IARO report 9.06

Security on airport railways

IARO Report 9.06: Security on airport railways

Editor: Andrew Sharp

Published by

International Air Rail Organisation

3rd Floor, 30 Eastbourne Terrace

London W2 6LE

Great Britain

Telephone +44 (0)20 8750 6632

Fax +44 (0)20 8750 6647

website www.iaro.com, www.airportrailwaysoftheworld.com

email int-airrail@baa.com

ISBN 1 903108 07 1

£250 to non-members

Our mission is to spread world class best practice and good practical ideas among airport rail links world-wide.

Contents

Introduction---- 4

List of abbreviations and acronyms ---- 5

1 Some general principles – detect, deter, delay and prevent attacks.--- 7

2 Detect ---- 11

3 Deter and delay ---- 16

4 Prevent ---- 20

5 Explosives. ---- 26

6 Chemical, radiological and biological threats---- 31

7 Fear---- 34

8 Fire ---- 35

9 Baggage. ---- 36

10 The airport station – the interface ---- 37

11 Employees – the positive. ---- 40

12 Employees – the negative ---- 42

13 Plan, practice and learn. ---- 43

14 Precursor events – the warning signs. ---- 46

15 Resources available ---- 48

IARO's Air/Rail conferences and workshops ---- 53

Introduction

There are many aspects of security affecting railways to airports in particular. Some are common to all railways: some are more specific. As a portal to excellence in airport railways, IARO is publishing this report which discusses the issues and some of the counter-measures which have been developed.

Arriving air passengers and their baggage will have been screened at the airport of embarkation. Other passengers could pose a threat – and one which is higher in the case of some airport railways because of their high profile nationally.

Information in this report does not replace national guidance, which is likely to be more up-to-date and more geographically specific. Nor does this report deal with personal security – issues like assault and theft.

It will be updated from time to time in line with new technology (which seems to change almost daily) and emerging experience: it is hoped that there will not be too much of that. It gives examples of worldwide good practice, and therefore may repeat what some readers have seen elsewhere. Organisations like the TRB and the Mineta Transportation Institute at San Jose State University are continuing research into transport terrorism: their publications and web-sites need to be kept under review. See section 15, Resources available, on page 48.

Railways have been the target of terrorists for over 120 years. There is always a need to be alert, to be vigilant. A responsible transport operator will always want to be realistic and practical in protecting passengers. But there are two dangers to watch for. First, we do need not to give in – not to stop travelling, not to change our life-styles. Second, we must not make the travel experience so tightly secure that it is too difficult to use. Because if we do, the terrorist has won.

Andrew Sharp

Director General

List of abbreviations and acronyms

APTA	American Public Transport Association
BTP	British Transport Police
CCTV	Closed circuit television
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security (USA)
ECMT	European Conference of Ministers of Transport
ETP	Explosives Trace Portal
FEMA	Federal Emergencies Management Agency (US)
FTA	Federal Transit Authority (US)
HOT	Hidden, Obviously suspicious, Typical (see page 11)
G8	Group of 8 major industrial nations
IARO	International Air Rail Organisation
IED	improvised explosive device
IRA	Irish Republican Army
ISO	International Standards Organisation
IT	information technology
K-9	detection method involving the use of trained dogs
MTA	Metropolitan Transportation Authority (in this report, of New York)
NCHRP	National cooperative highway research program
OECD	Organisation for economic cooperation and development
PIR	Passive infra-red
SCADA	Supervisory Control and Data Acquisition
TCRP	Transit Co-Operative Research Program
TRIP	Transit and Rail Inspection Pilot (USA)
TSA	Transportation Security Administration (USA)

UITP	Union Internationale des Transports Publics
UK	United Kingdom
US or USA	United States of America
VIPER	Visible Intermodal Protection and Response
VMD	Video motion detectors

Note that UK conventions are used for dates (day/month/year) and numbers (in 9,999.99 the comma , separates thousands: the full stop . is a decimal point). A billion is a thousand million, following US conventions.

1. Some general principles – detect, deter, delay and prevent attacks.

Introduction

This report discusses security threats against railways to airports. These threats are likely to come from terrorists (of widely mixed motives), from those – usually politically motivated - seeking publicity for a cause, or from the more mindless vandals.

