back post occurrence.

Help points should be fitted with call buttons for both day-to-day assistance and emergency assistance. These should be linked back to appropriate call centres (local control rooms, regional control rooms or the emergency services) which should be discussed on a station by station basis.

Help points should be covered by CCTV and provided with signage such that these can be located easily, including by those with visual impairments.

Further design guidance on help points is provided in Network Rail Station Facilities and Amenities Design Guide ref. NR/GN/CIV/200/03.

Note also that help points should be accessible and inclusive, following guidance in the Network Rail Inclusive Design Guide ref. NR/GN/CIV/300/04.

NR Guidance Suite Reference

Network Rail Inclusive Design Guide
NR/GN/CIV/300/04

Network Rail Station Facilities and Amenities Design Guide
NR/GN/CIV/200/03

Help Point
CALLS FROM THIS HELP POINT MAY BE RECORDED AND MONITORED
Departures from Greenford
Last Updated: 12:31
Time
Destination
Platform
Expected
12:39 Terminates Here 2 On time
12:46 London Paddington 2 On time
13:10 Terminates Here 2 On time
13:16 London Paddington 2 On time
13:39 Terminates Here 2 On time
13:46 London Paddington 2 On time
Push below to speak to an adviser
Speak here
Emergency
Push
Information
Push

Image 6.14: A Help Point on a station platform

Technological Security

6.11 Lighting

Security lighting is not normally required for Network Rail Stations. It may however be required for specific assets within or adjacent to stations.

General and feature lighting and lighting for the purpose of enhanced natural surveillance and to support technical surveillance may be required. Lighting should not interfere with technical surveillance CCTV, either obscuring camera views, causing glare into or around cameras or creating illumination differentials (either in uniformity or colour) that adversely affect CCTV camera performance.

Lighting for security purposes (or multiple purposes where security is one) should be designed following the guidelines laid out in Institue of Lighting Professionals (ILP) Lighting Against Crime and in accordance with the principles of Secured by Design and CPTED.

Colour changing, feature and wall wash lighting should be carefully coordinated with the CCTV system both in relation to the camera itself and the targets and field of view of the camera.

Image 6.15: Lighting at the Elizabeth Line platform

Standards Reference
Lighting at Stations, RISS- 7702
Lighting Public Places, BS EN 12464

Image 6.16: Lighting at London Bridge Station

Image 6.17
Edinburgh Waverley Station

7

Security at Stations Design Guide Manual

Designing For Blast Resistance

7.1 Introduction

In this section, guidance is provided on how to design common station components to resist a terrorist blast event. The National Railway Security Programme requires this type of design consideration on all projects involving stations in Security Categories A and B. For stations in other categories, this guidance is not compulsory.

The following guidance is high level. Where any doubt exists as to the suitability of component, fixture or fitting to resist blast loads, the advice of a Register of Security Engineers and Specialists (RSES) principal member, qualified in blast effect should be taken .

Further guidance on the approach to be used when designing for blast, including blast analysis input data, can be found in Security In the Design Of Stations (SIDOS) guidance, as well as in publications by the Centre for Protection of National Infrastructure.

These guidance notes reflect best practice and are supported by physical testing and or engineering calculations. In some cases specific products are referenced as at the time of publication, these are known to be certified as meeting the required design criteria. The use of such tested, certified products might well be cheaper and more efficient than the use of bespoke arrangements and should be considered by designers when designing for blast is relevant. Much of the following guidance references laminated glass use, please note that whilst laminated glass is not a mandated requirement at all station security categories, it is considered good practice.

In all cases, the design guidance sketches provided should be read in conjunction with the design loading information included within the Appendix.

Standards Reference

National Railway Security Programme (NRSP)

Code of Practice Guidance

Security In the Design Of Stations (SIDOS) Guidance

Image 7.1: Glazed retail at London Bridge station

7.2 Glazed Canopy

Glazed canopies are shelters, provided to offer protection from weather. These are commonly positioned above walk ways, entrances and doors.

Glass in glazed canopies should be laminated with a minimum of 1.52 Polyvinyl Butyral (PVB) interlayer. This specification will meet the criteria set out in SIDOS as well as durability requirements set out in other regulations. The details opposite are indicative of the type of glazing supports and fixings required to produce an arrangement which complies with SIDOS guidance. Architectural changes can be made to this, providing these principles are followed.

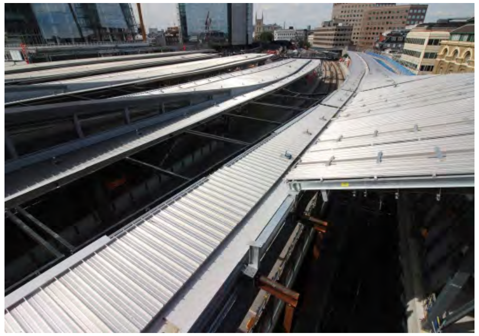


Image 7.2: Glazed canopy example

Key

1 Laminated glass: toughened (heat soaked) and laminated or heat strengthened and laminated, with Polyvinyl Butyral (PVB) interlayer.

2 Appropriate size universal “I” beam cut in half on the web, or universal “T”.

3 Illbruck SGT (Tremco Illbruck) Security Glazing Tape. Proper cleaning, surface preparation and priming of contact surfaces is vital, guidance should be sought from Illbruck.

4 Illbruck HIGT (Tremco Illbruck) High Impact Glazing Tape. designed for glass retention in bomb blast glazing applications.

5 Stitch welds

6 Mild steel block, drilled at 300 mm centres for counter sunk M10 fixing.

7 Counter sunk fixings

8 Mild steel plate (consider stainless steel alternative), appropriate size to form strong clamp

9 Mainframe fixing tie element if required.

10 Pin to design

11 Glass should be simply supported alongnminimum two edges

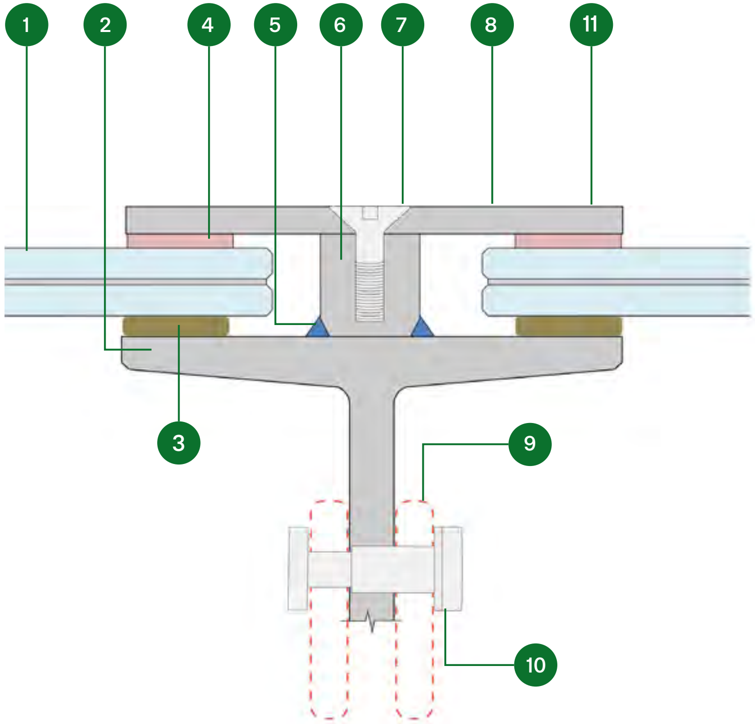


Figure 7.3: Indicative Sketches - Glazed canopy detail

7.3 Glazed Roof-Lights

There are two classes of roof lights:

→ Class 1 - Walked on for occasional maintenance. Designed to support the weight of people and equipment.

→ Class 2 - People are not intended to walk on the glass, but which are advised to be non-fragile to protect people where maintenance personnel walking adjacent to the glass rooflight could trip / fall onto the glass or fall onto the glass from access equipment.

→ Class 1 roof lights:

→ Be designed to withstand 2000-N/m2 UDL (Uniformly Distributed Load) and 2700-N point over a 50-mm x 50-mm impactor area (positioned worst case).

→ If the glass is to be walked upon, provide sufficient slip resistance to prevent slipping.

→ Class 1 rooflights should also meet the requirements of Class 2 rooflights.

Class 2 roof lights:

→ Have sufficient strength to support all anticipated loads, generally using an insulated double-glazed unit with monolithic toughened (heat-soaked) glass over laminated.

→ Have safe post-failure behaviour in the event of a glass breakage, utilising a minimum 1.52-mmPolyvinyl Butyral (PVB) interlayer.

→ Have sufficient rigidity to provide deflections under full load of less than L/75 where L equals the shorter dimension.

→ Have sufficient strength to withstand the static load test for injured person and rescuer as defined in Centre for Window and Cladding Technology Techincal Note 67 (CWCT TN 67).

A maintenance strategy should be considered such as surface anti slip treatments or glass obscuration. Surface anti slip treatments to the class can significantly lower the glass strength. A 5° pitch minimum helps to keep glass relatively clean and stop pooling.

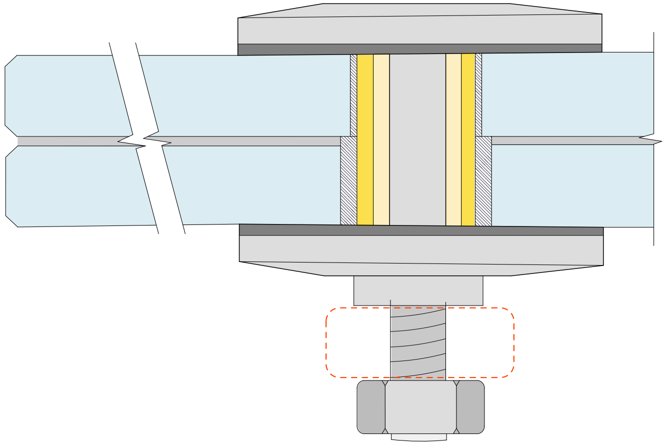


Figure 7.4: Indicative Sketches - Point fixing

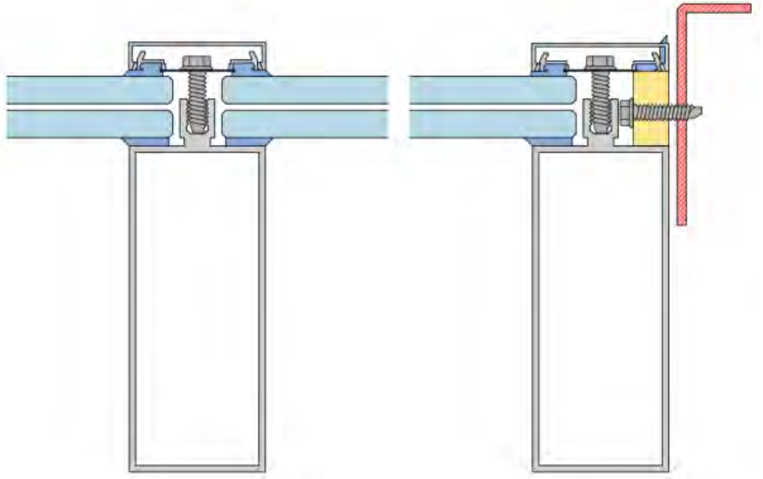


Figure 7.5: Indicative Sketches - Detail of glazed roof light support

7.4 Typical Glazed Shelters

Glazed shelters are structures provided to offer protection from weather. These are commonly used as smoking shelters, bus shelters and to provide covered seating in otherwise uncovered platforms.

Glass in glazed shelters should be laminated with a minimum of 1.52 Polyvinyl Butyral (PVB) interlayer. This specification will meet the criteria set out in SIDOS as well as durability requirements set out in other regulations.

Architectural or acoustic interlayers with a low to medium adhesion are acceptable (from Interlayer stiffness family 0 & 1 in accordance with EN 16612 and EN 16613). High adhesion or low plasticiser ES do not align with SIDOS guidance.

Image 7.6: Glazed shelter at station

Key

1	End arms secured to post via 4 M10 bolts and 2 M10 bolts to beam.
2	Roof glazing toughened (heat soaked laminate) if required
3	Circular hollow section (CHS) upright end posts or rectangular hollow section (RHS)
4	Mid arms secured to post via 4 M10 bolts
5	Neutral cure mastic joints between modules if required. Mastic should be compatible with interlayer
6	Minimum grade C30 concrete foundation to design. Local ground conditions should be considered.
7	Secured to post with spigot and 4 M10 bolts
8	Minimum 17.52mm laminated toughened with a 1.52mm Polyvinyl Butyral (PVB) interlayer
9	CHS or RHS, with glass clamp to design

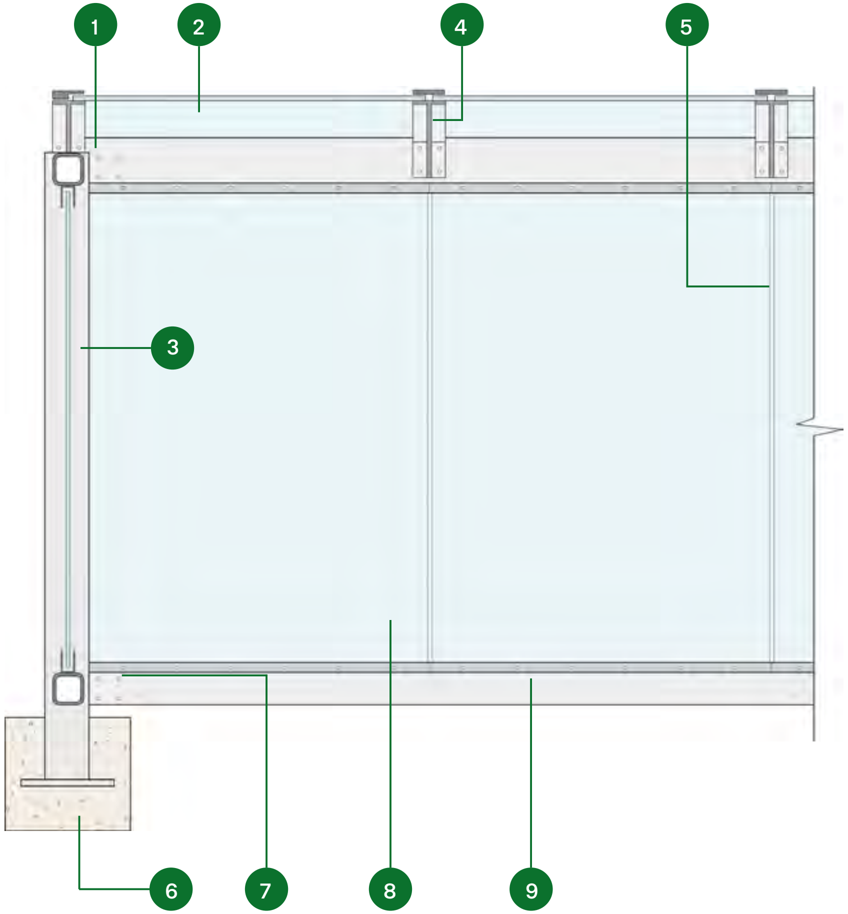


Figure 7.7: Indicative Sketches - Glazed Shelter

7.5 Typical Glazed Wall Linings

Glazed Wall Linings are sometimes used in station front of house environments. Typically, glazing is fixed back to a substrate which dissapates forces. Tested systems are available from: Lindner, Design Rationale, Sto, and MICAM Hedley Steel.

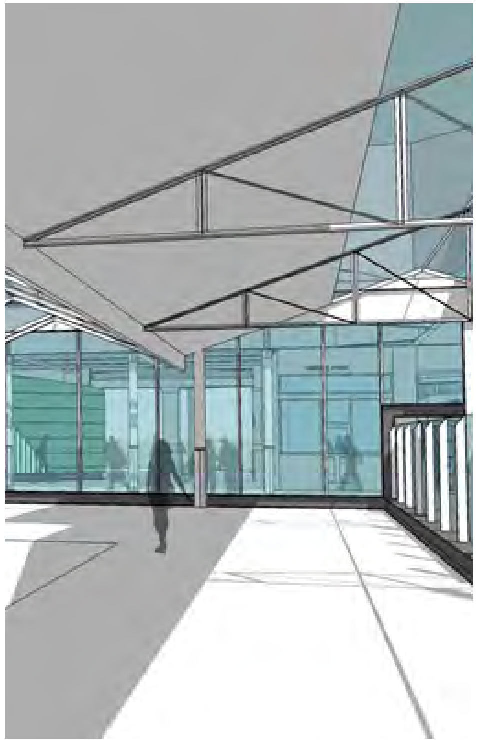


Image 7.8: CGI of glazed wall lining in station

1. Minimum severe duty (SD) or heavy duty (HD) classification drywall, or where applicable a security rated wall or shaft wall.
2. A suitable thickness of medium grade plywood. (18mm minimum expected unless technically justified to be different).N.B the use of plywood might not be acceptible from a fire engineering persective, advice should be sought from the project fire engineer.
3. One or more layers of a suitable thickness plasterboard or wallboard equivalent.
4. Suitable packing zone
5. Fixings
6. Adjustable anti jump stop in 3mm stainless or mild steel
7. Robust fixing to allow for loads to be transferred to substrate and still allow for panel replacement, joint alignment and architectural detail
8. Minimum 6mm x 40mm bite SIKA SG 400 or Dow 993
9. Appropriate thickness toughened (heat soaked) laminate. Glass thickness (and interlayers) to be designed for BS EN service loads by an approved specialist

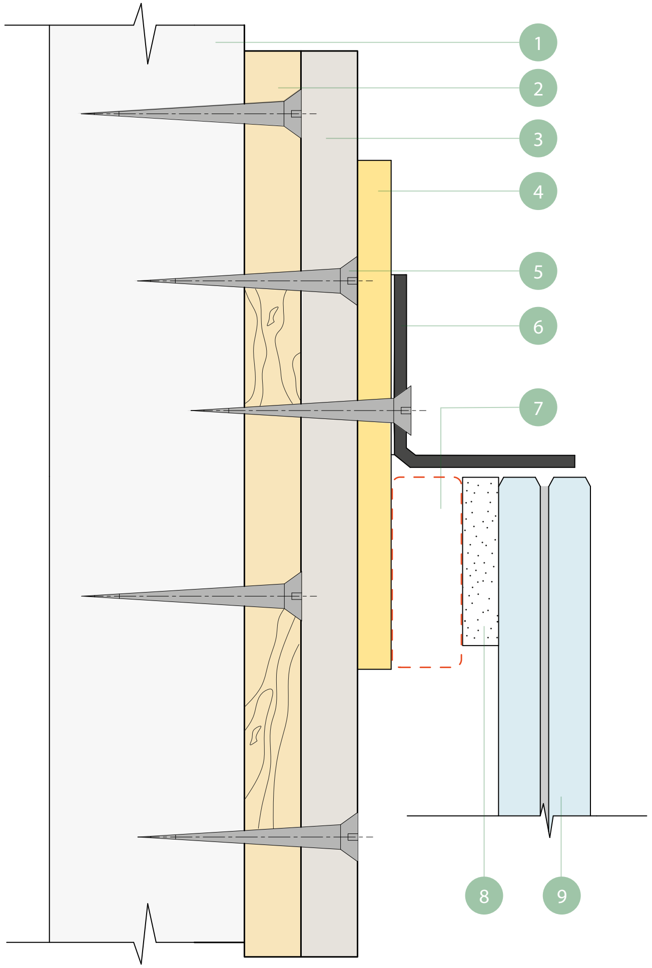


Image 7.9: Indicative Sketches - Glazed wall lining

Designing For Blast Resistance

7.6 Glazed Balustrades Up To 1.8m Tall

Glazed Balustrades are typically provided to staircases, terraces, or mezzanines. Their purpose is to protect a drop, acting as a barrier on the level.

There are currently two blast-tested, cantilevered, dry-clamped balustrade systems that comply with SIDOS guidance: Q Railing 3kN and Pure Vista BLASTguard systems. Manufacturers are advised to authorise the installers and certify the installation.

An alternative to a blast tested product is to use a BS 6262 clamp solution. In all cases, supporting engineer calculations are advised.

There are two load cases for the balustrade service:

→ Balustrade protecting a drop.

→ Balustrade not protecting a drop.

The correct service loads should be used. The use of clamp-clip balustrade systems is not recommended.

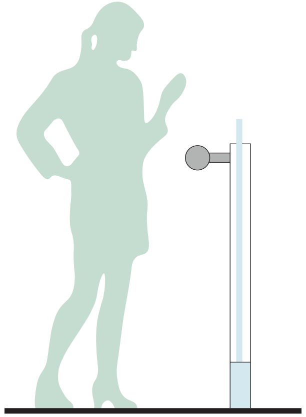


Figure 7.10 Indicative Sketches - Glazedbalustrade human scale

Image 7.11: Balustrade at Waterloo

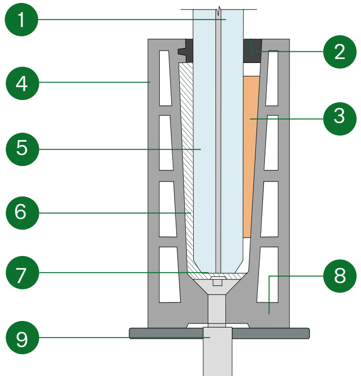


Figure 7.12: Pure Vista Blast Guard System

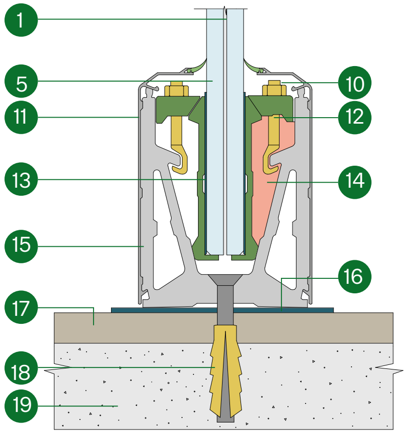


Figure 7.13: Q Railing Easy Glass Top Pro Mount3kN

1. 1.52mm Polyvinyl Butyral (PVB) interlayer
2. EPDM (Ethylene Propylene Diene Monomer rubber) gasket.
3. Blast rated PAF fixing liner (single side only) positioned as detailed on “blast rated detail”.
4. Blast rated3kN base channel, secured to substrate.
5. Minimum 25.5mm toughened laminated glass to withstand design load.
6. Blast rated fixing inlay (single side only).
7. M12 x 40 @ 20mm centres, DIN 7991.
8. Aluminium or galvanised levelling shims, max 5mm thick.
9. Anchor Fischer M12 RG18 x 125 to engineers design.
10. PureVista Mega Grip clamp bolts.
11. PureVista clip-on cover and glazing gasket.
12. PureVista Mega Grip glass clamps, equally spaced minimum 4 per m run.
13. PureVista Mega Grip clamp bar, predrilled for anchor bolts.
14. Two-part resin injected into wedges on one side post dry installation.
15. PureVista Mega Grip 3kN base channel for 25-33mm glass.
16. Aluminium or galvanised levelling shims, max 5mm thick.
17. Typical floor tile.
18. M12 bolts, gr8.8/A2-70, 200mm spacing to predrilled locations.
19. Typical substrate, eg. screen over concrete.

7.7 Glazed Ticket Barriers Over 1.8m Tall

Glazed Ticket Barriers are when glazing is incorporated in gate lines.

All design blast loads act in positive and negative directions. The glass should be toughened and laminated.

Gate lines can differ in height and size. Gate lines at stations are typically designed to be waist height or higher to provide a security barrier to restricted areas or behind paid lines. A ‘Q Railing Easy Glass Pro F Top Mount 3kN’ mount system is used on the typical glazed ticket barrier.

1. Minimum 2x glass thickness to edge of hole through glass
2. Spreader plate, minimum diameter = glass hole diameter + 30 mm
3. 1mm incompressible or 2mm compressible gasket
4. 3mm nylon or similar bush
5. Spreader plate fixed to structure
6. Minimum 1.52mm Polyvinyl Butyral (PVB) interlayer

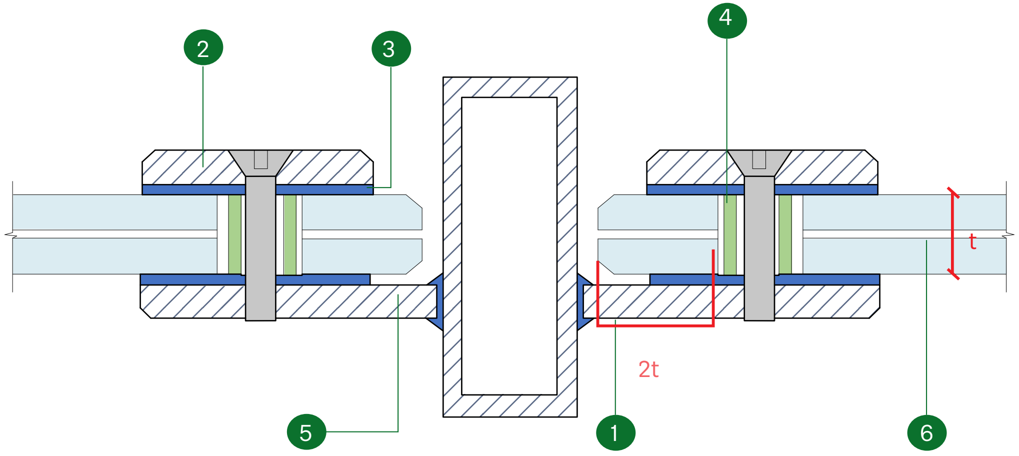


Figure 7.15: Indicative Sketch - Glazed ticket barriers detail

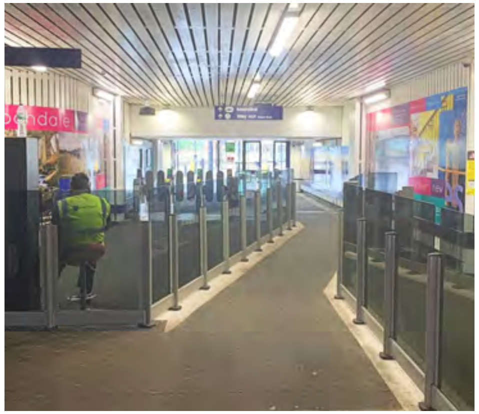


Image 7.14: Glazed ticket barriers used in station

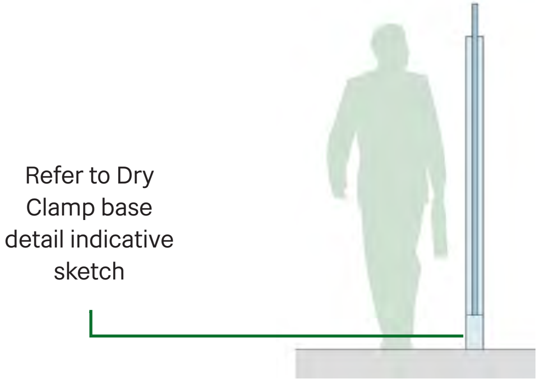


Figure 7.16: Indicative Sketch - Human scale next to tall glazed ticket barrier

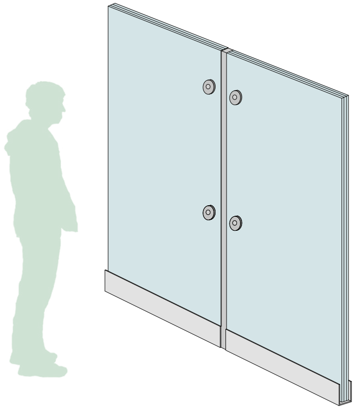


Figure 7.17: Indicative Sketch - Human scale next to tall glazed ticket barrier

Designing For Blast Resistance

7.8 Glazed Components Within Escalators or Travelators

New escalators / travelators should incorporate a laminated glazing component.

Normally the existing design of these products restrict the glass thickness to either 10mm or 12mm. Use the maximum thickness permissible with a minimum of 0.76-mm Polyvinyl Butyral (PVB) interlayer in conjunction with toughened glass.

For refurbishment projects, the project team should liaise with the Network Rail Security team for further guidance

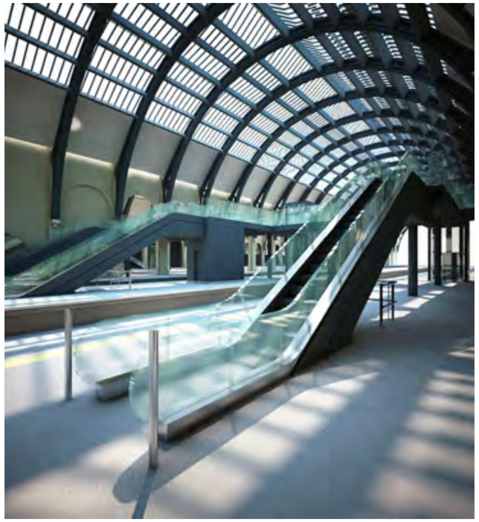
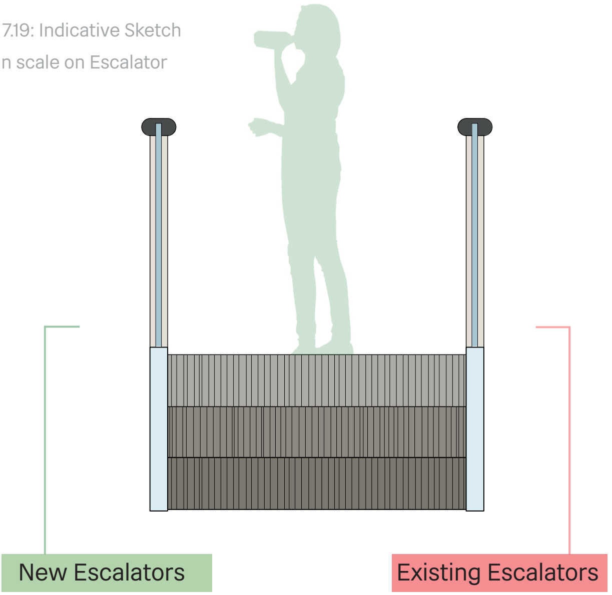


Image 7.18: King's Cross station glazed escalators

Figure 7.19: Indicative Sketch -Human scale on Escalator



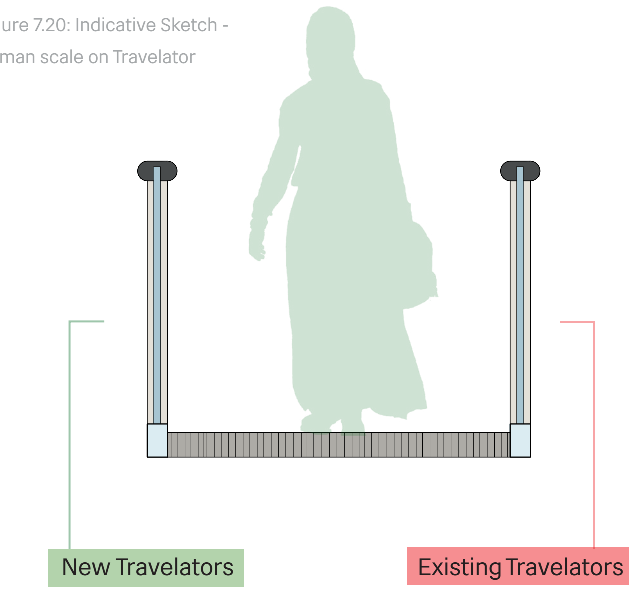
New Escalators

New escalators should use 11.76mm toughened laminate or preferably 12.76mm toughened laminate

Existing Escalators

Minimum 100µm ASF (GGF certified Anti Shatter Film) installed to inner surface according to manufacturer's instructions. Daylight film, inspect by a qualified person after 5 years, then every 2 years, replace if necessary. Allow for a maximum 10 year life before replacement is required

Figure 7.20: Indicative Sketch - Human scale on Travelator



New Travelators

New escalators should use 11.76mm toughened laminate or preferably 12.76mm toughened laminate

Existing Travelators

Minimum 100µm ASF (GGF certified Anti Shatter Film) installed to inner surface according to manufacturer's instructions. Daylight film, inspect by a qualified person after 5 years, then every 2 years, replace if necessary. Allow for a maximum 10 year life before replacement is required

7.9 Glazed Elements to Lifts

Glazing in station lifts should incorporate a laminated glazing component. Normally the existing lift design restricts the glass thickness which should be maximised to provide the best blast protection.
For all 4-side supported side systems, use a minimum of 21.52-mm toughened and laminated.

The minimum thickness of framed door elements is 13.52-mm toughened and laminated, cover minimum 12-mm, preferably 25-mm.

For all point fixed glazed systems, use 25.52-mm toughened and laminated. Note: the aim of the blast protection is to provide protection to persons inside a lift from a device on the concourse and to help limit the projection of debris into the concourse should a device be located within the lift car.

All glazing elements are to be checked against G085 subsurface glazing if appropriate.

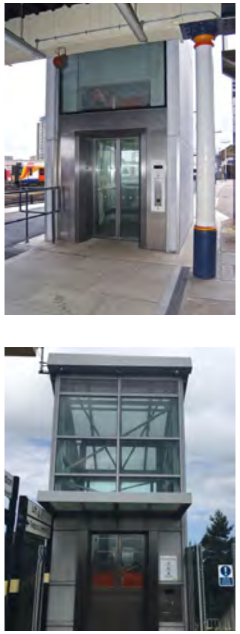
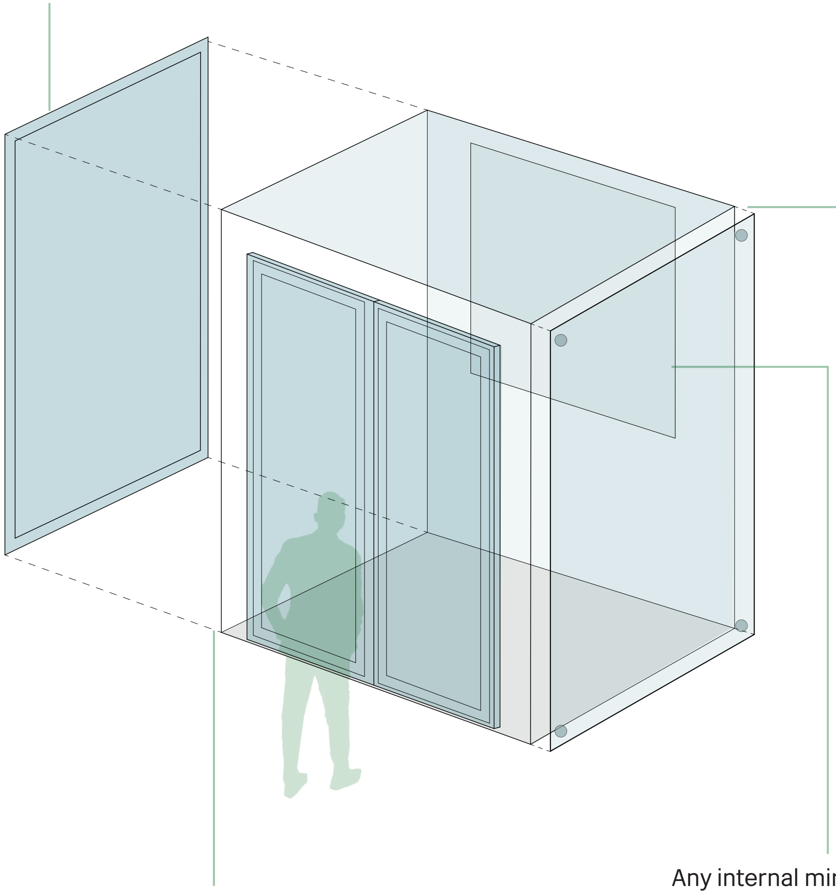


Image 7.21: Glazed lift examples at Network Rail stations



Glazing supported on 4 sides

Suitably designed corner protection will be expected

Any internal mirrors have a safety film and are robustly secured (i.e bonded, multiple fixings, or suitable framing).

Example of a point fixing

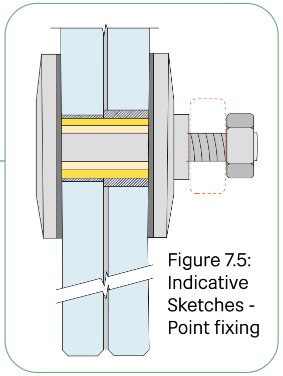


Figure 7.5: Indicative Sketches - Point fixing

Publicly available CPNI 2013 point fixing detail is available, which provides alternatives and options

Figure 7.22: Indicative Sketch - Glazed Elevator

Designing For Blast Resistance

7.10 Glazed Doors

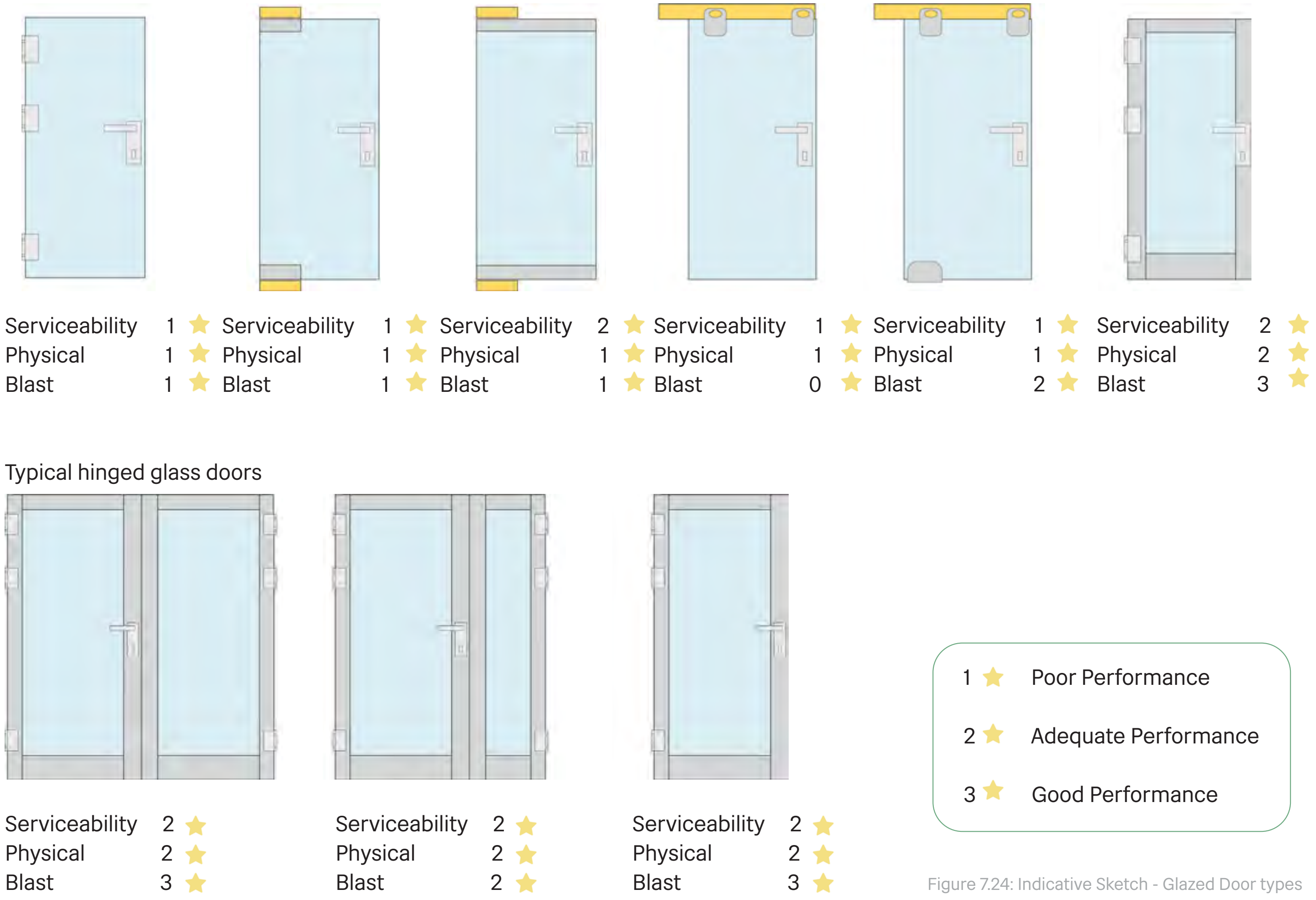
Glazed doors should not be specified if there is a fire requirement.

Glazed doors should only be specified if their short comings are fully understood. In many locations, solid doors are more appropriate.

Vision panels within conventional solid doors should utilise laminated glazing. Monolithic fire glass is not permitted.

All toughened glass should be laminated with a minimum of 1.52-mm Polyvinyl Butyral (PVB) interlayer.

Image 7.23: Glazed door at station



Typical glass door variation

Serviceability	1 ★	Serviceability	1 ★	Serviceability	2 ★	Serviceability	1 ★	Serviceability	1 ★	Serviceability	2 ★
Physical	1 ★	Physical	1 ★	Physical	1 ★	Physical	1 ★	Physical	1 ★	Physical	2 ★
Blast	1 ★	Blast	1 ★	Blast	1 ★	Blast	0 ★	Blast	2 ★	Blast	3 ★

Typical hinged glass doors

Serviceability	2 ★	Serviceability	2 ★	Serviceability	2 ★
Physical	2 ★	Physical	2 ★	Physical	2 ★
Blast	3 ★	Blast	2 ★	Blast	3 ★

1 ★	Poor Performance
2 ★	Adequate Performance
3 ★	Good Performance

Figure 7.24: Indicative Sketch - Glazed Door types

7.11 Internal Retail Glazing

In recognition of the difficulties in resisting the threats described in annex G of SIDOS it is recommended that retail glazing is designed to resist an ISO 16933 EXV 19 blast load with a category D (very low hazard) performance.

The preferred approach is to use a fully blast tested product to ISO 16933 at EXV 19 as a minimum, such as Schueco FW 80+XR. The product should be installed and supported as per the blast test details and manufactured and installed by an approved contractor (in the case of Schueco a Sabre approved contractor). The ability for the glass to withstand serviceability loads should be checked.

If a bespoke system such as a single spanning solution is desired then dynamic blast calculations are required from a competent blast consultant (such as an Register of Security Engineers and Specialists (RSES) member). The costs associated with these calculations can be relatively high and take a significant length of time.

Care should be taken on internal layout to avoid hazardous items being placed in front of the glass.

Door weights should be checked and power assited opening devices installed where neccessary.

1. Suitable laminated glass to withstand the blast load and the serviceability loads. The glass can be single or double glazed depending upon requirements. Under the blast loading the glass should be classified as a very low hazard failure (category D) or better in accordance with ISO 16933. Low hazard (category E) might be accepted in certain situations if approved by NR.
2. Break pressed aluminium cladding to architectural design minimum of 3 mm thickness for compliance to agreed SIDOS blast load.
3. Signage should be correctly designed for blast
4. Depending upon which system is chosen the doors should be compatible with the system and of the best possible blast rating. Glass should be laminated and framed to all four sides.
5. Locks to be appropriately selected for fire and security considerations. Locks above 2m from Ffl should be avoided.
6. Appropriate manifestation should be applied

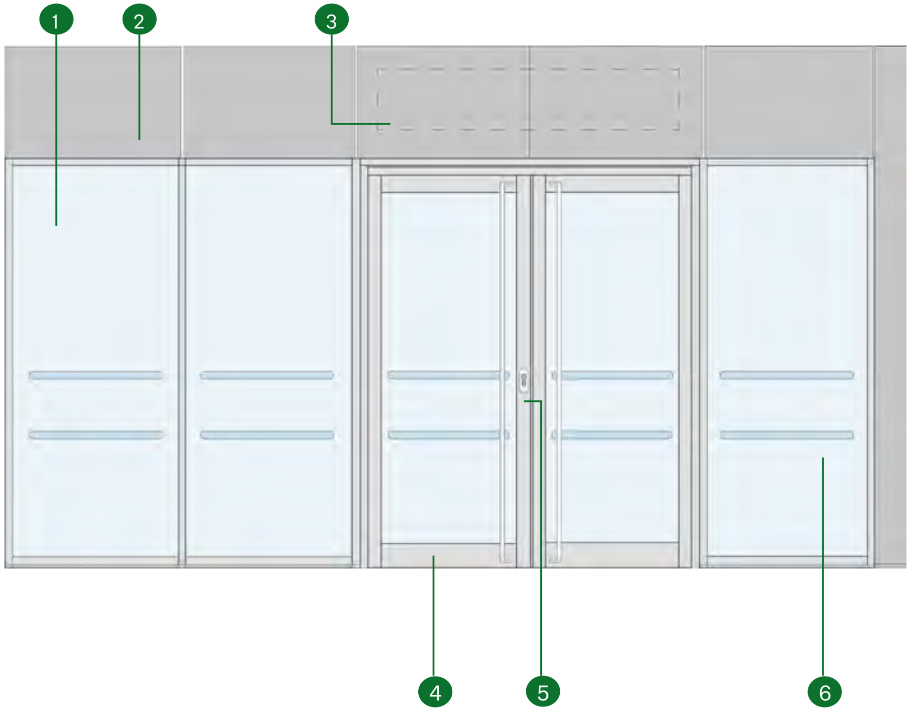


Figure 7.25: Indicative Sketch - Retail glazing

7.12 Solid Wall Linings

Wall linings of this type are used to enhance the appearance and robustness of both new and existing substrate walls. The suitability of the substrate wall should be assessed separately to resist loading.

Image 7.26: Solid wall linings at Birmingham new street station

1. Good quality plywood of the required thickness
2. Plasterboard or wallboard of the required thickness
3. 5mm packing zone
4. Adjustable top stop
5. Approved drywall lining material, resilient, non fragmenting with required fire rating.
6. Robust fixing to allow for loads to be transferred to substrate, but still allow for panel replacement and joint alignment
7. Minimum Severe Duty (SD) or Heavy Duty (HD) classification drywall or shaft wall

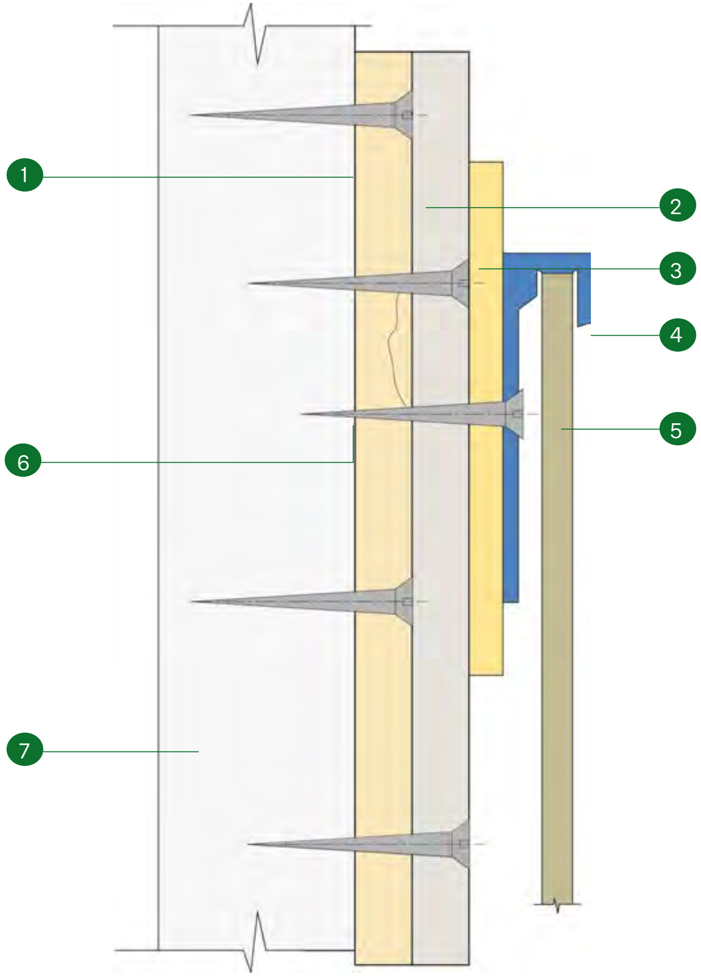


Figure 7.27: Indicative Sketch - Solid wall lining

7.13 Solid Doors

It is recommended that solid core doors with a minimum 1 hour fire rating are used to provide the required level of robustness. Details of the frame and method of fixing to the adjacent walls should be as fire tested.

It is not recommended that changes are made to doors that require fire rating without manufacture consultation.

Vision panel details should be as per the manufacturer's specification. Where vision panels are required, appropriate secure locking hardware is to be specified. If the station has a blast requirement, then vision panels are required to be laminated.

If fire rated glazing, insulating or non insulating is required then the security specialist should be consulted as there are options available.

Monolithic and georgian wire glass is not permitted.

1. Good quality solid core of the required thickness
2. Architraves should be pinned and glued in accordance with manufacturer's recommendations. It is important that these are resiliently attached to the substrate so that they do not become detached during a blast event. Details should be submitted to the security consultant prior to manufacture/installation.

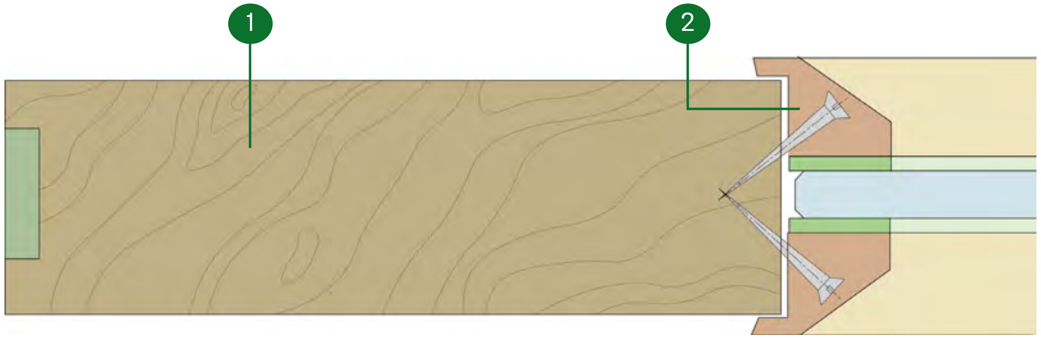


Figure 7.28: Indicative Sketch - Cross sections of door to vision panel

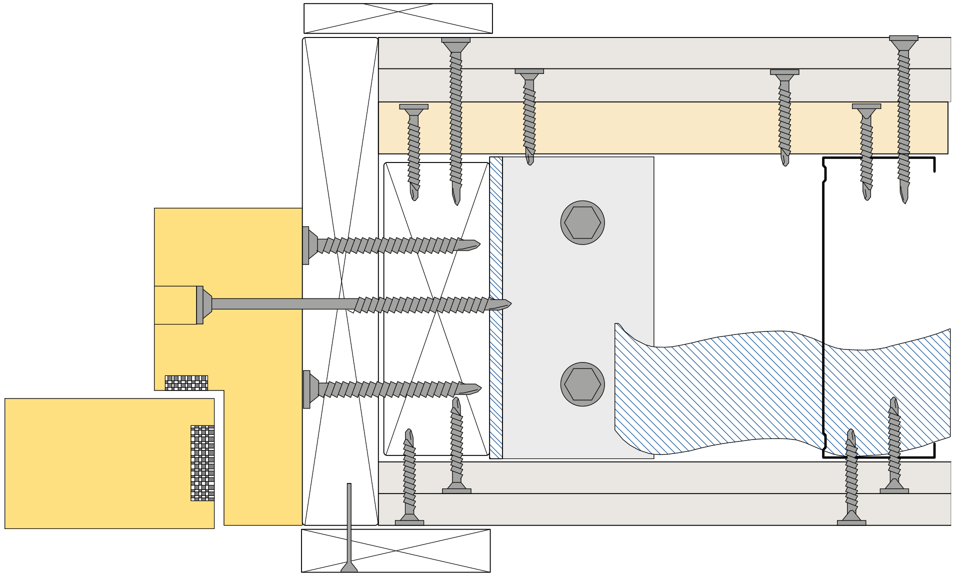


Figure 7.29: Indicative Sketch - Typical fire rated door frame to dry wall

7.14 Secure Walls

In some areas of the station, high performance security rated walls might be required. These might typically be used around cash offices, critical service equipment areas or station control rooms. These types of walls might need to meet a blast performance requirement as a physical security requirement. The use of dry wall systems with metal plate or metal mesh layers might achieve these. It is recommended that designers refer to the Centre for Protection of National Infrastructure (CPNI) for further guidance.

1. Minimum 18mm Plywood (medium grade - important) secured with drywall screws to vertical studs at 200mm centres
2. 12.5mm, 15mm or 18mm Fermacell - stagger joints to security mesh
3. Severe duty SD or Heavy duty HD classification standards of "robustness" drywall or shaftwall.
4. "I" or "C" stud (depending on drywall classification) at 300mm centres
5. Lathing (EML) Ref 50-75 HF or Securilath HD1 manufactured by Expamet Building Products Ltd, or 50-73F manufactured by Metal Mesh Ltd. Butt jointed tied with 1.6mm galvanised wire at 400mm centres
6. 38mm Ø washers fixed with drywall screws at 300 mm centres to drywall studs holding security mesh. Pay particular attention at joints in security mesh

The mesh should be cut to a maximum of 25mm away from any service penetration and fully secured with washers and fixings. Any service penetrations large enough for a person to pass through should have an internal grid fitted to prevent egress. This size should be agreed with railway security,

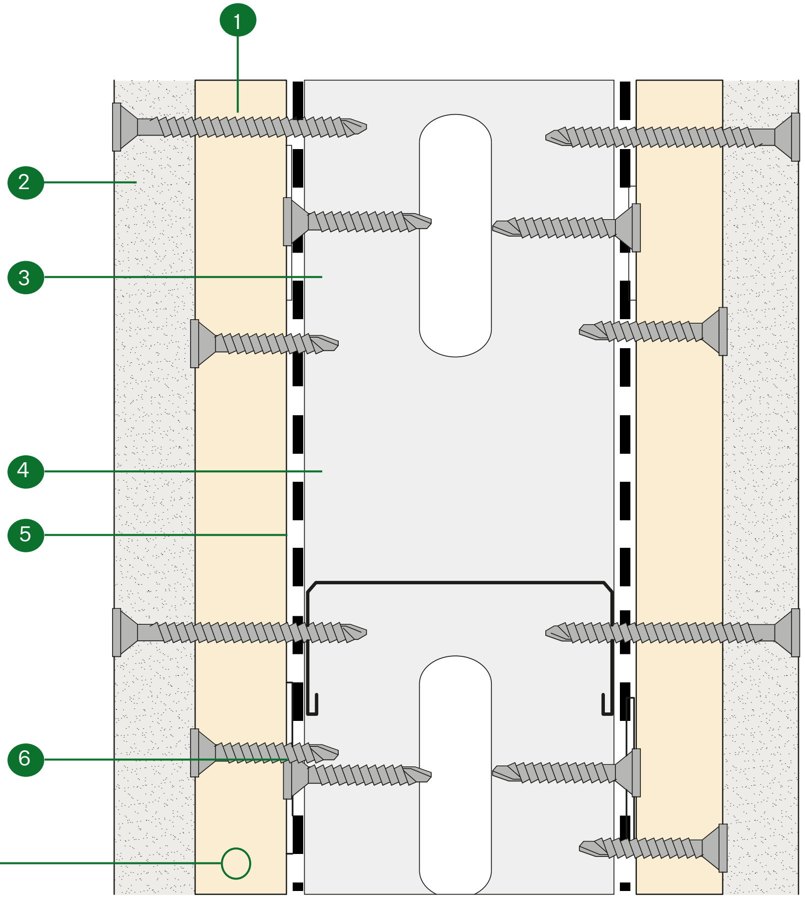


Figure 7.30: Indicative Sketch - EW03 (B10) MFES Solution Indicative Sketch

7.15 Suspension Solutions

Items that are fixed to ceilings, columns or walls and that weigh over 0.5 kg should be either:

→ Mechanically fixed in a robust manner to a suitable substrate or to a secure part of the substructure or

→ Tethered using an appropriate tether suspension kit, fixed to a suitable substrate or to a secure part of the structure or

→ Both mechanically fixed and tethered.

→ The tethers should be provided by an approved manufacturer.

→ Tethers should be tested and approved by a suitable security engineer, and should comprise of a braided wire type product.

To calculate the appropriate tether take 2x dead weight and use the manufacturers weight tables to pick the appropriate tether dimension. We are relying upon the Factor of Safety to cover the relative uncertainties and provide a high confidence in successful retention in blast.

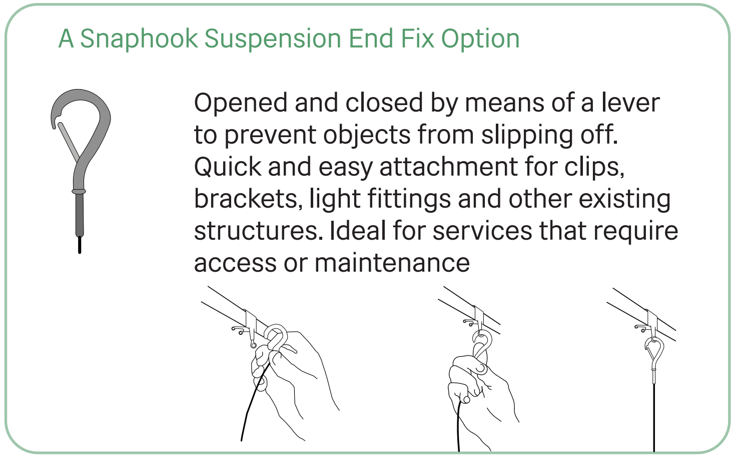
The tether is supplied as part of a complete suspension kit, comprising of the hanger and a high-tensile wire rope with a choice of end fixing attached to it. Many tethers are specifically designed to enable quick and easy installation of a variety of building services, signage, acoustic baffles and much more, and is a proven replacement to traditional threaded rod and chain solutions.