Whatever the source, whether the threat is real or not, there is always disruption and delay. These cost money. You need to assess the threat in order to

- reduce its severity (usually by deterrence measures),
- reduce its likelihood (usually by deterrence and by restricting access to key sites), and
- reduce any potential loss to the system (by detection and by target hardening measures).

The main counter-measures - detect, deter, delay and prevent – are discussed in the next few sections. Then some more specific issues are considered (with, inevitably, some duplication between sections). Some – like checked baggage - are more specific to airport railways than others: some are common to railways anywhere.

Governments, obviously, have the prime responsibility for combating terrorism at a national level. They should be monitoring and evaluating overall risks and threats and notifying operators when necessary. It is up to operators to analyse the vulnerability of their own system and to take appropriate protective action.

Vulnerabilities

What are the high value targets? Which parts of the system are particularly vulnerable? An analysis is needed to assess where (and when) there is most potential for loss of life, heavy environmental damage, high social costs or major problems of damage recovery or remediation. This should be the starting point of security planning.

Major city centre stations, major bridges, viaducts and tunnels, and iconic structures are obvious targets. The rush hours are probably the most likely time for an attack. This is when the Madrid and 7 July London bombs went off. There is speculation that those in Madrid were all targeted to go off simultaneously in an underground part of a major station, which would have caused the catastrophic collapse of the above-ground section. The three in London on 7 July 2005 were all detonated simultaneously, for maximum disruptive effect.

Railways are high-volume means of transportation. Heathrow airport, the busiest international airport in the world, sees over 60 million passengers a year – over a million a week. But three London Underground lines (District, Northern and Piccadilly) each carry over half a million people a day – three times Heathrow's throughput. Victoria underground station sees more passengers each year than Heathrow, Atlanta or Chicago O'Hare.

When priority targets have been identified, they need to be hardened – made less vulnerable, less penetrable. Responses to threats need to be planned, and these plans need to be tested. Staff need to be equipped and trained: emergency equipment needs to be acquired, maintained and from time to time replaced. Evacuation routes need to be tested, ideally with realistic volumes of people (and the travelling public can be remarkably willing to volunteer to help with these). Are these routes adequate for today's volumes of passengers? Lessons need to be learnt and fed back.

Station access standards may need to be checked – can all stations be evacuated in a sensible timescale? How many stations have two separate exits, in case one is blocked? Are there contingency arrangements for evacuation by train, if evacuation through normal exits is not possible?

Coordination and communications

Coordination and communication is needed with the emergency services and with other transport authorities (including, of course, the airport).

Coordination and communications are important. Could the fire and ambulance services find their way around your stations in the dark if they were full of smoke? Are there up-to-date plans of each station in a secure point where they can easily and quickly be accessed by the emergency services? As with some of the other points mentioned, this has a wider application than a terrorist attack.

What communications and control points are critical to your operations? If one of these was damaged, destroyed or just made inaccessible, how would you cope? What facilities need duplication so that you can continue to operate? What state of duplication is necessary in IT based systems – parallel running, hot standby or cold standby?

Communications strategies are necessary; and these also need to be pre-planned, tested and practiced as far as possible. This involves not only communications with the security services and the media, but also with passengers, intending passengers and those legitimately concerned about people caught up in an attack.

The power of the web needs to be used: your web-site would be a first port of call for many in an emergency, and it needs to be accurate, balanced and kept constantly up-to-date at that time.

Pre-planned announcements and pre-planned publicity are as valuable as pre-planned emergency responses.

Major events – major sporting activities, elections, public parades – are times when a terror attack could be particularly destructive. At the same time, there are likely to be many more people around – people, moreover, unfamiliar with the system. The planning for these events needs to take into account the security factor.

Risk management

Readers are referred to the international standard for risk management, ISO 17799 (see Resources available, page 48). This recommends development of a risk management system containing mitigation measures. Its basis is the identification of assets, threats and vulnerabilities; the quantification of risks; and the controls necessary to avoid, transfer or reduce risks to an acceptable level.

There are four key stages:

- asset identification and valuation, threat analysis, and vulnerability analysis
- asset, threat and vulnerability mapping,
- impact and likelihood assessment,
- risk results analysis

Assets are things of value to the owning organisation and therefore may need protection. They can be tangible (hardware) or intangible (software). They need to be identified: their ownership and value needs to be assessed.