Tethers should have a factor of safety of no less than 5:1 over the working load.

Tethers should be designed so that when activated they suspend the attached item at a height that should not cause injury to persons below i.e. do not make the tethers too long.

Tethers should not be pulled taught, some slack is required to prevent the tether immediately snapping under blast loading.

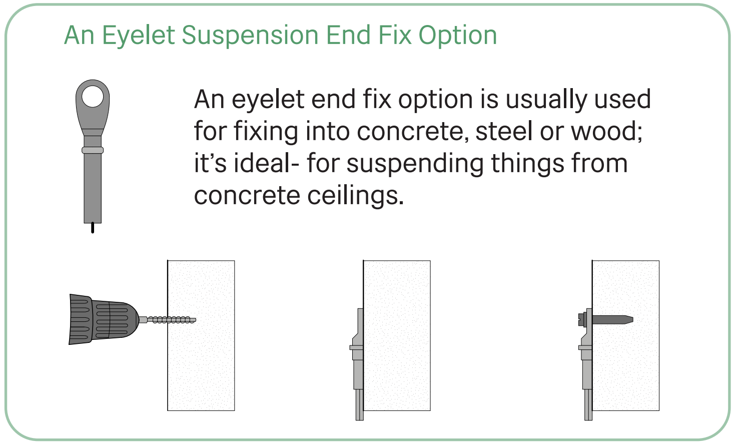
Image 7.31: Suspended signs at Waterloo Station



A Snaphook Suspension End Fix Option

Opened and closed by means of a lever to prevent objects from slipping off. Quick and easy attachment for clips, brackets, light fittings and other existing structures. Ideal for services that require access or maintenance

Figure 7.32: Snaphook suspension end fix option



An Eyelet Suspension End Fix Option

An eyelet end fix option is usually used for fixing into concrete, steel or wood; it’s ideal- for suspending things from concrete ceilings.

Figure 7.33: Eyelet suspension end fix option

7.16 Suspended Ceilings

Blast testing has shown that ceiling tiles might be picked up and projected under blast loading or they might be dislodged from the support system and fall. This can happen even at a substantial distance from the charge.

Ceiling tiles should be tethered to allow them to fall from the support system but not to strike persons below. For the tether to be effective, it should be anchored to a robust part of the structure that will not fail. There should be a minimum 2-metre clear space underneath any dislodged panel.

SAS and Armstrong are the main companies that produce suspended ceiling tiles. SAS have their own tethers that can be used with their ceiling systems. These tethers have a 5:1 factor of safety. Tether thickness and type should be calculated by taking the dead weight of the ceiling tile to be tethered and doubling this. The calculated weight is then used to look up the appropriate tether product.

→ Supporting calculations are advised.

→ E.g., if the weight of a ceiling tile was 20-kg, then the tether should have a 40-kg (2 x 20-kg) capacity.

The particular tether used in the example sketch, has a 5:1 safety factor and this is used to provide the advised margin of safety in blast. It is important that the connections have the same capacity as the tether and there are many connection types to select from.

Image 7.34: Suspended ceiling CGI

Correctly tethered ceiling

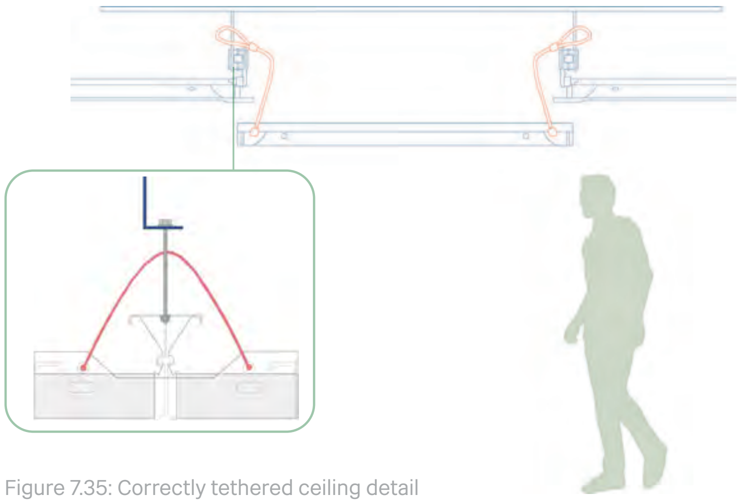


Figure 7.35: Correctly tethered ceiling detail

Incorrectly tethered ceiling

Persons underneath are struck by swinging ceiling panels, therefore posing extreme risk in cases of blast. The designer should aim for 2m clear space underneath any dislodged panel.

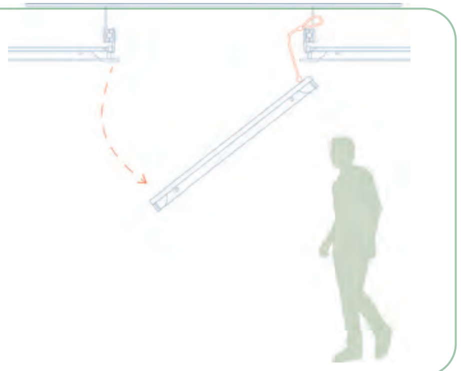


Figure 7.36: Incorrectly tethered ceiling detail

7.17 Suspended CIS

Customer Information Screens displaying information for passengers and station users. Usually found in areas like the concourse, plaforms, and public realm.

Approved screens should be utilised for the suspended information display screens.

The adjacent diagram is a particular illustration of a universal joint to minimise the forces on the connection to the structure.

Fixings should be designed by a Register of Security Engineers and Specialists (RSES) member or otherwise suitable engineer to resist the blast loading.

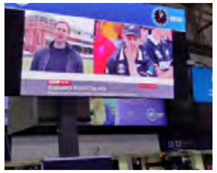
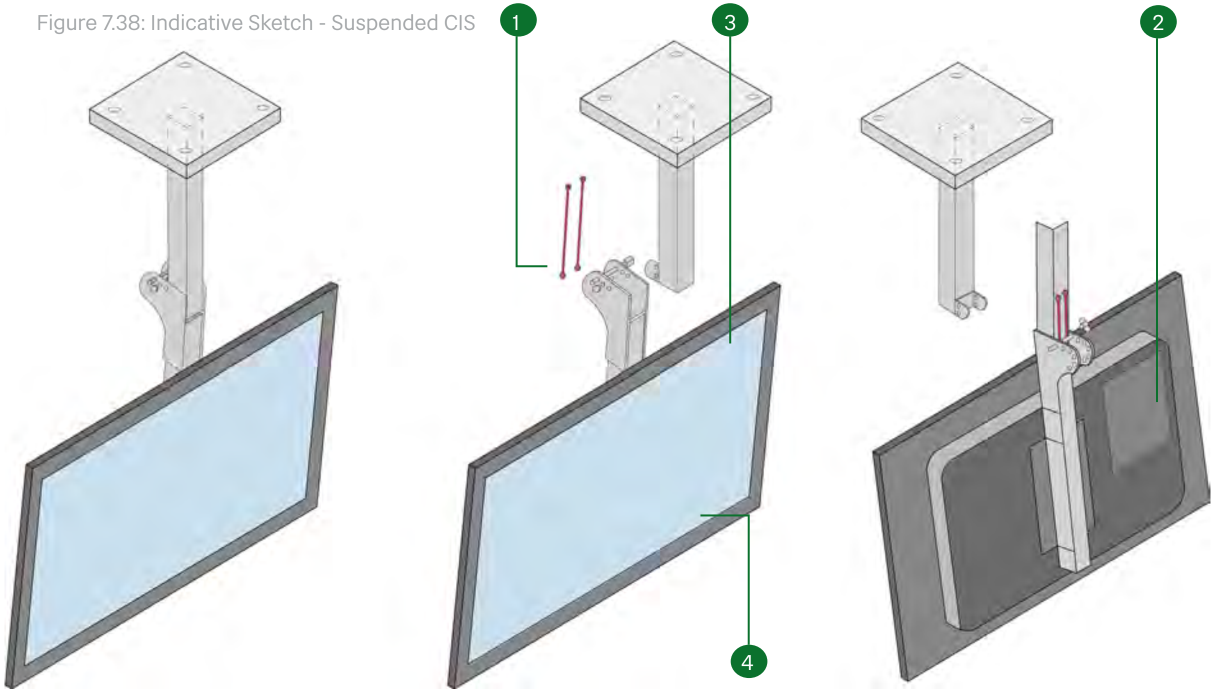


Image 7.37: Examples of suspended CIS at Euston Station

NR Guidance Suite Reference

Network Rail Video Level 2 Specification: Video Surveillance Systems
NR/L2/TEL/30135

Figure 7.38: Indicative Sketch - Suspended CIS



1 Tethers between the screen and supporting structure. Two tethers supporting the angle bracket should be utilised, the tether should have a capacity of minimum 2x mass, and a factor of safety 5:1. Tethers should not be tought.

2 All opening metal panels robustly fixed to internal framework, piano hinge preferred, otherwise tether.

3 Internal framework capable of transmitting all load to substrate.

4 All display panels robustly fixed to internal framework and mechanically locked in place with appropriate brackets.
All available rear fixing locations should be used.

7.18 Floor Mounted Monolith or Display Screens

Floor mounted monolith/display screens are screens for displaying information for passengers and station users. They are commonly found in spaces like Concourse, Public realm, Platforms.

All glazed display panels should utilise toughened laminated glass or approved interactive screens in preference to Polycarbonate or Acrylic sheet. The use of Polycarbonate or Acrylic sheet will require approval from the Station Facilities Operator (SFO) for single sided only.

All glass to be checked for suitability for serviceability loads.

Fixings should be designed by a Register of Security Engineers and Specialists (RSES) member or otherwise suitable engineer to resist the blast loading.

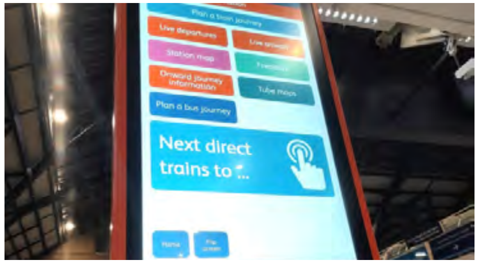
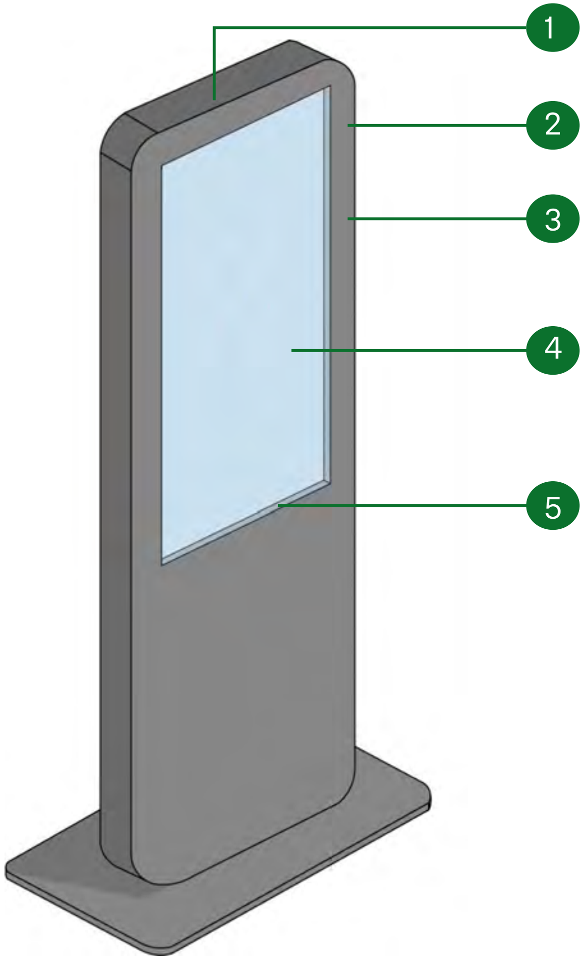


Image 7.39: Example of display screens on station concourse



1 All opening metal panels robustly fixed to internal framework, piano hinge preferred

2 All metal panels robustly fixed to internal framework – no lift off panels permitted unless mechanically secured or tethered

3 Internal framework capable of transmitting all load to substrate

4 All display panels robustly fixed to internal framework or contained within 15mm cover and bonded to subframe

5 All glazed display panels should utilise toughened (heat soaked) laminate glass (or monolithic toughened for single sided displays only) options or stretch fabric in preference to Polycarbonate or Acrylic sheet . Approval needed if using single sided polycarbonate or acrylic

Figure 7.40: Indicative Sketch - Floor mounted display screen

7.19 Retractable Belt Barriers

Retractable barriers are used to control and direct queues, and are used wherever queues might form for example the concourse.

The signage topper should be mechanically fixed to the post. Options for this include 2no M4 Tek screws passing into the pole, or a blast tested tether. The tether is likely to be external due to the complexities involved within the bolt wind mechanisms.

The maximum recommended size is A4. A3 can be permitted but advice should be sought from station security.

Infill materials like acrylic pockets are prohibited and should be replaced with the approved Foamex materials printed with graphic or with applied graphics. 2mm aluminium is permitted with self-adhesive graphics applied

Drop down barriers or other adaptions are not permitted as they result in a high hazard to surrounding users. This includes the use of solid dividing bars.

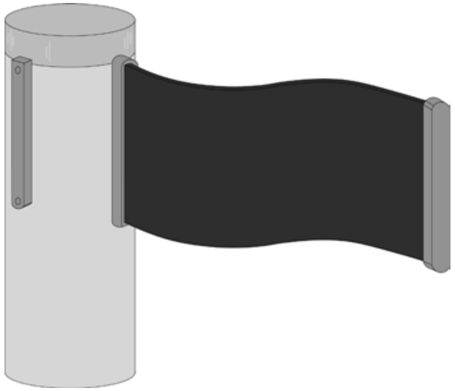


Figure 7.41: Indicative Sketch - Standard retractable belt barrier

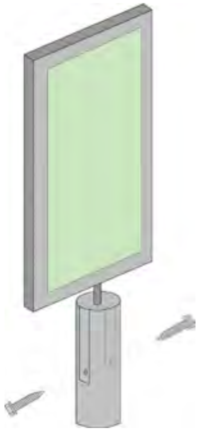
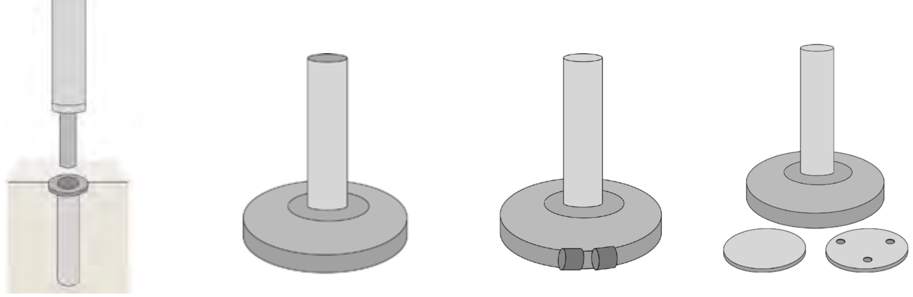


Figure 7.42: Indicative Sketch - Optional signage toppers

Floor Fixings

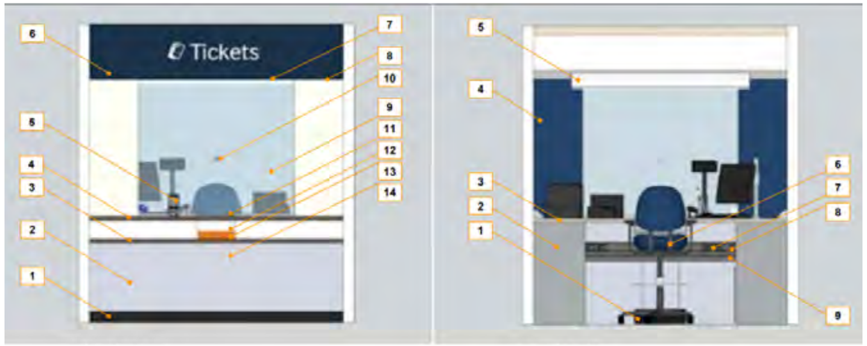
Standard retractable belt systems have been tested with various floor fixing options; spigoted base, weighted base,wheeled base, and magnetic base. All of these are acceptable for use.



7.20 Ticket Vending

Ticket issuing windows should generally follow the guidance set out in Network Rail Station Facilities and Amenities Design Guide ref. NR/GN/CIV/200/03. Where relevant, additional consideration might be required to check that new ticket issuing windows comply with blast resistance requirements. Where this is necessary, it is recommended that projects consult a blast specialist from the Register of Security Engineers and Specialists (RSES).

Image 7.43: Ticket vending machine in a station



EXTERIOR VIEW:

1. Plinth
2. Facia
3. Lower counter (750H)' - Under counter clearance 700mm minimum
4. Upper counter (950H)
5. Ergonomic chip & pin mount – Code: IDL-0116
6. Bulkhead sign - Code: IDL0134 Soffit with integrated LED down lights and speech transfer speakers Code: IDL-0122
7. Security shutter – Code: IDL-0133
8. LED Down lights – Code: 0122
9. Manual attack window – Code: IDL-0117
10. Customer microphone - Code: IDL-0123
11. Draught excluder – Code: IDL-0143
12. DFA Cash Tray™ (dual height counter transfer tray) – Code: IDL-0115
13. Extending drawer
14. Induction loop

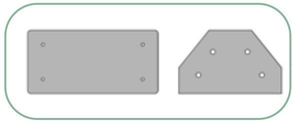
INTERIOR VIEW:

1. Adjustable height footrest - Code: IDL-0124
2. Cupboards with lockable top drawer - Code: IDL-0136
3. Counter tops - Code: IDL-0138
4. Pin boards - acoustic panels - Code: IDL-0125
5. Roller blinds 'Position Closed' - Code: IDL-0126
6. Adjustable chair with foot ring - Code: IDL-0130
7. Power sockets - Code: IDL-0128
8. Data sockets - Code: IDL-0129
9. Cable management - 2 compartment segregation - Code: IDL-0127

Figure 7.44: Layout of a ticket desk

For wall mounted versions the designer has a responsibility to check that the substrate (wall) can take these loads. This might need to be assessed by station engineering.

The Cammax base plate is secured with four suitable M12 gr 8.8 or equivalent security anchors, secured with a flat washer, lock washer and antivibration lock nut. Utilise the proprietary holes in the base of the kiosk.



All ticket vending machines should have curved or angled tops to avoid creating opportunities for the placement of threats.

Note: The unit is required to self-right when tipped to an angle of 30 degrees. This test is to be conducted without the fixings in place.

Tethers or robust base fixings required.

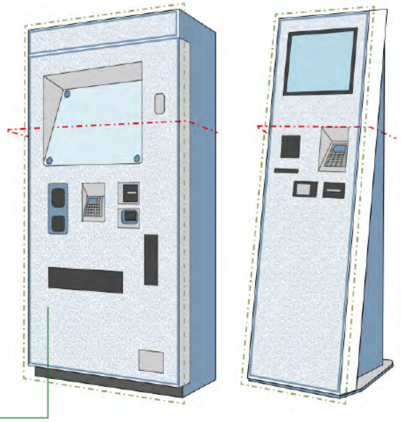


Figure 7.45 Indicitive sketches of ticket vending machine types

7.21 Gateline Technology

Gateline Technology is ticket gates forming the ticket line in a station.

All non-glazed materials should be carefully cleaned strictly following manufacturing guidelines. It is essential that the manufacturer of the element is consulted prior to applying any manifestation to the surface as it could cause irreparable damage.

7.21.1 Power and Data Services

It is critical that power and data services for the E-gates do not compromise the location and structural capability of fixings between E-gate components and the substrate. Locations of fixings should be considered when routing the power and data services to the E-gate installation.

Any trunking passing across or within the main access routes should be robustly mechanically fixed and have the appropriate slip resistance.

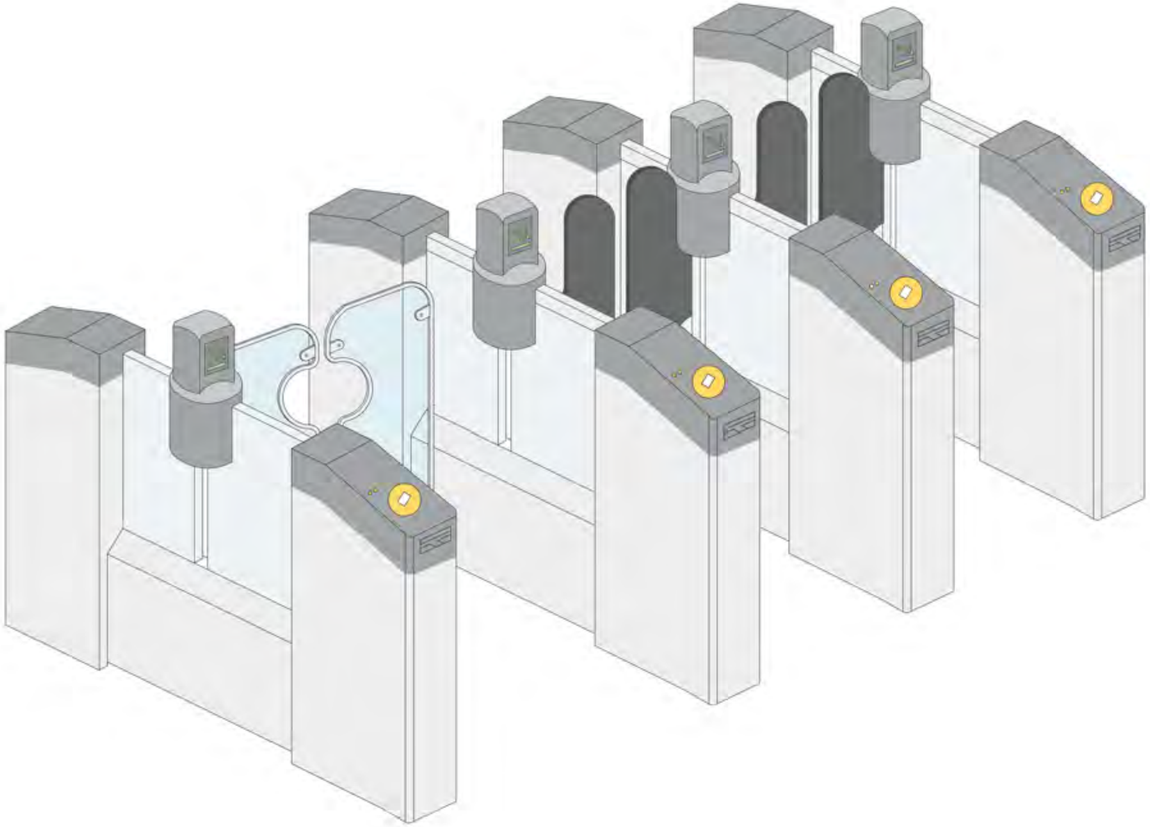


Figure 7.46: Indicitive sketch - Standard configuration with ‘End Gate’

NR Guidance Suite Reference

Network Rail Station Capacity Planning Design Manual
NR/GN/CIV/100/03

Designing For Blast Resistance

7.22 Concourse Seating and Furniture

Seating locations should be carefully chosen following Station Capacity Planning Guidance and recommendations in Security in the Design of Stations (SIDOS).

Any furniture should not impede the flow of passenger movement or emergency evacuation.

Seat base fixings should not extend beyond the profile of the seat causing a potential trip hazard.

Where possible all seating should be bolted to the substrate.

Any provided seating or furniture should be either fully enclosed or open to permit security sweeps to be made and prevent hiding of suspect packages.

Some items have been approved by blast testing or desktop study, this should be checked by a specialist consultant. Manufacturers with approved items include Herman Miller, OMK Design and Vitra.

Standard seating

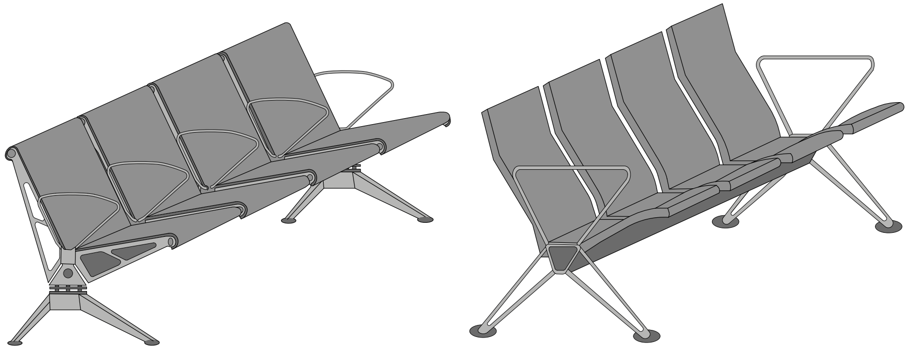


Figure 7.47: Indicitive sketch- Standard seating illustration

Timber slatted seating

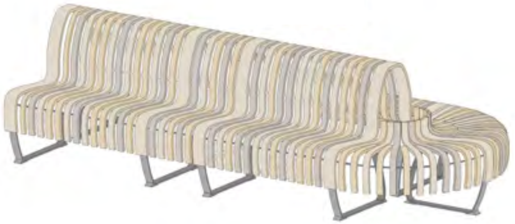


Figure 7.48: Indicitive sketch - Timber slatted seating

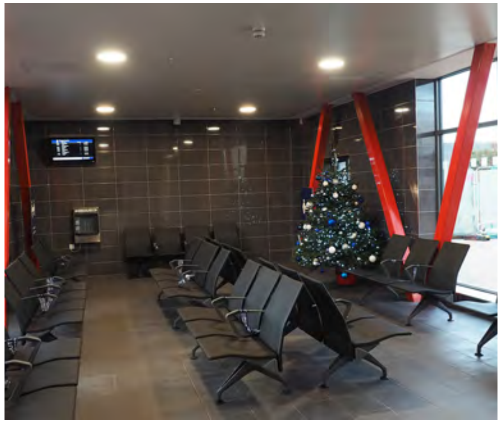


Image 7.49: Standard seating in station waiting area

Image 7.50: Victoria station seating

Image 7.51: Liverpool street station seating

7.23 Projecting Signs

A "Projecting Sign" is defined as a sign attached to the substrate, often in front of a retail unit, typically with a maximum dimension of 600mm x 600mm.

1. 2mm aluminium or mild steel support frame with overlap welded connections. Top and bottom sections to be 'U' channels with vertical edges facing upwards to allow connection with metal 'Z' brackets to reverse of signage infill panels.

2. Robust fixings to structure, number dependent upon site conditions. Fixings should be designed to retain supporting framework in position under the blast load. Large penny washer to be utilised between fixing head and 2mm section to minimise risk of pull through. Engineering calculations will be required.

3. Signage infill panels supported by internal flange and minimum 3no 5mm TEK screws [04]. The outer cladding feature requires additional tethering, Gripple tethers of the appropriate size for the net weight of all components, ends should be secured under penny washers and fixings to substrate.

4. Individual signage panels secured by internal flange and minimum 3no 5mm TEK screws to the 2mm U section, preventing the Z brackets easily dislodging. In a blast scenario these are expected to dislodge and be retained by tethers to stop items being projected.

5. Secure LED light drivers to lower U section, the fixings should be assessed if the drivers weigh more than 0.5kg.

6. Individual signage cassettes, manufactured from 2mm aluminium, the back face has a flange to accept fixings.

Image 7.52: Projecting sign example

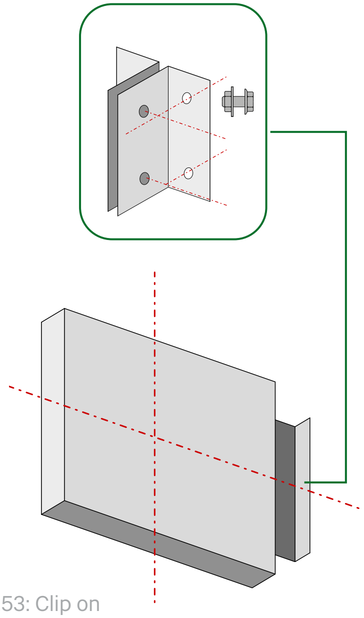


Figure 7.53: Clip on

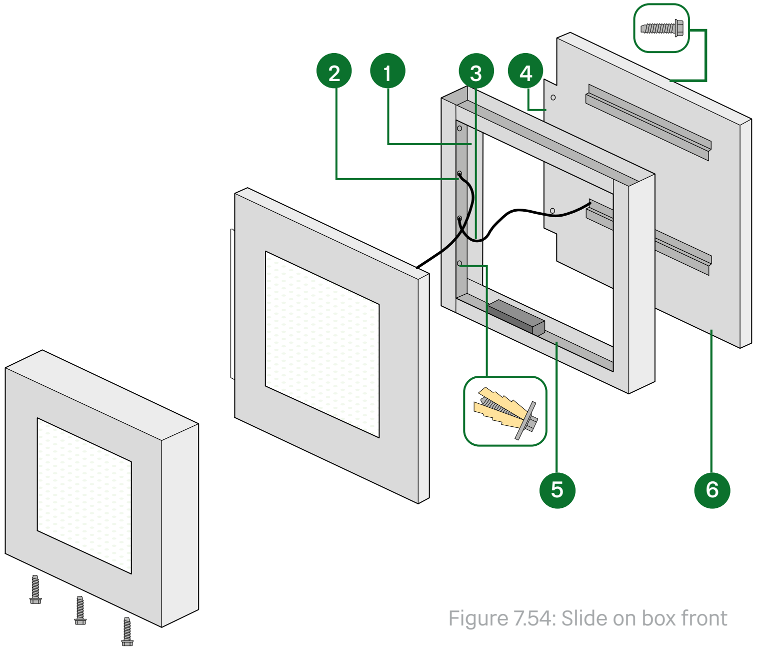


Figure 7.54: Slide on box front

7.24 Signage Infills

Signage infills should be robustly fixed, tethered where necessary and consider the frangibility of constituent components. 4 typical configurations are illustrated on this page.

Image 7.55: illuminated signage infill

1 2mm polyester powder coated aluminium#

2 Gravity hung ‘Z’ bracket, mechanically fixed to rear 2mm plate combined with anti jump fixings

3 Acrylic light distribution graphic material such as “opalux”, flat sheet adhered to inside of signage box with VHB. Use adhesion promotors and primers as required

4 Laser cut lettering to front of sign box, any central free standing graphic secured to light distribution material with appropriate flexible adhesive.

5 Flexible LED strips adhered to rear face by VHB (Very High Bond) pressure sensitive adhesive, use adhesion promotors and primers as required

6 Acrylic light distribution graphic material such as “opalux”, CNC cut sheet to provide projection of graphic material beyond face of sign box adhered to inside of signage box with VHB. Use adhesion promotors and primers as required

7 Graphic vinyl with high tack, low surface spread of flame, smoke and toxicity adhered to front face of sign box

8 Laser cut projecting back lit sign, flexible LED strips secured to front of sign box face through short acrylic stand offs, appropriate number and size of fixings to acrylic stand offs to be discussed based upon signage size and weight

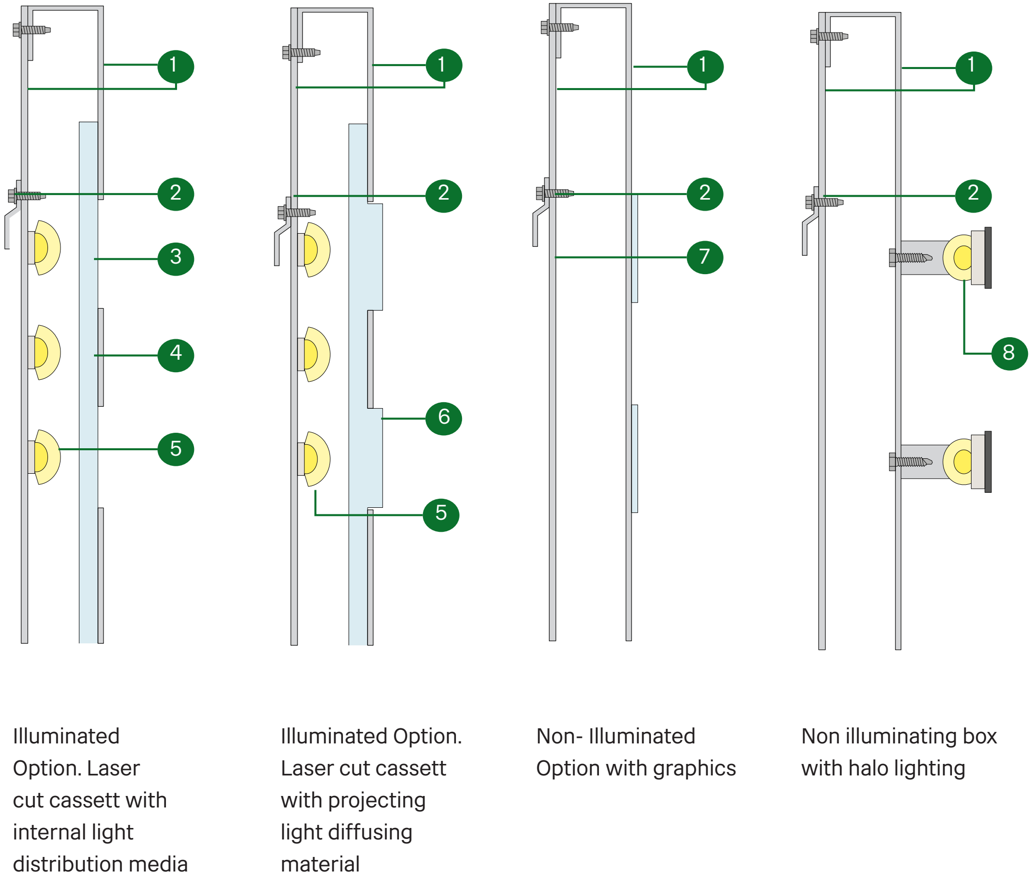

1
2
3
4
5
1
2
6
5
1
2
7
1
2
8
Illuminated Option. Laser cut cassett with internal light distribution media
Illuminated Option. Laser cut cassett with projecting light diffusing material
Non- Illuminated Option with graphics
Non illuminating box with halo lighting

Figure 7.56: Indicative sketch - Types of signage infills

7.25 Litter Bins

The location and design of litter and recycling bins in stations requires careful consideration.

The location of litter and recycling bins should be guided by a risk assessment. The Station Facilities Operator (SFO) should complete the risk assessment and a copy should be recorded with the Station Security Plan (SSP). This should take into account that bins should be located away from:

→ Corridors of station exits/ entrances;
→ Evacuation assembly points;
→ Sources of possible fragmentation such as overhead glazed canopies, within glass waiting shelters, windows, mirrors etc.;
→ Fire hydrants or electrical equipment; and
→ Structural columns, supports or similar.

All bins should consist of:

→ A clear plastic sack (mild tinting is permitted providing the colour does not obstruct view);
→ A metal hoop sack holder; and,
→ An integral bungee strap to secure the plastic sack.

Litter bins should not have a metal lid, although a rubberised lid might be used if there is written agreement with the DfT inspector.

In addition to hoop and sack bins that are built and installed in the specifications mandated, NRSP also allows for alternate designs of bins to be used if it can be evidenced that they achieve at least a 2* (two star) rating in accordance with Home Office Standard 23/14 version 2 dated June 2014 – "Test method for the determination of the explosion resistance of litter and recycling bins". Test 1C of this standard should be carried out in addition to any mandatory tests. Station operators should discuss the alternate bin design with the respective DfT station inspector before bin design and blast testing. Alternate bin designs should be mounted as per the tested version to the manufacture's instructions.

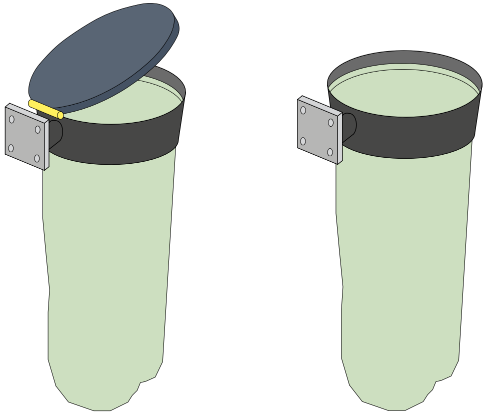


Figure 7.57: Indicative sketch -Blast compliant bins

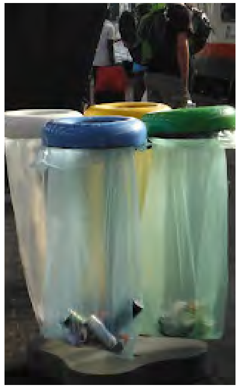


Image 7.58 Example of blast compliant bin

Image 7.59: Example of blast compliant bin

National Standard

National Railways Security Programme (NRSP) Section 7 – Station Security

NR Guidance Suite Reference

Network Rail Station Bin Security Requirements Guide

Designing For Blast Resistance

7.26 Public Toilets

Network Rail have published design guidance for public toilet facilities. As well as this, designers should consider the principles of Security in the Design of Stations (SIDOS) particularly with regard to robust fixings and frangibility of materials.

NR Guidance Suite Reference

Public Toilets in Managed Stations Design Guide, NR/GN/CIV/200/04

Code of Practice Guidance

Design of Stations (SIDOS)

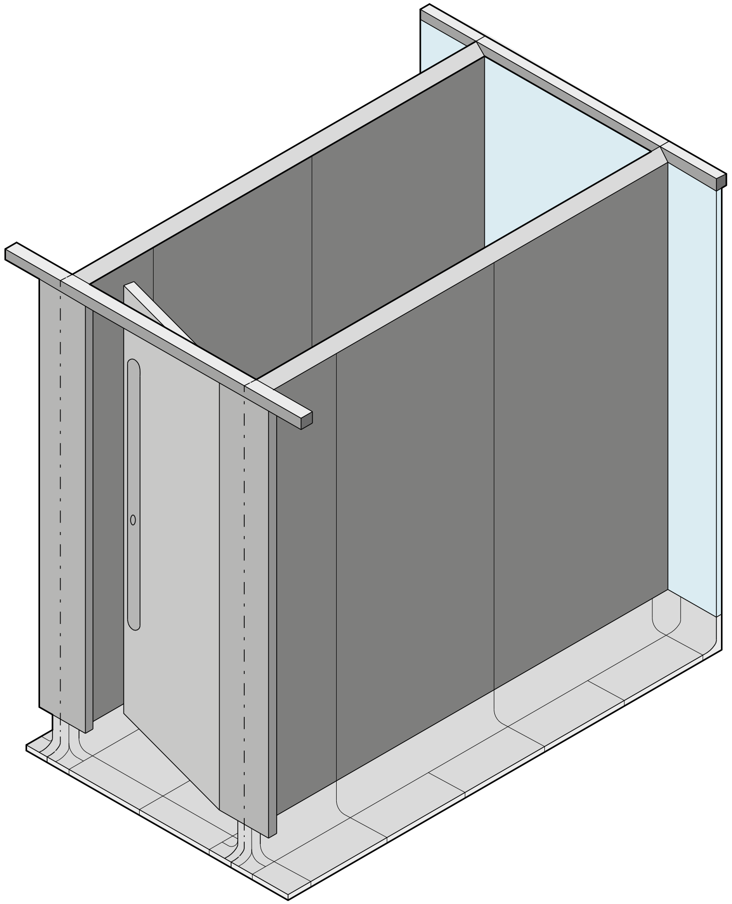


Image 7.60 Indicative sketch - standard station toilet cubicle

Image 7.61: Example of toilets at a station

Image 7.62: Example of newly renovated toilets at a station

Image 7.63
Passenger at Network Rail
Information Desk

8

Security at Stations Design Guide Manual

Station Approaches

8.1 Public Realm

The public realm around a station is the first part of the railway station that departing passengers will come into contact with the station security measures. This is the point where members of the public will begin to fall within the protection and the duty of care of the station. This is also the first opportunity for the station to provide territorial reinforcement as described in section 4.2 on CPTED.

The public realm areas around stations should benefit from both natural surveillance as well as comprehensive technical surveillance, with a particular focus on station entrance areas. Consideration should be given to potential nefarious uses of landscaping measures in the public realm to reduce opportunities of misuse (e.g. anti-social behaviour and vagrancy) as well as providing opportunities for hostile reconnaissance.

The security measures that are likely to define the public realm are Hostile Vehicle Mitigation (HVM). HVM can take many forms, e.g. bollards, street furniture, and level changes through landscaping measures. However, the purpose of HVM measures remain the same which is to provide protection against a Vehicle As a Weapon (VAW) attack againstpedestrians in the public realm or the station itself, or to enforce stand-off to the station building to provide protection against a Vehicle Borne Improvised Explosive Device (VBIED).

High pedestrian population and high-profile sites feature prominently in past vehicle borne attacks and larger railway stations would be considered as falling into those categories. Throughout the week, especially at peak times, and during weekends and public holidays, stations will have significant numbers of people congregating. This makes them an obvious target for vehicle borne threats.

As a minimum, HVM protection around stations should prevent unauthorised vehicle access to the station itself. Ideally, HVM should be used to maximise stand-off around the station and provide protection to external public realm areas as well.

The National Railways Security Programme (NRSP) mandates HVM at new Security Category A stations and recommended this at Category B Stations. This is also best practice at other categories. When conducting a significant upgrade of a station, if HVM is not present at a Category A station NRSP requires that it should be installed (recommended at Category B).

NR Guidance Suite Reference

Network Rail Station Capacity Planning Design Manual NR/GN/CIV/100/03

National Standard

National Railway Security Programme (NRSP) Section 7 Annex M

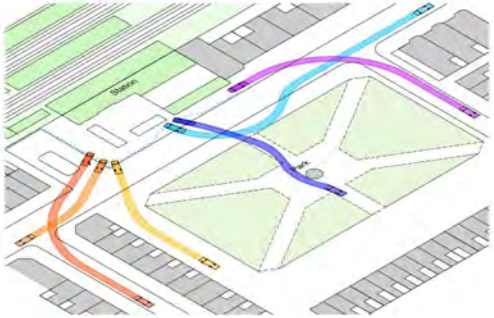
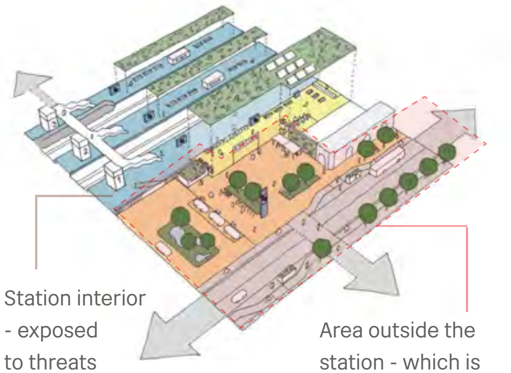


Figure 8.1 Ease of access from roadway to pavements, pedestrian zones and gardens



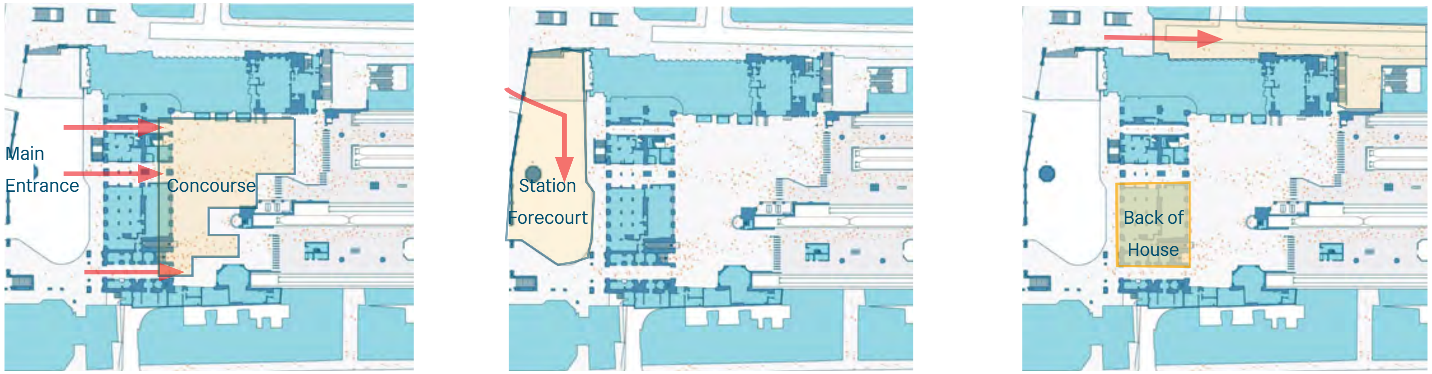
Station interior - exposed to threats discussed in Section 3

Area outside the station - which is exposed to hostile vehicle attacks to safety and security

Figure 8.2: Isometric sketch of standard station layout

Station Approaches

8.2 Entrance Points



Figures 8.3: Plan sketch of standard station layout

The main entry points to stations are those for pedestrians. These are typically doors located on the front of the line of the station behind the forecourt. They are designed for high footfall and provide direct access to the station concourse. They are the most trafficked and are the main locations for those using the station and are often wide enough for a vehicle to drive through, especially double doors. As well as serving as entry points, they are also used by those exiting the station buildings. Many stations have additional smaller entrances located on the sides on the building structure. Whilst these are not as heavily used as the main entrances, they often provide direct access to the station concourse.

Vehicle entrances to stations are varied. Access to station forecourts is often required for emergency or maintenance vehicles. Typically, this would be managed by station staff with managers and traffic marshals working to set operational procedures. It is essential that the correct procedures are followed to prevent any vehicles from coming into contact with stations users and operators. With regards to the line of protection provided by HVM measures, there should be provision for the movement of vehicles through the line. The measures might be removable or be able to be lowered and raised either locally or remotely in order to provide the required vehicular access.

Service entrances for vehicles are common at many stations. These typically include lorries and vans for deliveries to station shops and cafes, maintenance, contractors and the emergency services. They should be located away from the main public realm areas but can provide direct or indirect access to them, especially platforms and the concourse.

Code of Practice Guidance

Security In the Design Of Stations Guidance (SIDOS)
CPNI HVM Public Realm Guidance 2022

8.3 Hostile Vehicle Mitigation

HVM is the term used to describe measures which prevent the unauthorised access by a vehicle with hostile intent from gaining access to a specific area (through penetrative means or otherwise).

Historically, the principal threat against which HVM has been installed is that of a Vehicle Borne Improvised Explosive Device (VBIED). The intention of which was to enforce stand-off distance around the building and therefore mitigate the impact of any such attack. However, in recent years, the emergence of the Vehicle as a Weapon (VAW) attack has become increasingly prevalent. These attacks are those whereby an attacker will obtain a vehicle and drive at speed through a crowd with a view to killing and injuring as many people as they can. The relative simplicity of the VAW attack makes it appealing to any individual or group with hostile intent. Given the ease at which such an attack can be carried out, and the relatively little planning required, it is likely that such attacks will continue for the foreseeable future.

The ability to reach the target without being detected or stopped on route will be taken into consideration as will the ease of access. These scenarios include the following:

- Long linear attack routes with minimal obstacles, to deter, slow, divert or stop an attack.
- Ease of access from roadway to pavements, pedestrian zones and gardens, potentially at high speed.
- Pedestrians exposed to VAW threat due to HVM measures being set back from the roadway, leaving pavement spaces accessible to vehicles.

Pre-attack planning can range from the complex and detailed, undertaken over a period of time, to something based on the terrorist's familiarity with the target. During the planning phase, there will be a period of information gathering in order to confirm approach routes and point of attack to achieve the desired effect.

The installation of fixed structures such as barriers, planters and walls will act as a visual deterrent to a vehicle attack (street furniture such as street lighting and signage, or an intermittent police presence do not). It should be remembered that the terrorist is not deterred by the prospect of being caught or fatally injured in the act; their intention is to maximise harm. The method of attack will be dependent on the aim (propaganda, economic or mass casualty), but will be heavily influenced by the capabilities of the group carrying out the attack.

As a result, the threat will vary as outlined below in descending order:

- Large devices consisting of several hundred kilograms of commercial or home made explosives using trucks and vans (LVBIED).
- Mid range car bombs. (VBIED).
- Crude devices relying on a small quantity of explosives but enhanced with easy to obtain items such as cans of petrol or gas bottles.
- The 'lowest tech' threat simply using a vehicle as a momentum weapon. This is a trend that has been increasing. (VAW).

Image 8.4: Pick up/drop off point outside station

Code of Practice Guidance

Security In the Design Of Stations Guidance (SIDOS)

National Standard

National Railway Security Programme (NRSP)

8.3 Hostile Vehicle Mitigation Continued

There are five main types of vehicle borne threat. All can be used with or without the use of a suicide operative. In addition, the tactics might be combined, or used with other forms of attack. These are:

- → Parked Vehicle: A vehicle is parked in an unscreened area adjacent to the target, or in an onsite (legitimate) open parking area. This tactic easily blends in with normal day to day activity and in some cases, the terrorist may socially engineer Security Officers by visiting the area in the same or similar vehicle over several days prior to the attack; this familiarity is designed to influence Officers to be less stringent in their checks. The terrorist may also use a 'ringer' vehicle.

- → Encroachment: This is where the hostile vehicle is negotiated into the target area through an incomplete perimeter barrier without the need of impact or forced penetration. For example, gaps between bollards, crash barriers, street furniture or by driving along pavements from an entry point outside the control of the target location. Any gaps that are wide enough for vehicles to pass through can be exploited. An alternative encroachment tactic is to tailgate a legitimate vehicle through an access control point due to slow or ineffective barrier controls or exploit weaknesses in security procedures such as leaving gates or barriers open during periods of high traffic flow.

- → Penetrative Attacks: Penetrative attacks use the front or the rear of the vehicle as a ram in order to smash through any physical barrier. As a tactic, it has been used by criminals, as well as terrorists, most notably suicide bombers.
- → Deception: Deception tactics exploit human behaviour. For vehicle borne threats this may be by using a 'ringer' vehicle whose make, model, registration or livery is familiar to the site, or by the hostile occupants negotiating their way through by use of pretence, social engineering, or by using stolen or cloned access control or ID passes. Alternative methods include the surreptitious planting of a device on a vehicle that has access, or an 'insider' bringing an IED device into their own work site.
- → Duress: Duress against the driver of a legitimate vehicle who is forced to carry the IED to the target (commonly known as proxy attacks). Alternatively, threats are made against a Security Officer controlling a vehicle access control point.

Code of Practice Guidance

Security In the Design Of Stations Guidance (SIDOS)

National Standard

National Railway Security Programme (NRSP) Section 7 Annex M

8.4 Standards and Guidance

Where HVM is defined as a requirement at a train station, the design of HVM should be overseen by a Principal Member of the Register of Security Engineers and Specialists (RSES) admitted under specialist category E (Hostile Vehicle Mitigation).

The preference is that all HVM measures comprise measures that have been successfully tested in accordance with one of the following standards:

- → PAS 68: 2013 - Impact test specifications for vehicle security barrier systems
- → IWA 14-1: 2013 - Vehicle security barriers - Performance requirement, vehicle impact test method and performance rating

These standards specify the essential impact performance requirements for HVM measures and a test method for rating their performance when subjected to a single impact by a test vehicle.

Although IWA 14 is now the preferred testing standard for CPNI, all existing PAS 68 rated products and any future products which test to PAS 68 are still suitable for HVM. However, special attention should be given the differences in rating system between PAS68 and IWA 14-1, and particularly the reported penetration distance (this being the distance that an impacting vehicle was arrested beyond the HVM measures being tested).

For example, an automatic rising bollard tested in accordance with IWA 14 may achieve a rating of V/7200[N2A]/80/90:2.4.
This classification denotes:

- → V - Tested using the vehicle impact method;
- → 7200[N2A] – Tested with an impact from a 7,200kg N2A class vehicle;
- → 80 - Impact speed of 80kph (~50mph);
- → 90 - Impacted at 90 degrees to the front face of the bollard;
- → 2.4 – Where the vehicle reference point penetrated 2.4 meters beyond the original position of the front face of the bollard;

In line with PAS 68:2013, for the same impact test would yield the classification V/7500[N2]/80/90:2.1
/5.3 denoting:

- → V - Tested using the vehicle impact method;
- → 7500 – Tested with an impact from a 7,500kg N3 class vehicle;
- → 80 - Impact speed of 80kph (~50mph);
- → 90 - Impacted at 90 degrees to the front face of the bollard;
- → 2.1 – Where the vehicle reference point penetrated 2.1 meters beyond the original position of the rear face of the bollard;
- → 5.3 – The maximum debris throw from the vehicle following impact.

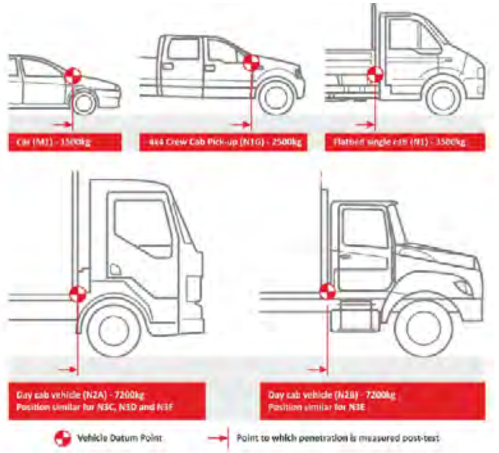

Car (M1) - 1500kg
4x4 Crew Cab Pick-up (N1G) - 2500kg
Flatbed single cab (N1) - 3500kg
Day cab vehicle (N2A) - 7200kg
Position similar for N3C, N3D and N3F
Day cab vehicle (N2B) - 7200kg
Position similar for N3E
Vehicle Datum Point
Point to which penetration is measured post-test

Figure 8.5: Vehicle impact datum points PAS 68

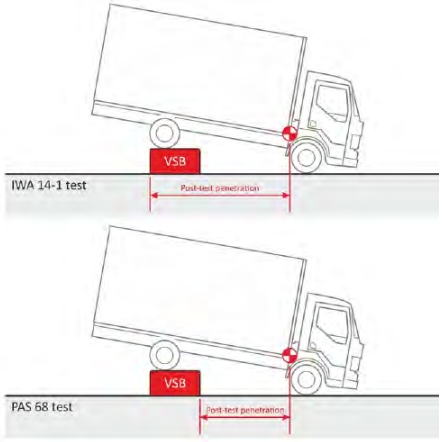


Figure 8.6: Differences between penetration distances in IWA 14-1 and PAS 68

8.5 HVM Design

The design of all HVM measures should be overseen by a Principal Member of the Register of Security Engineers and Specialists (RSES) with the Hostile Vehicle Mitigation specialist category. The person responsible for the HVM design should be able to demonstrate relevant experience in relation to the design of HVM schemes.

The selection of HVM measures around a station will be influenced by the specific operational requirements of the installations. The measures should have the following characteristics.

- → Minimal impact on existing traffic flow
- → Minimal impact on existing pedestrian permeability
- → Appropriate performance rating
- → Cost effective
- → Low maintenance
- → Easy to install avoiding the need for service diversions

The HVM solution is dependent on location which should be optimised to provide the maximum unhindered passage for pedestrians and vehicles. The final selection should be based primarily on the performance criteria for impact resistance, finished in keeping with the aspirations of the station and that of the local urban environment.

Security barriers tend to be steel, either painted or galvanised. Most security barriers are galvanised. Compliant bollards tend to be manufactured as circular hollow steel sections, with either a painted finish or some form of architectural cladding, such as stainless steel. Bollards can been clad in granite, cast aluminium sleeves or moulded plastic.

The bollards or security barriers requiring pedestrian access should be positioned such that the maximum clear distance between the barrier when measured at a height of 600mm above the finished pavement level does not exceed 1200mm. The height at which the dimension is measured is to allow for tapered sections and is to prevent the impact point of the vehicle from squeezing between the gaps between the measures.

When using bollards, typically they should have a minimum height of 900mm and a maximum height of 1200mm. When installed as part of a street-scape project, lighting columns and other street furniture can be enhanced to provide the appropriate level of crash-rating, therefore the height limits do not apply.

When installing to prevent unauthorised vehicle access, particularly from terrorist vehicles, it is necessary to maintain the maximum gap at the return ends of the line of protection.

Image 8.7: Helicopter image of a police car carrying out HVM measures

Station Approaches

8.6 Vehicle Dynamics Assessments

In order to determine the impact speed of a hostile vehicle at a specific location, a Vehicle Dynamics Assessment (VDA) is undertaken. The aim of the VDA is to establish the highest achievable impact speed to a single measure in any proposed line of protection, thus determining the required crash rating of the deployed product.

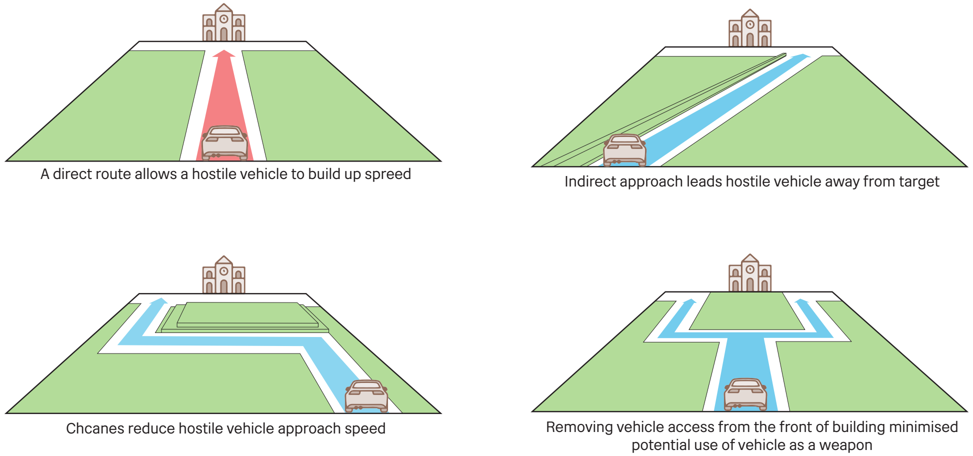
All routes to an identified target are explored and considered. These include the obvious routes for high-risk vehicles (such as the N2A), less obvious routes and finally those unlikely ones which would probably be restricted to smaller vehicles.

VDAs should be undertaken in accordance with the methodology set out in the CPNI Hostile Vehicle Mitigation Guide, adopting the vehicle handling charts provided. In accordance with the CPNI methodology, the presence of parked, standing, or contrary traffic is ignored to account for variables such as natural hourly and daily periodicity, temporary parking or access restrictions, accomplices effecting traffic control and such like. Further, it is assumed an attacking vehicle will not hesitate to run against road markings and signage to intimidate or confront opposing vehicles. In this regard, the increased conspicuousness and weight of a larger vehicle would be advantageous to the attacker.

Judgements might be made to balance the advantages of steering a course that overruns street furniture and/or over kerbs with the disadvantages of cumulative injury to the vehicle and/or driver which might render a controlled attack unfeasible. However, any such judgement should be discussed and agreed with Network Rail.

Consideration is also given to the considerable planning and resourcing required for a VBIED rather than a VAW attack, including possible actions by accomplices, both preparatory and on-the-day. Preparatory actions in the wider streetscape could include damaging or removing items of street furniture. On-the-day assistance might include actions such as exploiting push button controlled pedestrian crossings or stopping or parking a vehicle at key points to affect a measure of traffic control.

A VDA is carried out primarily as a desktop exercise but should be supported by familiarisation site survey. When interpreting the results, it is prudent to allow for an error of ±5% in quoted speeds. Although the VDA tests for maximum speed to a single measure, clearly in most cases impacts at more oblique angles or at higher speeds are possible at the line of protection. Consequently, the vehicle might be deflected and/or the impact will be to more than one measure.



A direct route allows a hostile vehicle to build up spreed

Indirect approach leads hostile vehicle away from target

Chcanes reduce hostile vehicle approach speed

Removing vehicle access from the front of building minimised potential use of vehicle as a weapon

Chicanes reduce hostile vehicle approach speed

Figure 8.8: Illustration of vehicle dynamics

8.7 Passive Measures

Passive measures covers those HVM measures which are static, and which do not have any moving or operational features. Ideally, all proposed vehicle barriers should have been tested to IWA 14-1 and PAS 68:2013. In circumstances where other design considerations require a more bespoke approach to landscaping design, the advice of a RSES engineer should be sought.

Passive measures on the footways can consist of a mixture of bollards, planters and seating, however, this is only feasible where there is sufficient space in which to install without affecting pedestrian permeability.

Any vehicle security barriers should not restrict pedestrian flow in the area. Where pedestrians are expected to flow through the HVM line, static bollards can be used. Thought should also be given to the prevention of using the vehicle barriers as somewhere to leave litter or place an IED.

The following details the types of passive HVM measures which can be considered for installation around a station. It should be noted that the pros and cons of each type of measure are in relation to their installation around a station.

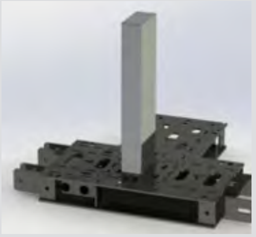
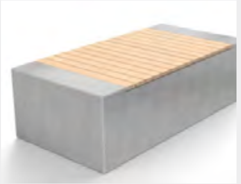
Static Bollards	Many different types of bollards are available with crash-ratings and in a range of styles and finishes. If necessary, they can be removable or automatic. Bollard schemes are designed to protect against vehicles while allowing pedestrians to flow through the secure line. Bollards are likely to be the primary HVM measure in a station protection scheme. Static bollards are typically installed in reinforced concrete foundations.	
Static Bollards (shallow)	Where there is insufficient depth to install reinforced concrete foundations, shallow plate solutions can be deployed. Requiring a much shallower depth than reinforced concrete solutions, shallow plate typically comprise large steel plates into which the bollard is installed.	 
Blocks	Impact tested blocks are very simple protection measures that can be deployed quickly and easily when needed but can also provide a more permanent solution. They are usually surface mounted and require no foundation. They can be incorporated into seating arrangements.	 

Table 8.9: A table with the different types of passive measures used in and around the design of stations, Passive measures have no moving or operational features

8.7 Passive Measures Continued

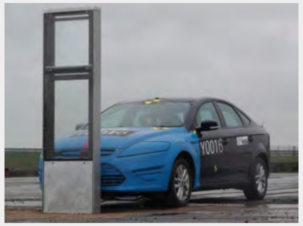
Cycle Hoops	Impact tested cycle hoops provide a usable HVM measure which blend well into the urban environment. They can be based on a standard static bollard or be a tested hoop. See also British Transport Police Cycle Parking Design Guidance	
Signage	Impact tested Wayfinding signage would be suitable for installation at a station.	
Seating	Impact tested seating would be suitable for installation at a station.	
Shelter	Impact tested shelters for bus stops and taxi ranks. Typically, these would be installed within a line of measures including products such as bollards, cycle hoops and other HVM street furniture.	

Table 8.10: A table with the different types of passive measures used in and around the design of stations, Passive measures have no moving or operational features

8.8 Active Measures

Active HVM measures are those which have moving components to provide access. They include gates, blockers, and removable and rising bollards. With the exception of blockers and certain types of gate, they can be operated automatically or manually from a remote or local position.

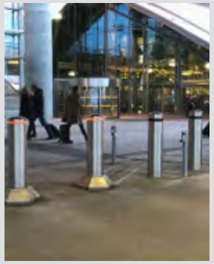
Rising Bollards	Rising bollards can be lowered and raised to allow the passage of vehicles. Typically, they do have substantial deep foundations, in some cases over 2m. They can be raised and lowered manually or automatically from a remote or local position.	
Sliding Bollards	Sliding bollards are an automatic or manually operated solution. The system can be surface mounted or recessed. The system consists of outer static bollards with central sliding ones. When operated the central bollards slide behind the outer static ones. The tracks in which the bollards slide can be seen in this image.	
Manual Rising Bollards	These are raised and lowered vertically by hand and are ideally suited to sites where there are few traffic movements but there is still a requirement for high-security protection. Typically, these bollards can stop a 3,500kg vehicle at 48km/h (30mph)	

Table 8.11: A table with the different types of active measures used in and around the design of stations, Active measures have moving components to provide access

8.8 Active Measures Continued

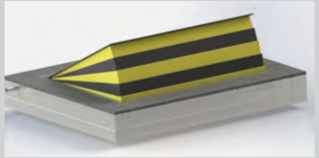
Horizontal Swing Gate	The Lockdown gate has fully removable posts allowing it to be permanently or temporarily deployed. If required, just the closing post or the hanging post could be removed. The gate is specifically designed as a manual gate for openings up to 8m.	
Rising Arm Barrier	The figure opposite shows a basic proprietary rising arm barrier which has been impact tested. The barrier is manually operated. These are cost effective and relatively simple to install. Automatic rising arm barriers are also available.	
Bi-fold Gate	Bi-fold gates have a clear opening of up to 4.2m and can be manufactured for heights up to 5m. They are hydraulically driven with a bespoke power pack and cylinder producing a smooth quiet operation with few moving parts.	
Blockers	Blockers provide an effective HVM measure. They have good performance against high impact speeds for a range of vehicles.	

Table 8.12: A table with the different types of active measures used in and around the design of stations, Active measures have moving components to provide access

8.9 Hard Landscaping and Bespoke HVM Features

Where it is determined, in agreement with the station security stakeholders, that bespoke HVM measures are to be developed as part of the protective line, this is acceptable so long as the residual risk associated with the use of non-proven (by test) measures are understood and accepted by the station risk owner. Any such bespoke design should be undertaken by the appointed RSES Engineer and would, ideally, be validated through full scale testing. However, this may not always be feasible within project constraints.

Hard landscaping can be applied as an HVM measure in those areas where there is sufficient space to provide the necessary features. It has the benefit of being an unobtrusive measure which can blend into its surroundings. Such features can include:

→ Reinforced concrete knee walls
→ Bespoke planting
→ Reinforced concrete seating
→ Significant level changes
→ Berms (designed in accordance with CPNI guidance)
→ Ditches (designed in accordance with CPNI guidance)

Crucially, the following should not be used as HVM measures, unless they have been proven through testing to be effective.

→ Trees and other planting
→ Security fences (unless specified as HVM rated fences)
→ Stairs
→ Narrow ditches or 'moats'.
→ Shallow water features

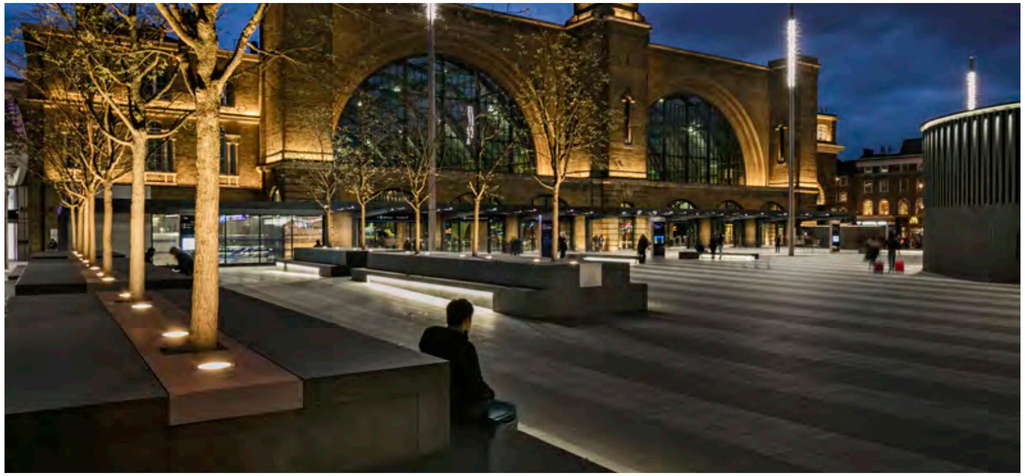


Image 8.13: Concrete seating outside King's Cross station

Image 8.14: Shallow water features outside Sheffield Park Hill station

8.10 Design & Installation Considerations of HVM Measures

The installation of HVM measures is rarely straightforward. Careful planning and investigative works are implimented beforehand to attempt a cost effective, timely and successful implementation of an HVM scheme. Frequently, those responsible for the design and management of an HVM project do not appreciate the significant costs over and above the initial purchase fee of the equipment. These additional costs typically include planning applications, utilities searches, legal fees, topographical and ground penetrating radar surveys, trial holes and detailed installation drawings. Where vehicle access barriers are to be deployed, consideration should be given as to how they are to be operated and monitored. It may be necessary to install CCTV if the barrier is to be remotely operated. Measures may also need to be integrated into existing traffic management systems.

NR Guidance Suite Reference

Network Rail Station Capacity Planning Design Manual. NR/GN/CIV/100/03

Land ownership is also a major consideration. It is often the case that public realm spaces around stations are not owned by Network Rail. This can include forecourts, footways and roads. Whilst the installation of HVM measures around a station provides protection against vehicular attack, it is not always the case the other landowners will agree to having such measures installed on their land in order to facilitate this. When considering the locations for HVM measures the land ownership where the proposed products are to be installed should be confirmed. Once determined, permissions should be sought from the landowner before any HVM measures are installed. It is worth noting that even if the land is owned by the local council, it cannot be assumed that permissions will be given to install HVM measures. The design may be restricted to having protection much closer to the station than preferable, solely due to the extent of Network Rail owned land around the station.

Image 8.15: Public Realm King's Cross station

Station Approaches

8.11 Services

Buried services are commonplace underneath the roads and streets of the United Kingdom. Typically, these services include water and sewage mains, surface water drainage, electricity, gas and telecommunications. The depth of services below ground level varies considerably and can range from 100mm to more than several metres. It is therefore inevitable that clashes will occur between the foundations for HVM measures and existing services. These can be overcome in several ways. Knowing the exact depth and location of the services will allow the measures to be carefully positioned to minimise or reduce any potential clash. Where this cannot be achieved, it is possible to modify the foundation to suit. However, the design of such modifications can only be undertaken by a suitably qualified professional engineer.

It may be necessary to carry out calculations to prove that the modified foundation will still perform to its tested or design level. It is possible to have services running through reinforced concrete foundations for HVM measures in split ducts. It is important to note that in such circumstances the rebar for the foundation should not be compromised.

In the first instance the location of the services should be determined wherever possible. Information can be requested from the utilities providers. However, whilst these searches provide useful information, they do not always detail the exact location of the service, but rather indicate their presence within the road or footway.

Image 8.16 and Image 8.17 show typical services and clearly illustrate how they could impact on the installation of a foundation for an HVM measure.

Image 8.16: Location services

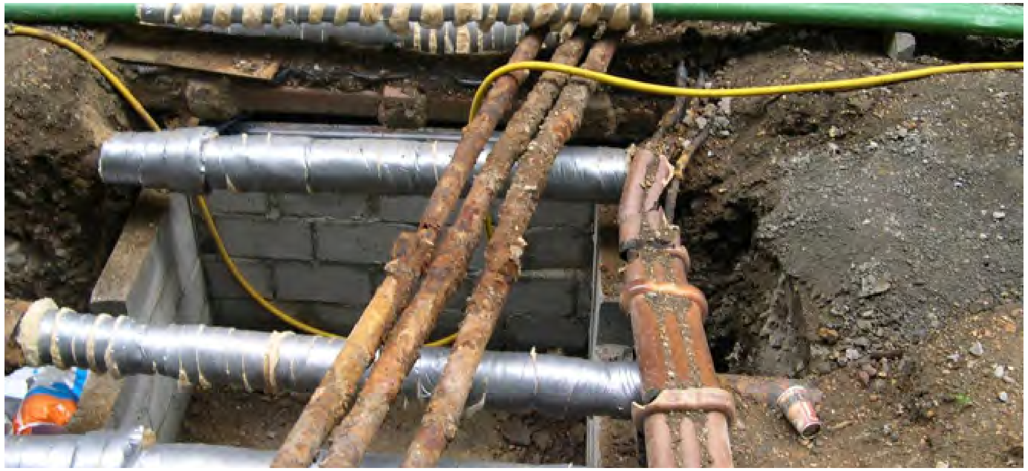


Image 8.17: Location services impact

8.12 Trial Holes

Prior to the installation of HVM measures in accordance with an agreed design, trial holes should be dug. Specific locations are identified where existing services or underground obstructions are thought to exist. By confirming the existence of such obstructions, trial holes are used to validate the design of an HVM scheme. Their sole purpose is to identify below-ground obstructions before construction begins. They will typically verify the existing services and utilities drawings.

By identifying the presence of any obstructions, the appropriate design modifications to the scheme can be carried out prior to installation. For example, it may be necessary to re-engineer the foundations for the HVM measures prior to starting on site. Knowing the exact location of obstructions helps to reduce construction risk.

In historic locations it is often common practice to dig a trial hole in the presence of an archaeologist. Should anything of historical importance be discovered this may necessitate stopping the installation of the works or at least delaying it whilst further site investigations are carried out. An archaeologist is shown at work in a trial hole in Image 8.18.

Correct recording of trial hole details is essential. The exact location of the trial hole should be determined and noted. The location of the trial pit should be provided by the scheme designer on a drawing. Measurements should be taken of the location and depth of any discovered services along with their use such as water or gas. Photographs should be taken for reference. The make-up of the ground conditions should also be documented. On completion of a trial hole the area should be reinstated to the same standard as that prior to the excavation.

Image 8.18: Trial holes

8.13 Topographical & Ground Penetrating Radar Survey

In order to undertake the detailed design of an agreed HVM scheme, drawings should be produced detailing the location, setting out dimensions and foundations, including reinforcement information where applicable. The installation of any HVM measures should take into account the topography of the installation location. For example, if there are falls in the vicinity of the location the foundation for the measure should take account of this. The fall may result in varying thicknesses of finishes over the foundation. If bollards are to be installed, bespoke lengths may be required to compensate for the variation in ground levels. When installing gates, it is important to consider varying ground levels to check that large gaps under booms are not produced. Not only will this have an impact on the tested performance of the gate it may render it impractical to operate.

2D Surveys are used for base plans for setting out measures.

To assist the designer topographical drawings of the installation location should be provided and, if not available, topographical surveys should be undertaken to provide the required details. Costs for such services should be allowed for any design.

Ground penetrating radar surveys can be carried out to help detect and determine the location of existing services. Whilst these surveys are a valuable tool in determining the presence and location of existing services, trial holes should still be dug to confirm their existence.

Images 8.19: Network Rail worker undertaking a radar survey

8.14 Drainage, Planning, and Detailed Design

8.14.1 Drainage

Some HVM measures such as rising bollards and blockers require drainage connections. The build-up of water within the structure of the product will result ultimately in the failure of the measure leading to lengthy repair or replacement. Downtime of the measure due to insufficient drainage might result in the location being unprotected and vulnerable. Difficulties often exist in finding suitable gravity drainage, hence sump pumps might be required necessitating power supplies and controls.

8.14.2 Planning

Costs associated with planning should also be taken into consideration. City centre locations, especially those in historic areas will require lengthy planning and approvals permissions. Local residents might object to the installation of measures in their neighbourhoods resulting in delays to a project.

8.14.3 Detailed Design

Once all the necessary surveys and approvals have been completed the detailed design for the installation of the measures can commence. The drawings should be of a suitable standard such that a competent contractor can procure and install the measures to provide a compliant solution. The detailed design drawings should show general arrangements, elevations and sections along with concrete reinforcement details where required.

8.15 Exterior Technology

In those areas where vehicular access is required it is important to have systems and procedures which only permit admittance for authorised vehicles.

Large public spaces such as station forecourts typically require operational procedures and the physical presence of station staff to lower HVM measures to allow vehicles to access the area. These vehicles are generally for maintenance or emergency reasons. Given the close proximity of the public, station staff should determine if it is safe for a vehicle to enter the area and when it does act as a traffic marshall to check the safety of those in the area. A vehicle requiring access may be required to notify the station prior to any visit and provide details of the vehicle and its occupants. On arrival it should report to station management and follow their instructions and procedures when entering the restricted area. HVM measures in public spaces may be operated locally by manual or electrical means. They can also be operated remotely from a control room once confirmation of vehicular access has been given by the station staff. Service entrances, which are generally located away from the public, can utilise more automated systems. For example, an entrance for delivery vehicles at the rear of a station may have a call point linked to a station security control room. The HVM measure may be operated remotely if the station staff are satisfied as to the legitimacy of the vehicle entering the premises. A visitor notification system may be adopted so that access permission is granted, and the station are aware of the vehicle's arrival beforehand.

However, it is essential that on arrival any vehicle is checked that it is legitimate and authorised to enter the site. This may be by someone physically checking the vehicle or by CCTV.

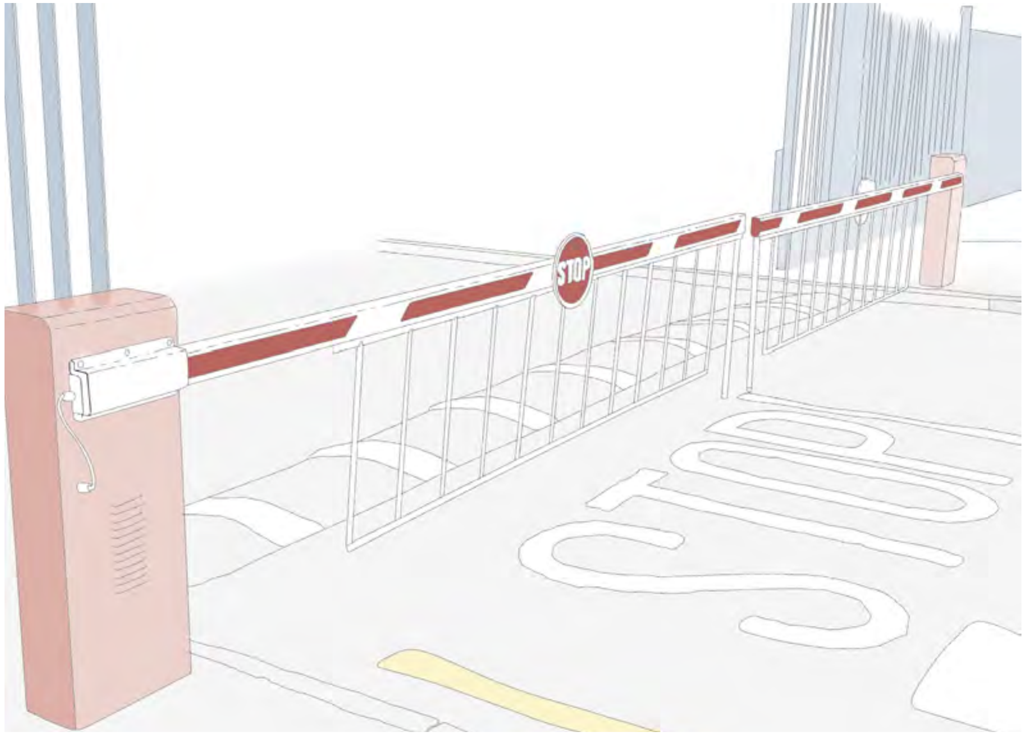


Figure 8.20: Illustration of exterior gate technology

Code of Practice Guidance

Security In the Design Of Stations Guidance (SIDOS)

National Standard

National Railway Security Programme (NRSP) Section 7 Annex M

8.16 Station Fencing

The need to secure and enclose stations does not mean that boundaries should look intimidating. The old fashioned use of Palisade fencing should therefore be avoided and alternatives are described in Appendix C.

Fencing will often be required at stations for various purposes. These might include:

→ To demarcate boundaries

→ To protect the station perimeter (from trespass or otherwise)

→ To protect key assets (such as plant equipment)

The materiality, height and security rating of fencing will vary depending on the purpose of the fencing, the asset or area it is protecting and the type of threat perceived likely in the threat and vulnerability risk assessment (TVRA). The design criteria for fencing should be discussed and agreed with the Network Rail project team in advance of detailed design taking place.

As well as security considerations, fencing design may be influenced by heritage and planning considerations. Where these conflict with security requirements, this should be raised to the Network Rail Security Team for resolution on a case-by-case basis.Whilst meeting the necessary performance requirements, fencing should also aspire to follow the principles of Crime Prevention Through Environmental Design (CPTED). Fencing should not inhibit opportunities for natural surveillance, by obstructing sight lines, nor should it create a maintenance burden or opportunity for vandalism or litter build-up. In some cases, territorial reinforcement, such as land banking or planting, might serve as alternatives to fencing, similarly bollards may also offer the required protection whilst maintaining natural access control.

The creation of dark alleyways and dark enclosed fenced areas (such as bicycle stores and equipment areas) should be avoided, and appropriate lighting proposed in all types of fencing scenarios. See Rail Industry Standard for Lighting at Stations, RISS-7702 and Lighting Planning, BS EN 12464-1 for further information on this, as well as guidance papers prepared by the British Transport Police (BTP).

Image 8.21: Aesthetic fencing security examples to reduce visibility of contents

Image 8.22:Fencing to secure a track

Image 8.23: Fencing where the object is still visible

Security at Stations Design Guide Manual

Integration Requirements

9

Image 9.1
London Paddington Station
Platform

9.1 Design Integration

It is crucial that security design measures are integrated in to the wider design of a station project.

Design integration might simply involve checking that there are appropriate new power supplies or structural elements in place for new security measures – on a less tangible level, security design measures should also be integrated in to the architectural design of a station project. This might mean careful integration of new CCTV systems in to new cladding or signage banding, or might mean carefully matching the colour, pattern or style of security measures to either existing or proposed architectural design items in the vicinity.

Crucially, new security design interventions should not feel like late additions or 'add-ons'.
Successful design integration offers many benefits beyond the aesthetic: integrating measures into the wider vernacular might hone their effectiveness – technological interventions might become less obvious and therefore less susceptible to hostile reconnaissance if integrated into context. HVM measures posing as street furniture add an extra layer of usefulness, bringing about added social value beyond the sum of their parts.

Similarly, it is crucial that the overarching security strategy for a station project is integrated with the strategies proposed by other designers and stakeholders. This might include integrating the security strategy with the fire strategy, diversity impact assessment or human factors (ergonomics) strategy or discussing the security strategy with the station operator, such that it can be implemented by the end user team.

Refer also to NR/GN/CIV/100/01 for guidance on the Design Advice Panel who can help with integrating designs generally, as may be required.

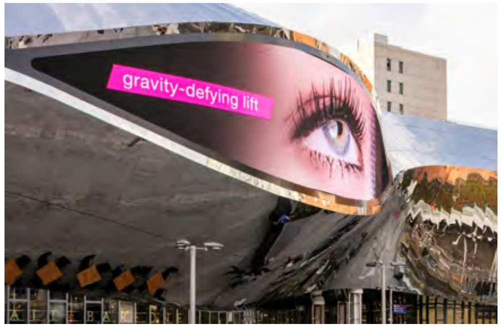


Image 9.2: Birmingham New Street station

Image 9.3 Internal concourse of London Bridge station

Image 9.4: Design review discussion

9.2 Technical Integration

In a managed environment most electronic security systems are provided to support human operators in the provision of security. People provide the security function, and the systems provide the tools to do more with either the same or fewer people.

This is especially the case in an environment where security is monitored and managed 24/7 but applies also to lock and leave premises where electronic systems (intruder detection, CCTV etc.) provide real time alerts and post event evidence.

Integration between systems maximises the benefits of each system to operators. In this context the "operators" are the human users of the system who work with the systems to deliver the security function.
It is recognised that in the future computers and artificial intelligence (AI) might take over some or all of the human operators' functions. It is expected that as this technology develops the systems will still require integration in order to maximise the advantages to the AI users.

At the most basic level, integration is based on cause and effect events. The purpose of the security systems is to support users in the security decision making process. The purpose of integration is to automate processes to make the support to the users more efficient and effective.

In terms of assisting users in the security decision making process, the majority of work involves security "incidents" and the tasks the systems users have to undertake involve categorising the incident and making decisions regarding an appropriate response to any given incident. The nature of the incident can be anything from apparent affray or disorder on a station platform or concourse to attempts to intrude into back of house, service or utility areas.

The CCTV system is probably the most useful tool available to the system operator. The operator will use the CCTV system to examine events of concern and make decisions on whether a response or intervention is required and if so the nature of the response/intervention and what priority should be applied. Accordingly, any system that provides notification of an "event" should be considered as a source to act on the CCTV cameras being presented to an operator/user.

In terms of security systems there are a number of typical systems including:

- → Video Surveillance Systems (VSS) and Closed Circuit Television (CCTV) systems. For the purposes of this guide these are the same.
- → Electronic (Automatic) Access Control
- → Intruder Detection and Intruder Alarm systems
- → Intercom Systems

Integration of these systems could take a number of forms. Consideration should be given to the factors noted in the following page.

9.2 Technical Integration Continued

9.2.1 Product/Vendor family integration

All the systems are from the same manufacturer. All systems work together and are wholly integrated.

Advantages	Disadvantages
Simpler to integrate systems from one supplier	Beholden to one supplier - failures and issues affect all systems
Single vendor may provide better costing	Potential to limit options - Options are only those available from the single system
Single support channels	Patching, service and maintenance - whole system potentially affected
Single product training	Whole life costs may be higher (no options to change, no competition (without major disruption)).

There are many options for integration between security systems and there are advantages and disadvantages of each option. The scale and complexity of the security system, existing arrangements, ongoing budgets plus level of resilience required will shape this decision and inform the best method for integrating technological security systems. For example, if a project proposes new assets to be added to an existing system, the existing integration methodology could be the one to follow. If a project has a lower capital expenditure budget (CAPEX) then separate systems with one identified integrator may be the most suitable option

9.2.2 Optionally different systems with an overarching integration system

All systems are separate, potentially from different vendors/ manufacturers and are integrated using a further integration system (often referred to as a Security Management System (SMS) or a Physical Security Information Management (System) ((PSIM)).

Advantages	Disadvantages
- Maximises options - Each system can be selected on its own merits	- CAPEX Cost - The additional layer adds additional cost
Unified training on the primary interface	- OPEX Cost - Drivers or connectors might need to be updated when subsystems change. This might incur costs
Each system, including the master can be managed separately	- "Integration" can only deliver some of the functions of the child/subsystems - Other elements have to be executed directly
Potential for increased integration with third party sources	

9.2.3 Separate systems with one designated as the integrator

All systems are separate, potentially from different vendors/ manufacturers but one system is designated master and all other systems are connected as child systems to the master.

Advantages	Disadvantages
- Reduced upfront costs. - Different systems and products can be selected.	- Operational costs might be higher due to different maintenance, testing and monitoring requirements.
-Potential for increased resilience -Each system can stand alone.	- Individual training - Subject to the level and type of integration training may be required on each
- Simple - Might allow options for different maintenance and support approaches.	

Table 9.5: Tables showing the advantages and disadvantages of the different types of technical integration

Image 9.6
Kings Cross Station

10

Security at Stations Design Guide Manual

Retail Generally

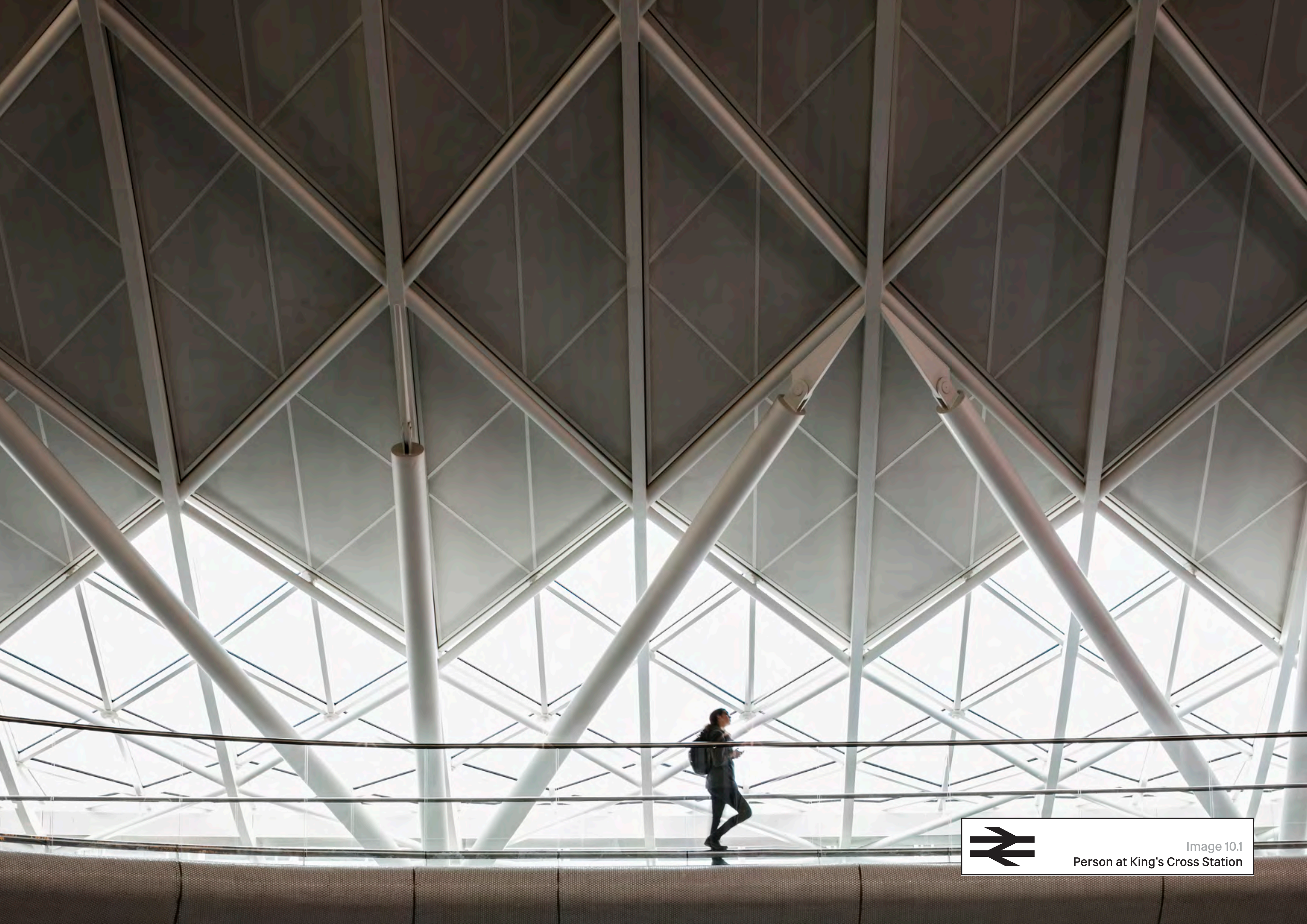


Image 10.1
Person at King’s Cross Station

10.1 Physical Retail Security

10.1.1 Retail Security Definition

Retail security is the responsibility of each retail tenant, operator or owner. Guidance set out in Security in the Design of Stations (SIDOS) applies to retail projects, as do the requirements within NRSP.

10.1.2 Physical Security

The physical security of each retail unit should be considered during the design of a Station or of its retail units.

Where retail units adjoin each other, the separating walls should delay forced intrusion between units. Where retail units adjoin Network Rail assets the walls separating should delay forced intrusion in either direction.

Retail units frequently include back of house areas for deliveries and servicing. These areas should be kept physically secure from unauthorised access. Doors leading from common back of house service areas are to be secured against physical intrusion. Clear lines of sight, the use of robust materials and fixings should be deployed in all cases.

10.1.3 Retail Façades and Glazing

Special blast resilient characteristics apply to retail, which are detailed within appendix C. Typically the façade is designed in accordance with a specific retailer requirements. However the following should be considered:

Retail units could represent a place of relative safety in the event of (for example):

- → A fire or emergency on the concourse or in an adjacent public domain
- → A marauding terrorist weapons attack (MTWA)

The Network Rail Security Team will advise on specific requirements to create safe refuge points within retail units, should this be relevant to a specific project.

NR Guidance Suite Reference

Network Rail Retail Design Guide Manual for Stations NR/GN/CIV/200/06

Image 10.2: Kings Cross Station retail shops

10.2 Technological Retail Security

Typically, the technical security systems (CCTV, Intruder Detection, Control of Access) and the Fire Alarm and Detection system of an individual retail unit are the responsibility of the retailer.

There should, however, be an option allowed in the Station systems design, to monitor the status of any alarm systems installed at each retail unit within or directly connected to a Station.

No liability for monitoring or responding to alarms is implied, but for situational awareness of assets within a Station it is useful for Station Control (locally or remotely) to have signals from each retail unit system (where fitted) to report:

- → Fire Alarm activation
- → Intruder Alarm
- → Set/Unset
- → Alarm activation

This will allow Station Control to be aware of the impending attendance by either the retail unit keyholder and/or the relevant emergency service.

For a station that is closed or for a station that is running skeleton night- time staff levels this allows for a response plan to dedicate an entry point at which to meet the keyholder and emergency services with an escorted route to the retail unit in question. For compliance with Data Protection/GDPR legislation the retail unit CCTV system should be standalone (or part of a wider retail company CCTV system). However, common areas, back of house service corridors, loading bays and similar areas are typically considered part of the Station and should be provided with CCTV surveillance as part of the overall Station CCTV system.

Similarly, there should be no direct sharing of Station CCTV cameras with any retail unit. If a retail unit requires surveillance of a common area this is normally acceptable but is provided through one or more additional cameras installed in the common area and connected to the specific retail unit CCTV system.

Code of Practice Guidance

British Transport Police Retail Crime Design Guide

Image 10.3: Glasgow Central railway station

10.3 Left Luggage and Lost Property

Projects are advised that there are specific security requirements to consider when Lost Property and Left Luggage Facilities are required.

These include siting this type of facility in close proximity to the station perimeter (or near an exit point), provision of specialist security scanning equipment and provision of security search areas for baggage and lost property.

National Standard

National Railways Security Programme (NRSP)

Image 10.4:: Left luggage area at Paddingotn station

Image 10.5: A scanner to inspect the safety of luggage left unattended

Image 10.6
King's Cross Station

11

Security at Stations Design Guide Manual

Emergency Evacuation and Signage

11.1 Emergency Evacuation

It is crucial that in an emergency scenario stations can be evacuated safely. This applies to a fire scenario, security event or other type of emergency which might require the station to be vacated swiftly.

Physical and technological security measures should support an evacuation. This includes doors opening to facilitate escapees, public address systems and sounders being used to announce the need for evacuation and clear signage to direct escapees to a place of relative safety.

The governing legislation for emergency evacuations can be attributed mostly to Fire Engineering Standards, chiefly BS9999 and BS9992.

Following these Standards will contribute towards creating safe station emergency evacuation strategies suited to security evacuations as well as fire and other scenarios.

NR Guidance Suite Reference
NR Wayfinding Design Guide NR/GN/CIV/300/01

NR Guidance Suite Reference
NR Station Capacity Planning Guide NR/GN/CIV/100/03

Standards Reference
Approved Document B - Fire Safety BS9999 - Fire Safety in Rail Infrastructure BS9992 - Fire Safety in Buildings

Image 11.1: King's Cross station busy platform

11.2 Signage

Signage should be installed in all stations to suit various purposes. These include:

- To provide wayfinding
- To provide key station and train information
- To provide emergency evacuation information
- To provide key security messages

NRSP requires that security messages are displayed at all stations. This might take the form of static signage, such as large format posters, or as powered dynamic signage.

The location of security signage should be prominent to passengers and sited near entrances to stations, on concourses, platforms or in waiting spaces.

Security signage graphics can be obtained from the Department for Transport (DfT), BTP and other security stakeholders. Security campaigns will change over time so projects should consider how easy it is to change and update security signage either digitally or manually.

SEE IT.
SAY IT.
SORTED.
Have they left a bag unattended?
Speak to staff. For police, text 61016 or call 0800 405040.
We'll sort it.
SEE IT.
SAY IT.
SORTED.
Are they checking security?
Speak to staff. For police, text 61016 or call 0800 405040.
We'll sort it.
SEE IT.
SAY IT.
SORTED.
No Entry
Are they somewhere they shouldn't be?
Speak to staff. For police, text 61016 or call 0800 405040.
We'll sort it.
Chiltern Railways
Together, we've got it covered
BRITISH TRANSPORT POLICE

Image 11.2: British Transport Police (BTP) See it. Say it. Sorted. campaign poster

Image 11.3: 'Small actions, Big consequences' CPNI campaign poster

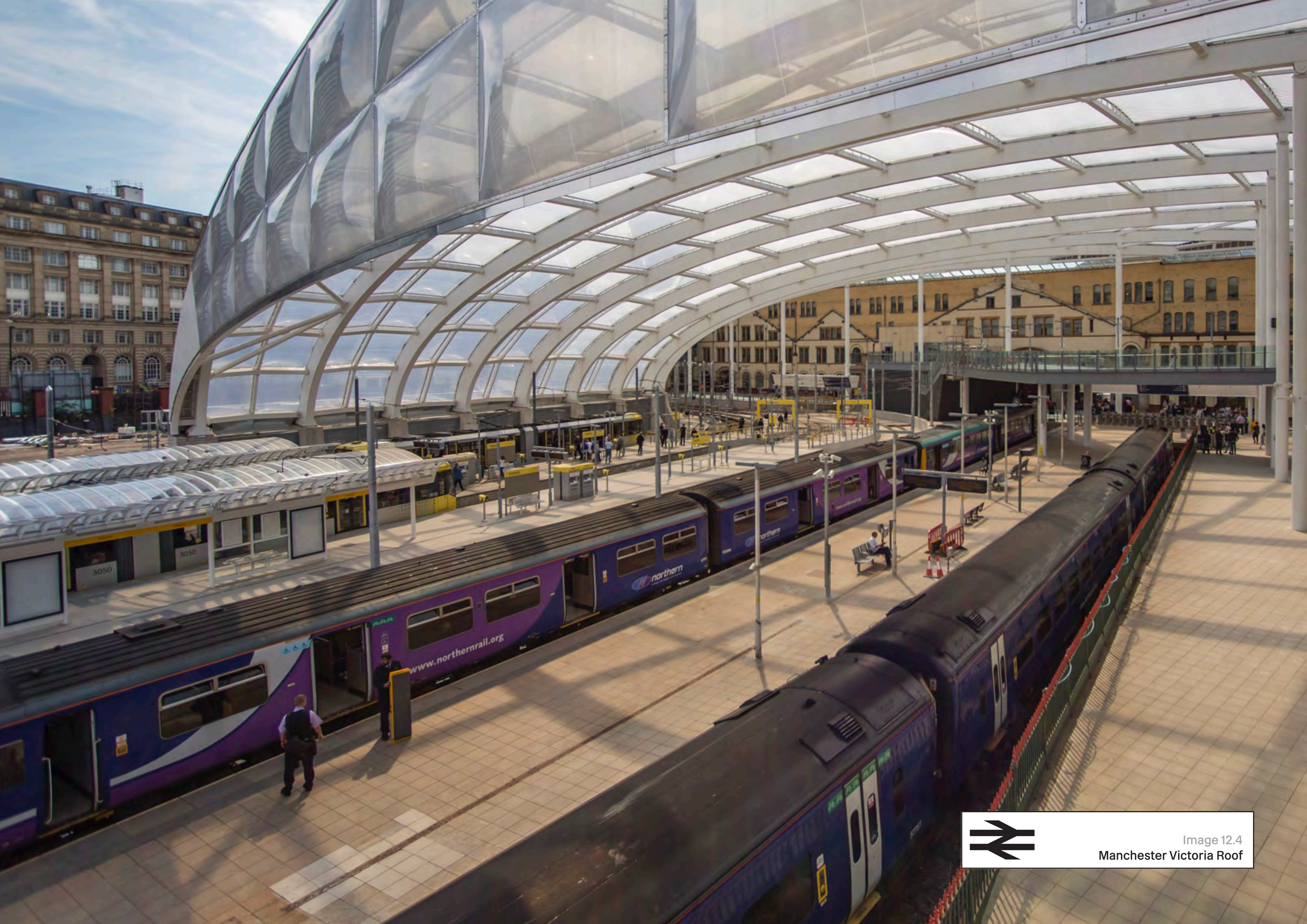


Image 12.4

Manchester Victoria Roof

12

Security at Stations Design Guide Manual

Control Rooms

12.1 Control Room Introduction

12.1.1 Overview

It is unlikely that a station will have a control room dedicated to “security”. It is more likely that a station will have an operational control room, which will perform all operational functions including security. Accordingly this guidance should be applied to the Operational Control Room as well as to any security control room should the latter be required at a Station or for any specific project.

12.1.2 Criticality

The Operational Control Room should be considered a high value asset. Compromise of any part of the Operational Control Room will significantly affect the operation of a station, either from a service provision or a security perspective. Accordingly, the Operational Control Room should be considered a highly critical asset and should be suitably protected at all times.

The Operational Control Room should be located:

→ As far from any likely or identifiable threat sources as possible.
→ To facilitate ease of arrival and departure, specifically during security or operational incidents.
→ Access to and from the operational control room should not be hindered by large scale evacuations.
→ Access to and from the operational control room should continue in the aftermath of a significant event such as a terrorist attack.

The operational control room should be located away from public pedestrian and vehicle access routes and should be protected from the very events that the control room will be needed to manage and control.

12.1.3 Space Allowances

The operational control room should be designed to accommodate a population commensurate with an emergency response.

Normally, unless other arrangements are in place, the operational control room is the place senior decision makers will gravitate to when there is a crisis that needs managing.

As a result, the population of the operational control room can expand significantly and given this expansion in numbers is the result of an emergency it is likely that the atmosphere will be or will become highly charged. Accordingly allow space of not less that 12m^2 per person for normal running with a further space for a temporary increase in population of 50% of normal running.

Normal Running	Space at 12 m2	Plus 50%	Total Space
10 People	120 m2	60 m2	180 m2
6 People	72 m2	36 m2	108 m2

Image 12.2: Example of space allowances table

12.1.4 Crisis Management Suite

An alternative to providing additional space within an operational control room is to provide an adjoining space to act as a crisis management suite.

The crisis management suite could be multi purpose, for example a meeting or conference room but should be able to be switched into an operational crisis management suite both at a moment’s notice and without any delay in reconfiguration.

Code of Practice Guidance

Centre for Protection of National Infrastructure (CPNI) Control Room Guidance

12.1 Control Room Introduction Continued

12.1.5 Welfare Facillities

The Operational Control Room is likely to be functional 24/7. The Operational Control Room should include integrated and adjoining welfare facilities suitable for the highest expected population (the crisis or emergency population) to include:

- → Toilets
- → Rest area
- → Kitchen/kitchenette, food storage/reheat and eating

Staff working within the control room (or the crisis management suite) should not have to leave the physical security boundary of the area to use the welfare facilities.

12.1.6 Physical Security

The whole operational control facility (including a crisis management suite) if provided and the welfare facilities should be physically secured against forced intrusion/attack.

The operational control room would be a primary target for attack for the purpose of disruption of services and should be physically secure.

The facility should be behind not less than 3 physically secure lines (LPS 1175 C5 SR3 minimum) with the final security to the control facility being LPS 1175 D5(SR4) barriers.

Entry to the operational control room should be via an interlocked entry (two doors interlocked together or a single “portal” type entry system).

Arrangements should be made for the entry of large items of equipment (such as computer racks and similar) whilst preserving physical security. The walls and any services penetrations should be to the same level.

The primary control room will not normally include any windows. If windows are required:

- → Provide suitable forced entry protection
- → Check location and orientation in relation to rising and setting sun does not create glare onto any monitors

Where there is a requirement for direct oversight of an operational area this is likely best served through a secondary monitoring location as opposed to from the primary operational control room.

Not only would having direct oversight put the monitoring position in close proximity to a possible security related event, the protective engineering required would incur significant unnecessary costs.

12.1.7 Control of Access

Control of access to a highly critical working space such as an Operational Control room will likely take one of four forms:

- → Access only through High Security Electronic Access control with not less than dual factor authentication
- → Permitted access through intercom systems
- → Users call to request/be given access
- → Operators within the Control Room manually check authorities and manually grant access.

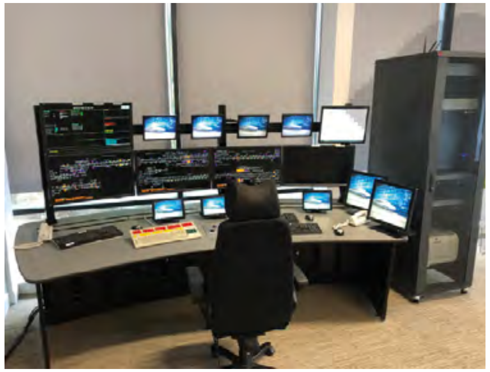


Image 12.3: Control Room desk example

12.2 Escape, Wayfinding, and Services

12.2.1 Emergency Escape

Ideally escape doors will be avoided, however, where mandated through emergency evacuation travel distances or similar should be:

- → Lobbied
- → Clean faced on the attack side (no locks, cylinders, signs etc)
- → Be status monitored for
- → Door position (close protection (closed/not closed))
- → Lock Status (close protection)
- → Local alarm sounders (if opened)
- → Supressed during a fire evacuation

Image 12.4: Push button

Image 12.5: Fire door

12.2.2 Wayfinding

The location of the operational control room/facility should not be obvious and should not be signposted. Anyone who needs to access the operational control room will know where it is and how to get to it without signs

Anyone authorised to visit should be escorted/hosted and therefore will be taken to and from the operational control room.

No purpose is served by marking the door to the operational control room with its function or in signposting routes to the operational control room.

12.2.3 Services

Services, including but not limited to:

- → Environmental Conditioning
- → Electrical Power
- → Communications
- → Water (potable)
- → Foul

Should be designed to be resilient against all the threats that could apply to the control room itself. Foul services are often overlooked. The control room will soon cease operating if the toilets are blocked as an act of sabotage.

Electrical power and environmental conditioning should be sized for the total expected population (during crisis management mode). Environmental conditioning systems should take account of the heat load of all the people in a highly charged and fast paced emergency condition plus the heat output of all the systems, including additional systems that the Emergency Services and First responders may bring in the event of an emergency/crisis.

All electrical power for critical services should be from essential supplies, continuous and uninterruptable.
There should be a facility to bring a suitable whole load generator into use (either on site ready to run or brought in). If brought in protected facilities should exist for location and electrical connections.

Autonomy periods for continuous uninterruptable supplies should be set to exceed the longest time period to either resolve any grid supply issues or to bring to site and run up to full power any external generator supply. Where generators are used suitable arrangements should be made for the secure fuel replenishment. Fuel stores should not become a target for attack.

Fresh air supplies should be secured against both indirect attack (attacking of the air supply, deliberate introduction of contaminants, accelerants or noxious/poisonous chemicals) and as a potential route into the building and or the secure control room. Exhaust ducts should be similar arranged so as to be inaccessible and physically protected.

12.3 Control Room Considerations

12.3.1 Equipment Room

Typically operational equipment critical to the function of the operational control room should be physically secured to the same standards as that of the control room itself.

Ideally access to the core technical equipment should be through or controlled from within the Operational Control Room. In this way, no one can gain physical access to the critical equipment room without staff working in the control room being aware. This is not the same as relying on rights and permissions of access to the critical space – the arrangement is for physical oversight of access, on top of permissions.

12.3.2 Fire

The operational control facility (including all routes to and from) should be highly resistant to fire and smoke. The operational security control room should represent a safe haven in the event of a widespread fire or significant terrorist event (such as a bomb blast) or security related event. While life safety takes precedence over security, the operational control facility should be the last place to be evacuated and should be a primary safe haven.

The rooms should be constructed to resist the spread of fire for a considerable period of time (hours) and all routes to and from surrounding areas should have a low or very low fire load. Water and mist fire extinguishing systems should be considered to approaches to and escape routes from the control room facility, including in spaces below and above the control facility (where applicable).

12.3.3 CCTV/VSS Monitoring Positions

CCTV/VSS monitoring as part of the general functions of an operational control room should be located in a dedicated area. Desks/workstations should include:

- Not less than 3 number 24" HD or 4K desk monitors arranged:
- Active/interactive primary CCTV monitor
- Alarm and alert information, CCTV mosaic display
- Business purposes: Emails, Reports, News feed, etc.
- Hardware CCTV control joystick
- Mouse and Keyboard
- Keyboard Video Mouse (KVM) switch is required
- Space for note taking (hand written notes remain useful during a fast paced event)
- Task lighting to facilitate note taking or reading of documents without disturbing adjacent operators.
- Space for:
  - Personal mobile radio handsets,
  - Intercoms (where required),
  - Manual gate or active HVM controls
  - Books, binders and reference material

Desk design is important to account for human factors and usability. Surfaces should be durable and easy to clean. Associated computer and electronic equipment will generate significant heat gain. If enclosed within the desk (often located within the desk base or adjacent pedestals) suitable forced air movement and or cooling will be required. Note, venting heat output from the equipment enclosed in a confined space over or across the user's legs should be avoided.

Desk design should account for all users and should therefore be adjustable for height and reach. Monitor (and similar) mounts should allow for adjustments to height (rise and fall) and angle (tilt and turn).

Image 12.6 Fire exit sign example

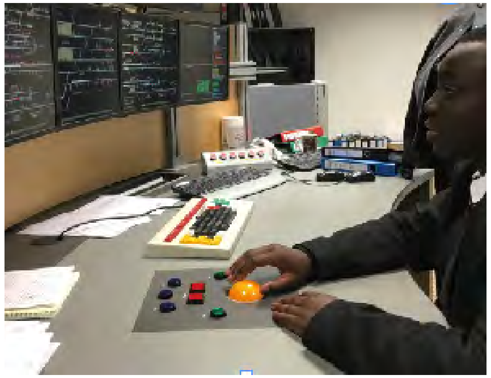


Image 12.7 Control room desk

12.4 Space Allocation

The numbers of workstation/desk positions should be assessed according to the number of cameras and associated activity to be monitored.

Assuming human operators, a person can only concentrate or focus on one CCTV image at a time but may be expected to monitor multiple cameras. There is no specific metric that defines the numbers of cameras a single operator should be responsible for monitoring, however CPNI have provided guidance (CPNI Control Rooms Guidance Dec 2016), The Surveillance Camera Commissioner's code of practice and CCTV User Group should also be consulted for best practice advice.

The number of cameras that can be monitored depends on the scene of each camera (busy scenes need more attention) and whether the camera is fixed or otherwise. The number of cameras to be monitored will also depend on what other duties or time constraints an operator has.

Typically the monitoring of a CCTV system under normal conditions requires intensive focus which cannot be sustained indefinitely.

CCTV monitoring positions should be configured to support absences for work breaks, shift changes etc. while at the same time being able to cater for emergency monitoring situations A three-desk arrangement is likely to be the minimum for most systems of up to 200 cameras, with two desks being dedicated to CCTV monitoring (allowing one operator to take a break or to cater for shift changes) with the third desk being for supervisor duties but able to take over full monitoring duties where necessary. Such an arrangement also allows for continued monitoring during engineering interventions

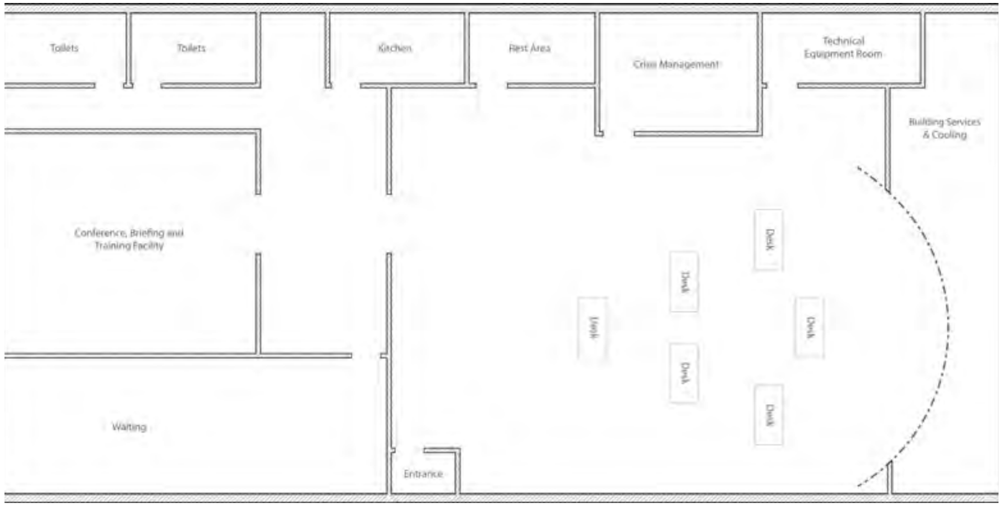


Image 12.8: Example layout of a control room

12.5 CCTV Monitoring Area

The CCTV monitoring area of an active operational control room should focus on the welfare and wellbeing of the operators. The Display Screen Equipment Regulations will apply to the designs, both of the desks and the environment in which the desks sit.

Typically, the area for CCTV surveillance should be kept quiet and free from external disturbances. The internal environment should be suitably lit to avoid creating glare onto or reflection off the screens.

In accordance with Principle (f): Integrity and confidentiality (security) of the Data Protection Act 2018 only people who have a right and an authorised purpose to view CCTV images should be able to do so. This implies a segregated area within the Operation Control Room for CCTV monitoring unless everyone within the Operational Control Room is authorised to view CCTV images.

The environment within the CCTV viewing area should be free from services such as pipes, cables and ducts that could affect the operations of the system. For example: an air conditioning duct running across the ceiling above the CCTV system could introduce distracting noise or could create distracting reflections if made of shiny metal (such as galvanised steel or untreated aluminium) or: a foul waste-water pipe which will also create distracting noises and would cause significant damage and system loss if leaking or ruptured. It is good practise to provide a dedicated area for the review of CCTV.

Individuals have a right to request to see CCTV images of themselves (Subject Access Rights) and it is not appropriate or suitable to take someone to the Operational Control Room for this purpose.

Similarly, for CCTV systems not connected to emergency services the Police and others might require evidence from the system. Similarly it might not be appropriate to review evidence in a busy Operational Control room or to distract operators from normal monitoring duties. Accordingly, a provision should be made for a replay suite, located away from the Operational Control Room.

Design teams should work with station teams to check CCTV cameras are placed/pointing toward areas of high risk of crime, Anti-Social Behaviour and safety risks (Station colleagues will hold knowledge of their individual hotspot locations and issues). Input, collaboration and regular review at local level can help check CCTV is best positioned for the individual needs of the Station.

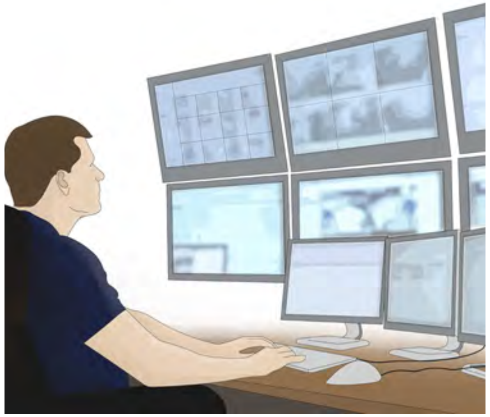


Image 12.9: Control room in use illustration

Image 12.10: Control room computers

12.6 Human Factors and Ergonomics

Human factors and ergonomics are critical for a CCTV monitoring area, but also apply to the wider requirements of an Operational Control Room.

Human factors are about how a person interacts with their “world” (in this case their working world). It combines aspects such as psychology, physiology and engineering with personal value, feelings of belonging and wellbeing, rewards and benefits.

This is a complex multidisciplinary topic that is not directly covered in the design guide however the following design measures will support:

- Compliance with ISO 11064-4:2013 - Ergonomic design of control centres
- Space
- To work (at the workstation)
  - Is the workstation cramped or uncomfortable?
  - Can all the tasks be performed without having to juggle items or rest
  - One item on top of another?
- To move around. Is there space to move the chair from the workstation without hindrance

Noise/distractions

- Does the design assure a good environment for focussed or concentrated working?

Lighting

- Task lighting should be provided
- Area lighting should be muted and not glaring
- Area lighting should be controllable – by area and intensity
- Consider daylight lighting for rooms without windows
- Consider impacts on night workers
- Lights should not cause glare onto or reflected off screens

Facilities

- Are there suitable welfare and rest facilities close by?
- Does an operator lose a lot of personal (or work) time having to travel long distances to use the facilities?
- Are there suitable facilities for shift changes?
- Are there suitable facilities for group or individual briefings?

Environmental

- Is there sufficient fresh air?
- Is the space cool enough in summer and warm enough in Winter?

12.7 Public Address/Voice Alarm & Personal Mobile Radio

The Public Address/Voice Alarm (PAVA) system is used to direct members of the public in the event of an emergency. To this end it is important that PA announcements are clear when broadcast and to achieve this the PAVA system microphones and controls should be in a dedicated space adjoining or directly connected to the CCTV monitoring area.

By convention, in an emergency situation, the CCTV system is used to monitor events and the PAVA system is used to direct the public to places of relative safety. Accordingly, during an emergency there is a need for direct interaction between senior decision makers using/viewing the CCTV system and the PA announcer.

NR Guidance Suite Reference

Network Rail Telecoms Design Standards,
NR/L1/TEL/30100

A subset of the communication system is the Personal Mobile Radio (PMR) (and for certain stations include Emergency Services Communication Systems (Airwaves (where used) and Tetra).

The design of the system should provide for unbiquitous coverage for all PMR systems. The design should also include dedicated positions for changing systems for handsets.

The CCTV monitoring positions should have direct access to PMR communication systems sufficient to allow CCTV operators to easily communicate with field resources being directed to incidents observed via the CCTV system.

Image 12.11: illustration of a PAVA in use

Image 12.12: Illustration of a PAVA loud speaker

5
4
364
362
1-3, 6-11, 13 & 14 via stairs
Way out
1 to 3, 6 to 12 level access
13 & 14 via lift from platforms 8/9 & 10
1-3
1 to 3
13 & 14 via lift from platforms 8/9 & 10

Image 12.13

Manchester Piccadilly Station Platform

Document References

A

Security at Stations

Acknowledgements

Definitions

Referenced Documents

Image Credits

Appendix A
Acknowledgements

On behalf of Network Rail, the production of this design guide has been led by Atkins, member of the SNC Lavalin Group, with support and input from Crossley Consult and Thornton Tomasetti.

ATKINS
Member of the SNC-Lavalin Group

CROSSLEY
CONSULT

Thornton
Tomasetti

A working group, comprising members from Network Rail (Architecture and Security and other departments), SIDOS Ltd., British Transport Police (Designing Out Crime and Counterterror) and Centre for Protection of National Infrastructure (CPNI) have also been consulted.

Appendix A
Definitions

ATG	Automated Ticket Gates
APM	Association for Project Management
ATOC	Association of Transport Operating Companies
BTP	British Transport Police
CCTV	Closed Circuit Television
CDM	Construction Design and Management
CIS	Customer Information Screens
CPNI	Centre for the Protection of National Infrastructure
CPtED	Crime Prevention through Environmental Design
DfT	Department for Transport
GRIP	Governance of Railway Investment Projects
HVAC	Heating Ventilation and Air Conditioning
HVM	Hostile Vehicle Mitigation
IDS	Intrusion Detector System
ILP	Institute of Lighting Professionals
LCCA	Life Cycle Cost Analysis
MEP	Mechanical, Electrical, and Plumbing
NTSN	National Technical Specification Notice
NR	Network Rail
NRSP	Network Rail Security Programme
OGC	Office of Government and Commerce
PIDs	Passenger Information Displays
PTE	Passenger Transport Executives
PMR	Private Mobile Radio
PVB	Polyvinyl Butryal
PRM	Person of Restricted Mobility
RDG	Rail Delivery Group
RFI	Radio Frequency Identification
RUS	Route Utilisation Strategy
RSES	Register of Security Engineers & Specialists
TfL	Transport for London
TVM	Ticket Vending Machine
TVRA	Threat, Vulnerability, and Risk Assessment
SIDOS	Security in the Design of Stations

Referenced Documents

British Transport Police (BTP) - A Guide to Reducing Retail Crime at Railway Stations

British Transport Police (BTP) - Designing Out Crime Officer (DOCO) – Architectural Liaison Projects input

British Transport Police (BTP) - Secure Stations Scheme

Bicycle Association - Standards For Public Cycle Parking

Caroline Kingston - Preventing Suicides on Railway

Criminal Justice Review - Reducing Assaults Against Staff Using Body-Worn Cameras (BWCs) in Railway Stations

CPNI - Public Realm Design Guide, Hostile Vehicle Mitigation

Cross Rail Designing for Security - CRL1-XRL-O6-STD-CR001-00023

Crossley Consult - Aviation Security in Airport Development Advice Notes

Department for Transport (DfT) - Guidance to local authorities: Mitigating security vulnerabilities outside railway, bus and coach stations

Department for Transport (DfT) - Land Transport Security Compliance Polict Framework

Department for Transport (DfT) - Protecting Crowded Places: Design and Technical

Department for Transport (DfT) - Security in the Design of Stations Recommended Best Practice

Department for Transport (DfT) - Cycle Infrastructure Design – Local Transport Note 1/20

HM Government - Government Functional Standard, GovS 007: Security

HM Government - Protecting Crowded Places: Design and Technical Issues

LPCB - Security Systems, Protecting People and Property

Network Rail - Station Design Guidance

Network Rail - Station Capacity Planning

Network Rail - Inclusive Design

Network Rail - CNI Physical Security Guidance

Network Rail - Boundary Measure Specification

Network Rail - National Operating Procedures, Management of Station Security & Crime

Network Rail - National Operating Procedures, Station Security & Event Plans

Network Rail - Our Principles of Good Design

Network Rail - Rail Delivery Group (RDG) Body Worn Video Use

Rail Safety & Standards Board Ltd (RSSB) - Interface between Station Platforms, Track, Trains and Buffer Stops

Rail Safety & Standards Board Ltd (RSSB) - Rail Industry Standard for Station Infrastructure

Rail Safety & Standards Board Ltd (RSSB) - Rail Industry Standard for Automatic Ticket Gates at Stations

Station Design Best Practice Manual - Designing for Crime Reduction at Stations

Station Design Best Practice Manual - Designing for Escalator Safety at Stations

Station Design Best Practice Manual - Designing for Safety at Stations

Construction Design Management (CDM) - The CDM Regulations 2015

The Equality Act 2010

Appendix A
Image Credits

Image;		Page
0.1	© Network Rail Media Centre	08

Section 1

Image;		Page
1.1	© Network Rail Media Centre	10
1.2	© Network Rail Media Centre	11
1.3	© Network Rail Media Centre	13
1.4	© Atkins Global	17
1.5	© Network Rail Media Centre	18

Section 2

Image;		Page
2.1	© Network Rail Media Centre	20
2.2	© Atkins Global	21
2.3	© Network Rail Station Design Guide, Weston Williamson + Partners	21
2.4	© Atkins Global	22
2.5	© Atkins Global	23
2.6	© Atkins Global	24
2.7	© Network Rail Station Design Guide, Weston Williamson + Partners	25
2.8	© Network Rail Media Centre	26

Section 3

Image;		Page
3.1	© Atkins Global	28
3.2	© Atkins Global	29
3.3	© Atkins Global	30
3.4	© Atkins Global	31
3.5	© Atkins Global	32
3.6	© Atkins Global	33
3.7	© Atkins Global	34
3.8	© Network Rail Media Centre	36

Section 4

Image;		Page
4.1	© Network Rail Media Centre	38
4.2	© Network Rail Media Centre	39
4.3	© Network Rail Media Centre	39
4.4	© Atkins Global	40
4.5	© Atkins Global	41
4.6	© Network Rail Media Centre	42
4.7	© Atkins Global	43
4.8	© Network Rail Media Centre	44
4.9	© Network Rail Media Centre	45
4.10	© Network Rail Media Centre	46

Section 5

Image;		Page
5.1	© Network Rail Media Centre	48
5.2	© Network Rail Media Centre	49
5.3	© Network Rail Media Centre	49
5.4	© Network Rail Media Centre	49
5.5	© Network Rail Media Centre	51
5.6	© Atkins Global	53
5.7	© Atkins Global	54
5.8	© British Gypsum	55
5.9	© R&R Ready Mix	55
5.10	© Network Rail Media Centre	55
5.11	© Latham's Steel Security Doorsets	56
5.12	© HM Group Portsmouth	56
5.13	© Door Stuff	57
5.14	© Dormakaba	58
5.15	© Atkins Global	58
5.16	© Atkins Global	59
5.17	© Network Rail Media Centre	60

Section 6

Image;		Page
6.1	© Network Rail Media Centre	62
6.2	© Network Rail Media Centre	63
6.3	© Atkins Global	64
6.4	© Atkins Global	64
6.5	© Atkins Global	65
6.6	© Atkins Global	65
6.7	© Network Rail	67
6.8	© Flickr	67
6.9	© Network Rail	68
6.10	© Network Rail	68
6.11	© Atkins Global	69
6.12	© Atkins Global	70
6.13	© Atkins Global	71
6.14	© Flickr	72
6.15	© Network Rail Media Centre	73
6.16	© Network Rail Media Centre	73
6.17	© Network Rail Media Centre	74

Section 7

Image;		
7.1	© Network Rail Media Centre	76

Appendix A
Image Credits

Section 7 continued

Image;		Page
7.2	© Network Rail Media Centre	77
7.3	© Crossley Consult Ltd and Atkins Global	78
7.4	© Crossley Consult Ltd and Atkins Global	78
7.5	© Crossley Consult Ltd and Atkins Global	79
7.6	© Network Rail Media Centre	79
7.7	© Crossley Consult Ltd and Atkins Global	80
7.8	© Crossley Consult Ltd and Atkins Global	80
7.9	© Network Rail Media Centre	81
7.10	© Crossley Consult Ltd and Atkins Global	81
7.11	© Network Rail Media Centre	81
7.12	© Crossley Consult Ltd and Atkins Global	81
7.13	© Crossley Consult Ltd and Atkins Global	82
7.14	© Network Rail Media Centre	82
7.15	© Crossley Consult Ltd and Atkins Global	82
7.16	© Crossley Consult Ltd and Atkins Global	82
7.17	© Crossley Consult Ltd and Atkins Global	83
7.18	© Network Rail Media Centre	83
7.19	© Crossley Consult Ltd and Atkins Global	83
7.20	© Crossley Consult Ltd and Atkins Global	84
7.21	© Network Rail Media Centre	84
7.22	© Crossley Consult Ltd and Atkins Global	85
7.23	© Network Rail Media Centre	85
7.24	© Crossley Consult Ltd and Atkins Global	86
7.25	© Crossley Consult Ltd and Atkins Global	86
7.26	© Network Rail Media Centre	87
7.27	© Crossley Consult Ltd and Atkins Global	88
7.28	© Crossley Consult Ltd and Atkins Global	88
7.29	© Crossley Consult Ltd and Atkins Global	89
7.30	© Crossley Consult Ltd and Atkins Global	90
7.31	© Network Rail Media Centre	90
7.32	© Crossley Consult Ltd and Atkins Global	90
7.33	© Crossley Consult Ltd and Atkins Global	91
7.34	© Network Rail Media Centre	91
7.35	© Crossley Consult Ltd and Atkins Global	91
7.36	© Crossley Consult Ltd and Atkins Global	92
7.37	© Network Rail Media Centre	92
7.38	© Crossley Consult Ltd and Atkins Global	93
7.39	© Network Rail Media Centre	93
7.40	© Crossley Consult Ltd and Atkins Global	94
7.41	© Crossley Consult Ltd and Atkins Global	94
7.42	© Crossley Consult Ltd and Atkins Global	95
7.43	© Network Rail Media Centre	95
7.44	© Network Rail, Station Facillities & Amenities Design Manual	95
7.45	© Crossley Consult Ltd and Atkins Global	96
7.46	© Crossley Consult Ltd and Atkins Global	97
7.47	© Crossley Consult Ltd and Atkins Global	97
7.48	© Crossley Consult Ltd and Atkins Global	97
7.49	© Network Rail Media Centre	97
7.50	© Network Rail Media Centre	97
7.51	© Network Rail Media Centre	98
7.52	© Getty Images	98
7.53	© Crossley Consult Ltd and Atkins Global	98
7.54	© Crossley Consult Ltd and Atkins Global	99
7.55	© Network Rail Media Centre	99
7.56	© Crossley Consult Ltd and Atkins Global	100
7.57	© Crossley Consult Ltd and Atkins Global	100
7.58	© Network Rail Media Centre	100
7.59	© Network Rail Media Centre ?	100
7.60	© Crossley Consult Ltd and Atkins Global	101
7.61	© Network Rail Media Centre	101
7.62	© Network Rail Media Centre	101
7.63	© Network Rail Media Centre	102

Section 8

Image;		Page
8.1	© Network Rail	104
8.2	© Network Rail, Public Realm at Stations	104
8.3	© Network Rail, Public Realm at Stations	105
8.4	© Network Rail Media Centre	106
8.5	© Network Rail	108
8.6	© Network Rail Media Centre	109
8.7	© Network Rail	110
8.8	© Network Rail Media Centre	111
8.9	© Network Rail Media Centre	112
8.10	© Network Rail Media Centre	113
8.11	© Network Rail Media Centre	114
8.12	© Network Rail Media Centre	115
8.13	© Network Rail Media Centre	115
8.14	© Network Rail Media Centre	116
8.15	© Network Rail	117
8.16	© Network Rail	117
8.17	© Network Rail	118
8.18	© Network Rail	119
8.19	© Atkins Global	121
8.20	© Lang & Fulton	122
8.21	© Godalming	122
8.22	© Cochrane Clearview	122

Appendix A
Image Credits

Section 9

Image;		Page
9.1	© Network Rail Media Centre	124
9.2	© Network Rail Media Centre	125
9.3	© Network Rail Media Centre	125
9.4	© Network Rail Media Centre	125
9.5	© Atkins Global	127
9.6	© Network Rail Media Centre	128

Section 10

Image;		Page
10.1	© Network Rail Media Centre	130
10.2	© Network Rail Media Centre	131
10.3	© Network Rail Media Centre	132
10.4	© Eas Envimet	133
10.5	© Robert Devlin	133
10.6	© Network Rail Media Centre	134

Section 11

Image;		Page
11.1	© Network Rail Media Centre	136
11.2	© British Transport Police	137
11.3	© Centre for the Protection of National Infrastructure	137
11.4	© Network Rail Media Centre	138

Section 12

Image;		Page
12.1	© Atkins Global	140
12.2	© Network Rail Media Centre	141
12.3	© CPC Farnell	142
12.4	© HM Group	142
12.5	© Screwfix	143
12.6	© Network Rail Media Centre	143
12.7	© Atkins Global	144
12.8	© Atkins Global	145
12.9	© Network Rail Media Centre	145
12.10	© Atkins Global	147
12.11	© Atkins Global	147
12.12	© Network Rail Media Centre	148

Appendices

Image;		Page
A1	© Network Rail Media Centre	156
B.1	© Network Rail Media Centre	158
B.2	© D-Tours	159
B.3	© Chapman Taylor	159
B.4	© Crossley Consult Ltd	159
B.5	© Network Rail Media Centre	160
B.6	© Network Rail Media Centre	160
B.7	© Network Rail	161
B.8	© Network Rail	161
B.9	© Network Rail	161
B.10	© Network Rail	162
B.11	© Network Rail	162
B.12	© Network Rail	162
C.1	© Crossley Consult Ltd	164
C.2	© Crossley Consult Ltd	164
C.3	© Network Rail	166
C.4	© Network Rail	166
C.5	© Network Rail	167
C.6	© Network Rail	167
C.7	© Network Rail	168
C.8	© Network Rail	168
C.9	© Network Rail	169
C.10	© Network Rail	169
C.11	© Network Rail	170
C.12	© Network Rail	171

Covers

Front	© Network Rail Media Centre	03
Back	© Network Rail Media Centre	172

Image A.1

London Paddington Station

Case Studies

B

Security at Stations

Heathrow Airport Terminal 5 – Blast Design Guidance

London Bridge Station – Smart CCTV

Gatwick Airport Railway Station Upgrade – Excessive Blast Mitigation

Perry Barr Station – Security Performance Requirements

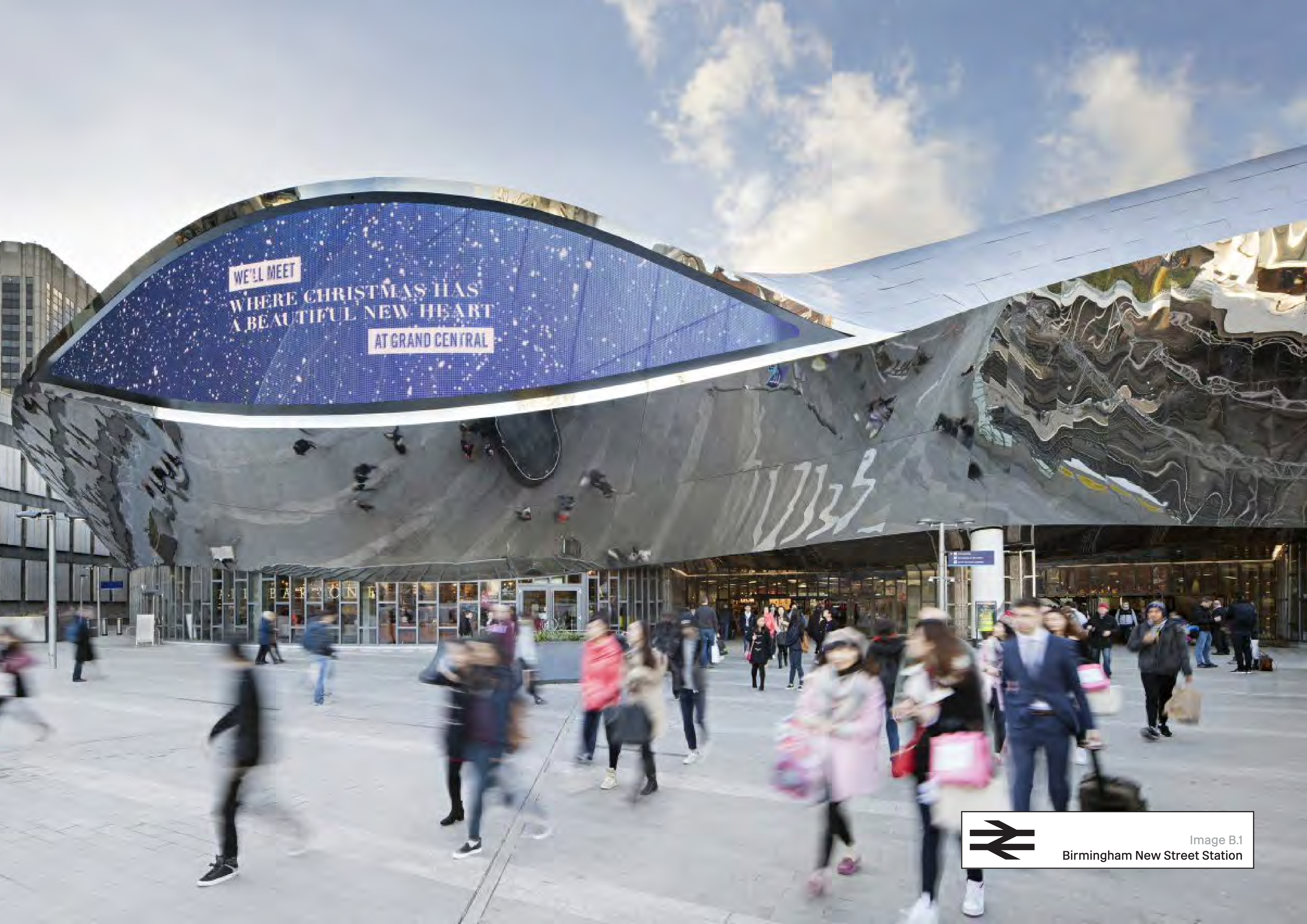


Image B.1
Birmingham New Street Station

Heathrow Airport Terminal 5 – Blast Design Guidance

Projects across the Heathrow Airport estate follow a carefully compiled series of blast design guidance manuals. These notes offer advice on various common components commonplace in an air terminal environment, including various different types of glazed elements, bins, seating, wall systems, suspended items, kiosks, screens, barriers and check-in desks.

These design guidance notes form part of appointment and construction contracts to designers and contractors and should be followed in all cases. This approach creates a uniformity across the Heathrow estate and helps to check new designs are resistant to blast, using physical and numerical testing to backup design proposals.

Image B.2 Heathrow Terminal 5

Image B.3 Heathrow Terminal 5 ceiling

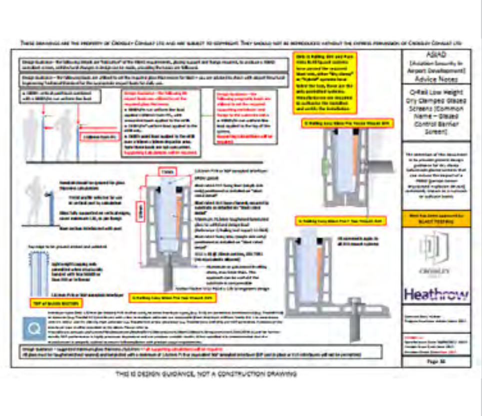

ASIAD
(Aviation Security in Airport Development)
Advice Notes
Q-Rail Low Weight Dry Clamped Glazed Screens (Common Name – Glazed Control Barrier Screen)
Heathrow
THIS IS DESIGN GUIDANCE, NOT A CONSTRUCTION DRAWING

Image B.4 Crossley Consult blast resistant details

London Bridge Station – Smart CCTV

London Bridge uses a smart CCTV system to alert station staff to issues emerging in real time. This new technology is being honed to observe criminality, such as civil disturbances and criminal behaviour, pedestrian flow issues, such as overcrowding and safety incidents such as trips, slips and falls. This new system alerts station staff to these type of events such that responses can be rapid. This also helps to reduce the burden of CCTV monitoring by station staff. This is new and emerging technology that works in accordance with Network Rail's Data Protection Act obligations.

Image B.5 London Bridge concourse

Image B.6 Shard concourse at London Bridge

Gatwick Airport Railway Station Upgrade – Excessive Blast Mitigation

The Gatwick Airport Railway Station upgrade project is an example where complex regulatory requirements around the interface between Aviation and Railway security regulations and an over cautious security approach resulted in higher blast resistance requirements than are strictly necessary for the location. This led to significant investment in complex blast analysis, blast design and installation of significant blast mitigation features.

The level of threat identified in the threat and vulnerability risk assessment (TVRA) was lower than what the project anticipated and had the TVRA been done at an earlier stage of the project it could have resulted in significant savings. Projects should gain a clear understanding of blast design requirements from Network Rail before investing in analysis, design and on site installation.

Image B.7 CGI Railway entrance

Image B.8 CGI Platform 3 & 4 lift

Image B.9 CGI Airport entrance

Appendix B - Case Study 4

Perry Barr Station – Security Performance Requirements

There were considerable security concerns raised during the upgrading of Perry Barr Station, in preparation of the Commonwealth Games that included development of the public realm to counter vehicle incursion, as well as adequately securing the station itself. This led to several rounds of stakeholder discussion, very late during the detailed design project stage.

This ultimately resulted in Technical Authority Group Security issuing a Security Risk Estimate notification, and some consequential re-design. Particularly of note is the confusion surrounding the correct SR rating being applied to a particular category/ risk profile of station. This project illustrates both good and bad practice in the lack of early security planning, particularly for a station planned to cater for a large event. Albeit, detailed security consideration was applied, late on in the project lifecycle.

Image B.10 Outside Perry Barr station

Image B.11 CGI of Perry Barr station

Image B.12 Inside support van outside Perry Bar station

Loading Information & Fence and Bollard Details

C

Security at Stations

Key loading Information when Designing for Blast Resistance

Typical Fence and Bollard Details

Loading Information

The following design guidance loads should be utilised to set the required glass thicknesses where blast loading is relevant. In all cases, the appointed structural engineer is advised to check that these loads are applicable to the project and in alignment with the relevant standards. In addition to those noted, there is a possibility that additional project specific loads may also be applicable.

There are 2 overriding criteria which determine the glazing loading:

- → Is the product on the same level i.e. not protecting a drop (Load case A)?
- → Is the product protecting a drop (which might be as little as 300 mm) (Load case B)?

Generally, the supporting metalwork, framing, glass or infill and fixings to the substrate floor should be designed to the following British Standard serviceability load cases.

It is recommended that glazing is designed using the “limit state design process” as defined in The Institution of Structural Engineers “structural use of Glass in buildings (second edition) February 2014 is used to calculate the appropriate glass types, interlayers and thicknesses.

C.1 Load Case A – for an installation that is not protecting a drop, the following loads should be considered:

- → 1500 N / m run uniformly distributed line load applied 1100 mm from FFL (finished floor level) in the positive and negative direction.
- → 1500 N /m2 uniformly distributed load applied to the infill beneath the line load in positive and negative direction.
- → 1500 N point load applied to a 100 mm x 100 mm impact area in the worst-case position applied in the positive and negative direction.
- → 600 N /m2 uniformly distributed internal wind load applied to the entire surface area in the positive and negative direction.
- → If applicable, external wind loads should be obtained from the project engineer.
- → 4 kPa for the design of connections applied in the positive and negative direction.
- → These loads are not concurrent but note the recommendation for the glass to be designed using a “limit state design principles”.
- → Additional load combinations may be applicable and should be considered by the project engineer and Network Rail.

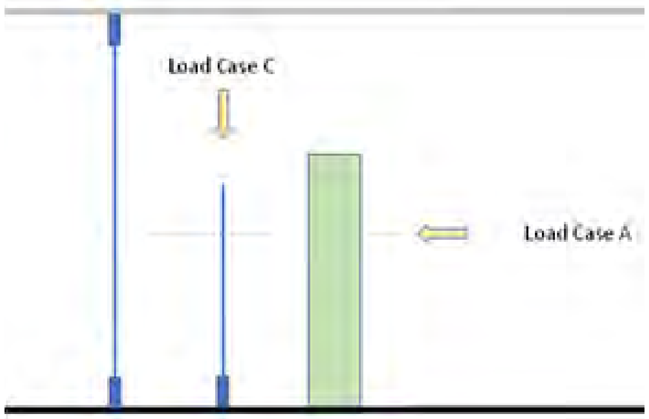


Figure C.1: Loading information diagram

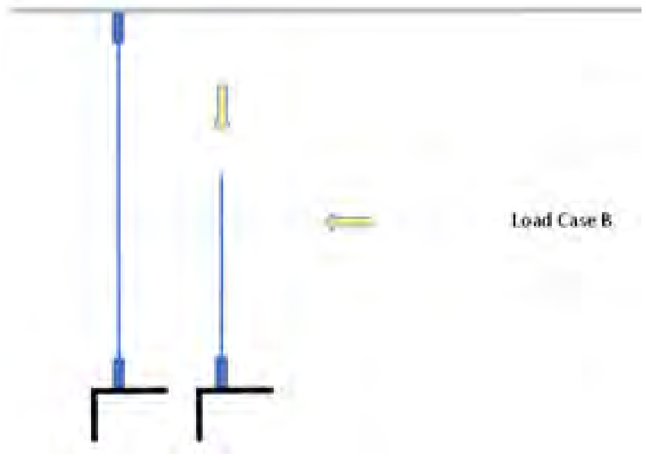


Figure C.2: Loading information diagram

Loading Information Continued

C.2 Load Case B – for an installation where the item is protecting a drop, the following loads should be considered:

- 3000 N / m run uniformly distributed line load applied 1100 mm from FFL (finished floor level) in the positive and negative direction.
- 1500 N /m2 uniformly distributed load applied to the infill beneath the line load in positive and negative direction.
- 1500 N point load applied to a 100 mm x 100 mm impact area in the worst-case position applied in the positive and negative direction.
- 600 N /m2 uniformly distributed internal wind load applied to the entire surface area in the positive and negative direction.
- If applicable external wind loads should be obtained from the project engineer.
- 4 kPa for the design of connections applied in the positive and negative direction.
- These loads are not concurrent but note the recommendation for the glass to be designed using a “limit state design principles”.
- Additional load combinations may be applicable and should be considered by the project engineer and Network Rail.

C.3 Load Case C – for installations where loads can be placed on the top of the glazed element, and if applicable the supporting metalwork, then an additional load case would be applicable.

- 1000 N vertical point load applied to a 100 mm impact length, in the worst-case position

C.4 Additional crowd loading

In addition to these load cases Network Rail sometimes requires the glazing and supporting metalwork to resist exceptional crowd loading in which case the item may be required to be designed to the following load case.

- 3000 N / m run uniformly distributed line load applied 1100 mm from FFL (finished floor level) in the positive and negative direction.
- Please note that on specific projects the Network Rail engineers have some time specified a higher load.
- In recognition that this static load conditions is extremely high sometimes depending upon the method of support of the glazed element and supporting metalwork the deflection limits are relaxed and normally limited to 50 mm for customer confidence.

C.5 Balustrade construction and numbers of ply

If the glass is protecting a drop and if it is clamped at the base and there is no vertical metalwork and handrail to take the line load and should toughened glass be utilised in the glass construction, then additional considerations should be factored into the balustrade design. It is common with toughened glass to check that the glass can perform with one ply of the glass broken. This will often dictate that a three-ply construction is required i.e. glass/interlayers/glass/interlayers/glass. The theory being that with one broken ply of glass but glass can perform as required.

C.6 Exceptions

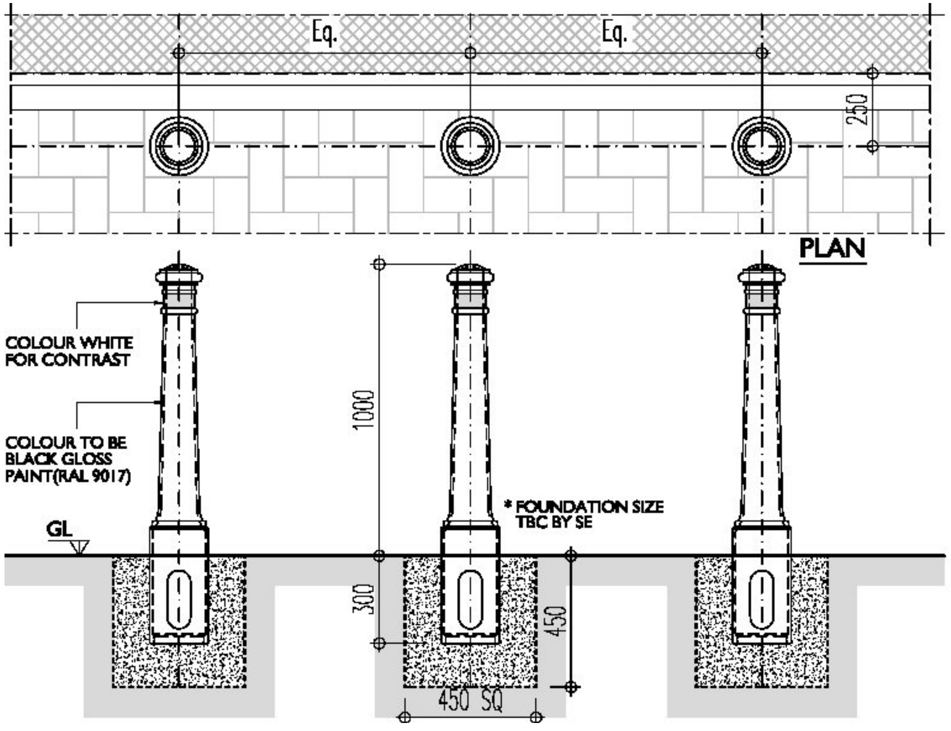
Overhead canopy glass would be designed to Centre for Window and Cladding Technology (CWCT) loading criteria.

- Glass within rooflights would be designed to the CWCT loading criteria.
- Glass protecting a lift shaft would be designed to specific loading criteria.
- Point fixed glazing systems would be designed to specific criteria applicable to lift shafts.
- Holes In glass dictate a requirement for toughened or thermally processed glass.

Advice from a member of the Register of Security Engineers and Specialists (RSES), experienced in designing for blast resistance, should be sought for further load case information.

Figure C.3: Ductile cast iron bollard sectional elevation

All components on this drawing is shown for illustration purposes only. All fixings are to manufacturers' recommendation.


Eq.
Eq.
250
PLAN
COLOUR WHITE FOR CONTRAST
COLOUR TO BE BLACK GLOSS PAINT(RAL 9017)
GL
1000
300
* FOUNDATION SIZE TBC BY SE
450
450 SQ

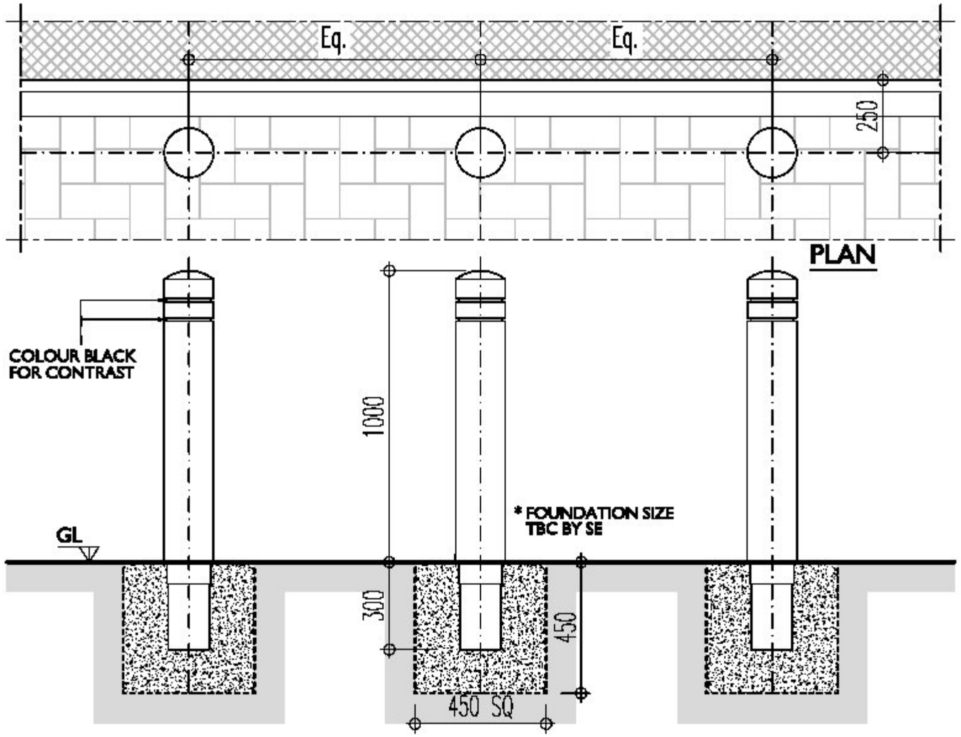


Figure C.4: Round top satin stainless steel bollard sectional elevation

Typical Fence and Bollard Details

All components on this drawing is shown for illustration purposes only. All fixings are to manufacturers' recommendation.

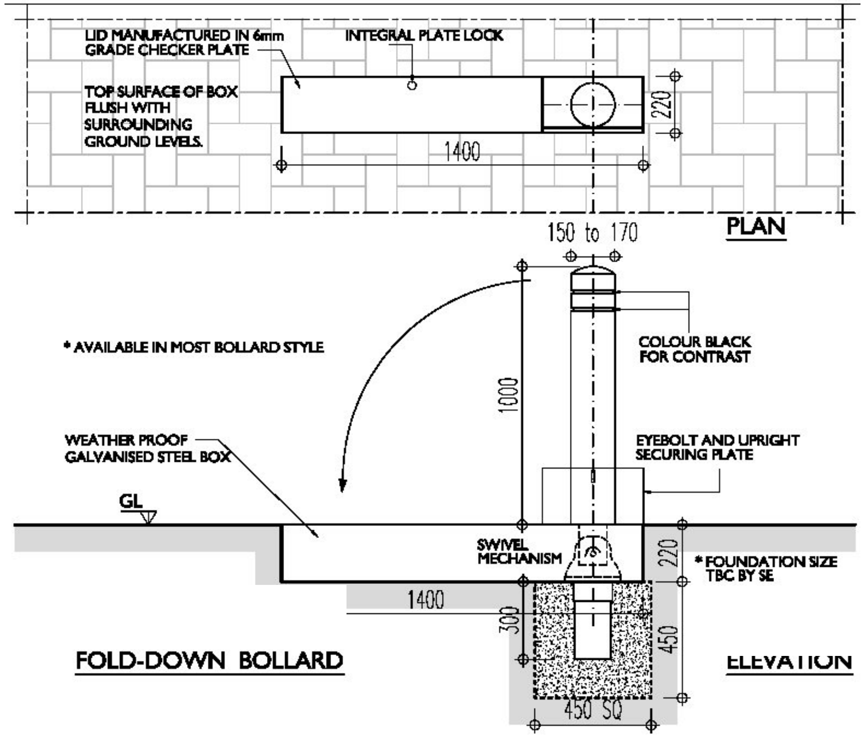

LID MANUFACTURED IN 6mm GRADE CHECKER PLATE
INTEGRAL PLATE LOCK
TOP SURFACE OF BOX FLUSH WITH SURROUNDING GROUND LEVELS.
220
1400
150 to 170
PLAN
* AVAILABLE IN MOST BOLLARD STYLE
COLOUR BLACK FOR CONTRAST
1000
WEATHER PROOF GALVANISED STEEL BOX
EYEBOLT AND UPRIGHT SECURING PLATE
GL
SWIVEL MECHANISM
220
* FOUNDATION SIZE TBC BY SE
1400
300
450
FOLD-DOWN BOLLARD
ELEVATION
450 SQ

Figure C.5: Fold-down bollard sectional elevation

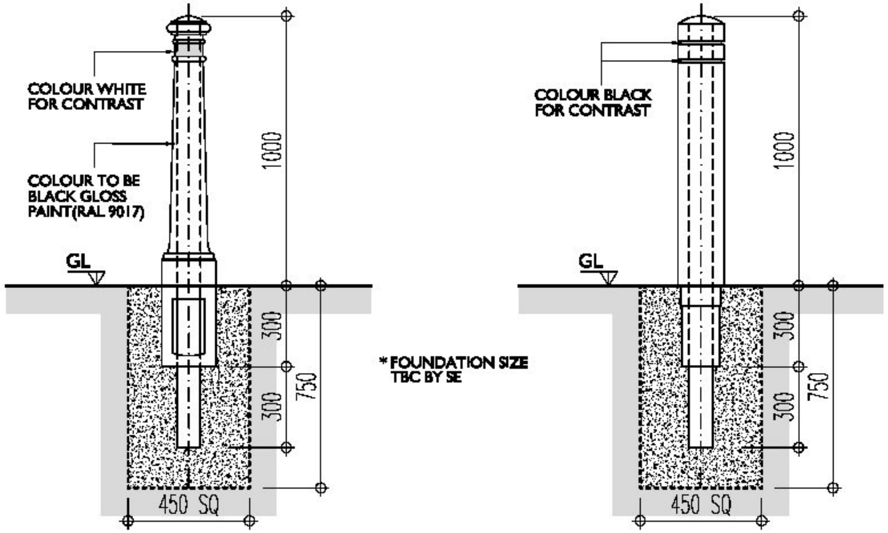

COLOUR WHITE FOR CONTRAST
COLOUR TO BE BLACK GLOSS PAINT(RAL 9017)
1000
GL
300
300
750
450 SQ
* FOUNDATION SIZE TBC BY SE
COLOUR BLACK FOR CONTRAST
1000
GL
300
300
750
450 SQ

Figure C.6: Ductile & stainless steel anti-ram bollard sectional elevations

Typical Fence and Bollard Details

All components on this drawing is shown for illustration purposes only. All fixings are to manufacturers' recommendation.

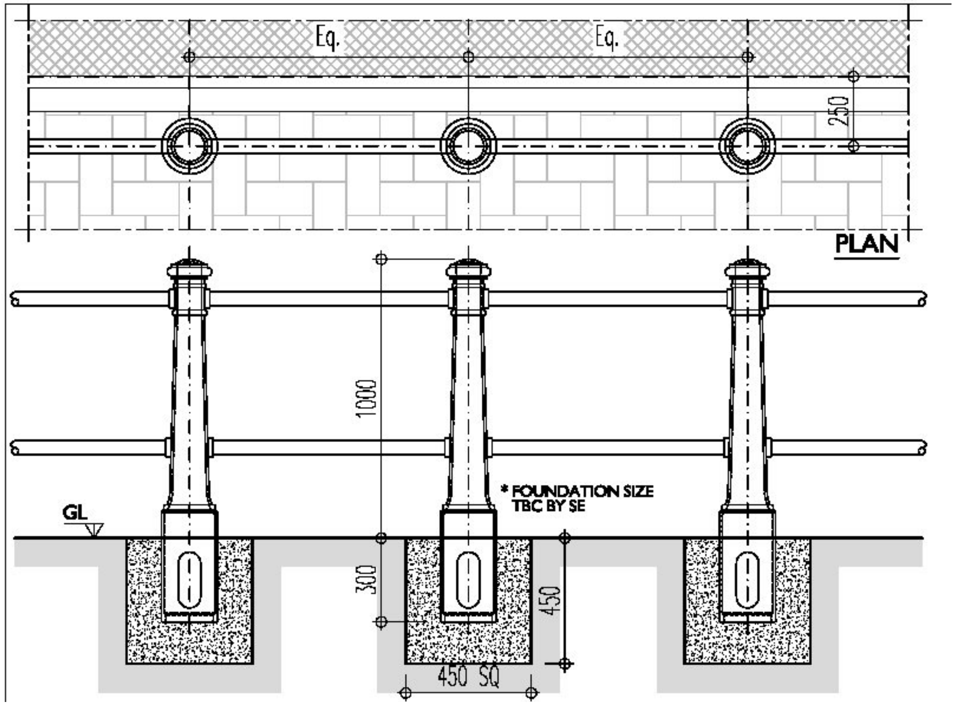


Figure C.7: Ductile cast iron pedestrian route separation sectional elevation

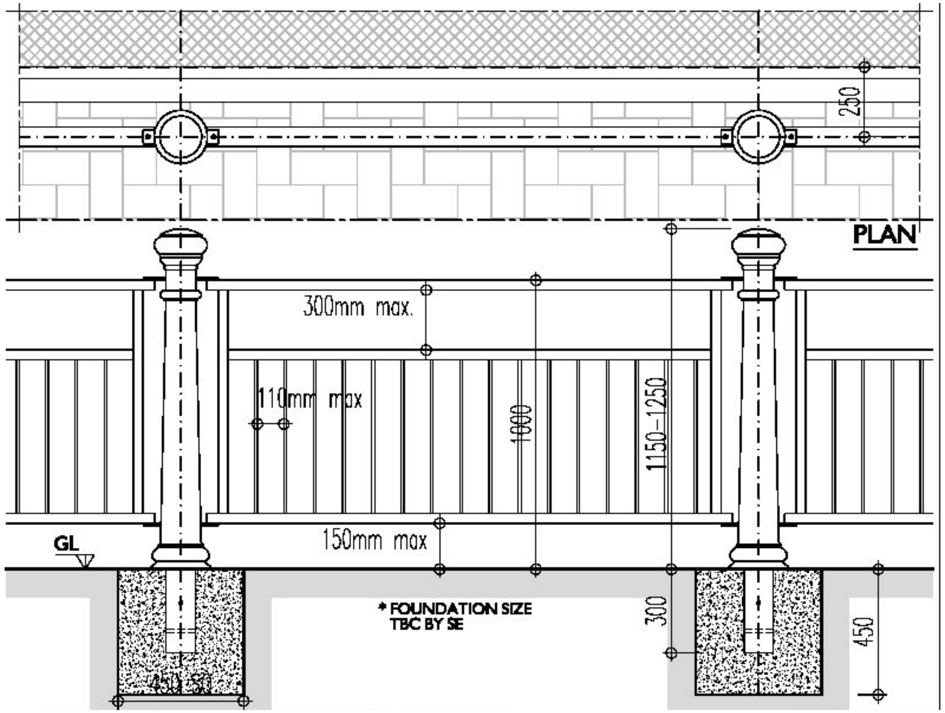


Figure C.8: Heritage type pedestrian barrier sectional elevation

All components on this drawing is shown for illustration purposes only. All fixings are to manufacturers' recommendation.

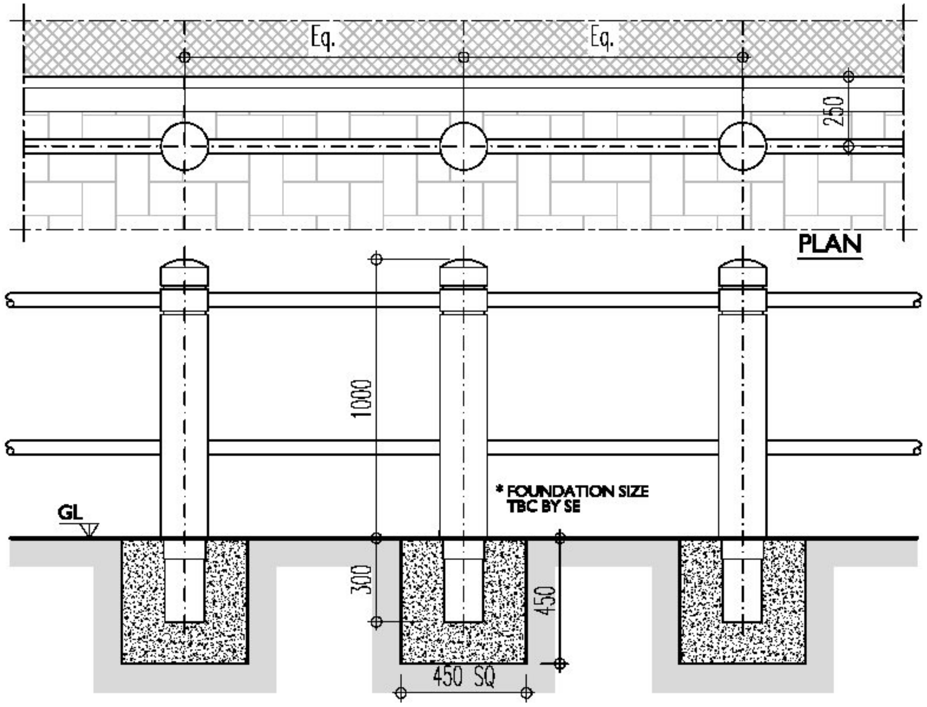


Figure C.9; Round top stainless steel pedestrian route separation sectional elevation

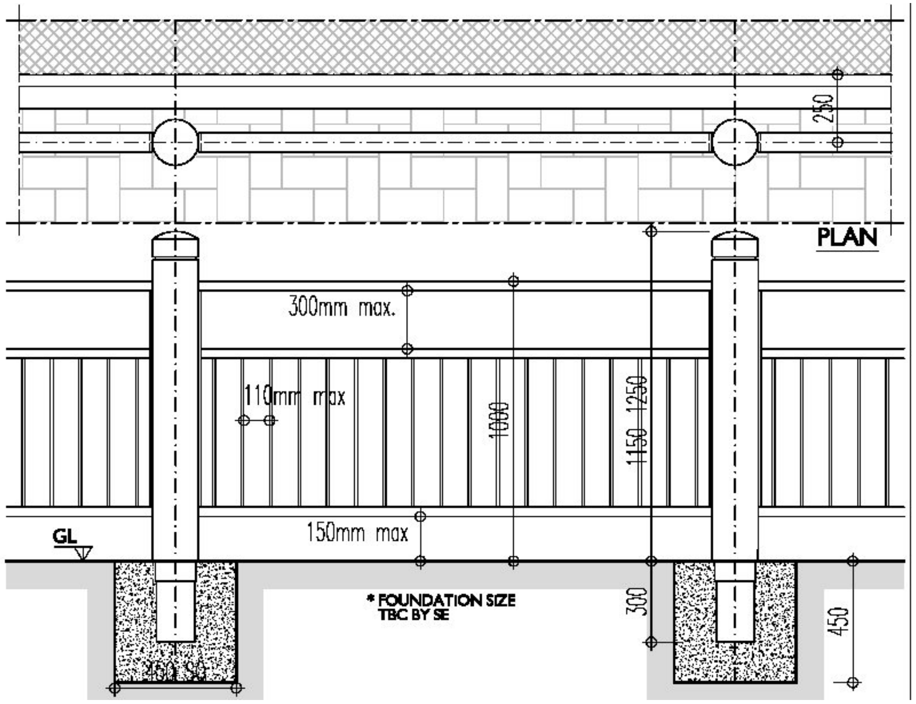


Figure C.10: Round top stainless steel pedestrian barrier sectional elevation

All components on this drawing is shown for illustration purposes only. All fixings are to manufacturers' recommendation.

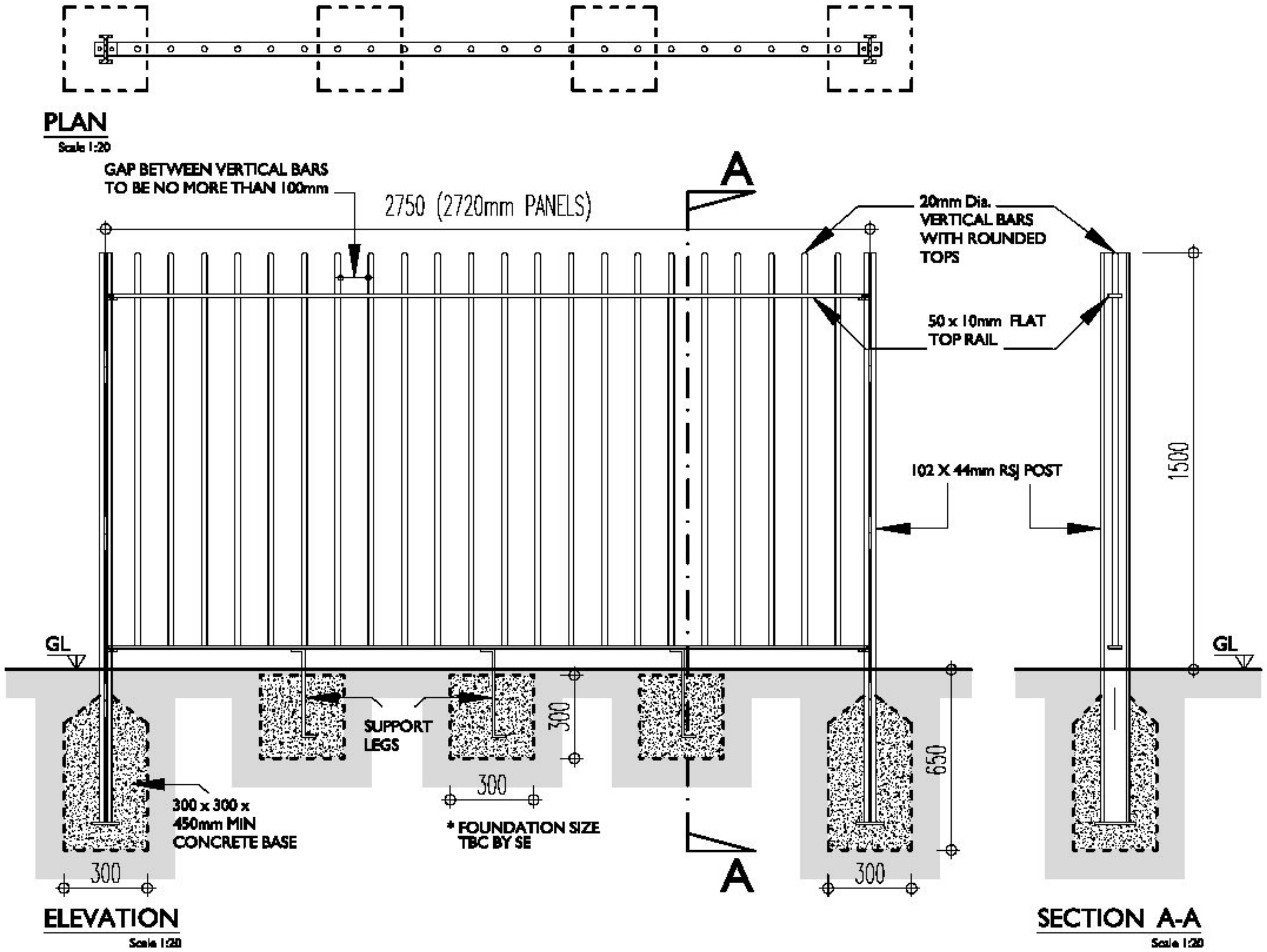

PLAN
Scale 1:20
GAP BETWEEN VERTICAL BARS TO BE NO MORE THAN 100mm
2750 (2720mm PANELS)
A
20mm Dia. VERTICAL BARS WITH ROUNDED TOPS
50 x 10mm FLAT TOP RAIL
102 X 44mm RSJ POST
1500
GL
GL
SUPPORT LEGS
300
650
300 x 300 x 450mm MIN CONCRETE BASE
300
* FOUNDATION SIZE TBC BY SE
A
300
300
ELEVATION
Scale 1:20
SECTION A-A
Scale 1:20

Figure C.11: Platform fencing / steel railing plans, sections, elevations

Typical Fence and Bollard Details

All components on this drawing is shown for illustration purposes only. All fixings are to manufacturers' recommendation.

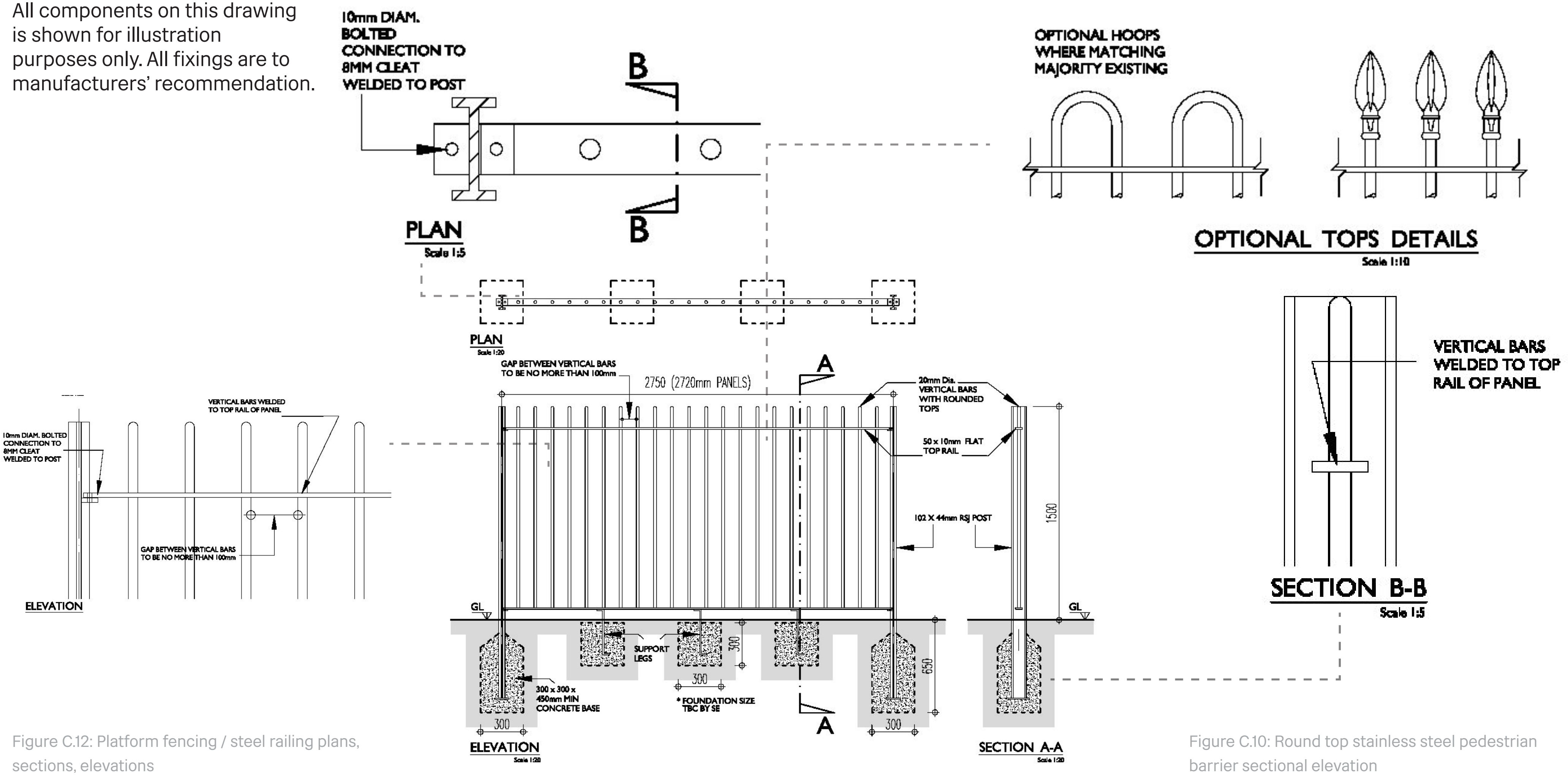


Figure C.12: Platform fencing / steel railing plans, sections, elevations

Figure C.10: Round top stainless steel pedestrian barrier sectional elevation

4b
Buffet
Waiting room
Lift
Way out
Manchester Picc 11:59
2nd Holyhead 12:25
4b
Telephone
4a
175107
Wilson
3

300/

03