Threats exploit vulnerabilities to create risks. Realistic threats to different assets which are likely to result in serious harm need to be assessed.

Vulnerabilities are deficiencies in assets which can be exploited by threats to create risks.

Assessing threats and vulnerabilities – the process of mapping – can identify likely problems in need of attention.

Impact assessment estimates the harm or loss likely from realistic events. The likelihood analysis estimates the frequency and probability of a threat materialising.

The results for each asset are normally analysed in a matrix, where impact and likelihood are rated high (3 points), medium (2) or low (1) over three risk categories (confidentiality, integrity, availability). Risk level is impact times likelihood: a score of 3 or less is low, 4 – 6 medium and 7 and above high.

The analysis provides the basis for establishing technical, operational and administrative requirements for each asset: this leads to decisions on strategies for accepting, reducing, avoiding or transferring risk (since it cannot be completely removed).

Case study: Mass Transit Rail Corporation Ltd., Hong Kong

In 2003, Mass Transit Rail Corporation Ltd. initiated an Information Security Programme to look at vulnerabilities of key elements of the IT systems. This reviewed the effectiveness of the existing security systems, and then looked at risks and vulnerabilities for those systems which were critical to provision of service and revenue. On completion in 2005, an investment programme was proposed to enhance security controls in accordance with priorities which the analysis had revealed.

The Conditions of Carriage of many transport undertakings specifically exclude terrorism as something for which they accept responsibility. However, this exclusion could well be open to a successful challenge in a court of law. After the attacks on London and Madrid, it is unlikely that an operator could claim that a terrorist attack was so unforeseeable that no specific precautions need to be taken. Nowadays, operators will need to ensure that they have taken all reasonable steps to detect, deter, delay and prevent attacks and to minimise their consequences.

2. Detect

Resources available

Employees and passengers, especially regular passengers, are potentially very useful in detection. They need to be used to spot and report anything odd, anything unusual, by means of awareness programmes.

Passengers are valuable eyes and ears. They are able to spot the odd, the abnormal: they need to be told what to do and how to react if they do so. Several systems use their standard publicity media for this – on-train and on-station poster advertisements, recorded public address announcements, electronic newsletters, timetables and other printed material – in conjunction with a dedicated phone line and an email address for reports. New York's Metropolitan Transportation Authority (MTA) is one of several which uses the message, "If you see something, say something" – a message which might not work in all cultures, but can be valuable.

This kind of public awareness campaign helps to reassure your passengers that you are doing your best, that you are alert to the problems: this can be invaluable in reducing alarm and panic if an attack occurs.

Employees need to be trained and briefed, in what to look for and how to react. The advice of the security services may be necessary in training and briefing staff. Potential threats need to be quickly assessed – is the bag lost property, abandoned rubbish, or a bomb or incendiary device deliberately left? If the threat is real, the area needs to be evacuated and trains either halted or cautioned. The acronym HOT may be useful – is the suspicious item

- Hidden (as a bomb would probably be) – or just dropped, abandoned or left behind?
- Obviously suspicious (with wires and batteries) – or just a food wrapper?
- Typical (like the carrier bag from the local fast-food outlet) – or a well-wrapped parcel?

Case study – British Transport Police

The British Transport Police are to be equipped with portable x-ray scanners, to help evaluate suspect packages.

There is a solid body of experience with dealing with these, but the new detectors add to the versatility of the force and reduce risks to valuable personnel.

The equipment is being supplied by Image Scan Holdings plc.

As a generalisation, security systems need to look for anomalies so that you can decide whether or not these are threats.

Training, briefing and warning needs to be done regularly, to ensure that vigilance is maintained. Some authorities use colour-coded levels of alert – from green (normal) through yellow (vague warnings) and amber (heightened security) to red (a real and credible threat). At particularly high levels of alert, it may be necessary to re-deploy all staff in support of operations staff, to assist in patrolling, reassuring passengers and deterring attacks by their obvious presence. Security staff in high-visibility clothing provide both reassurance and a resource – someone for passengers to report problems to.

A corporate culture of security is necessary. Guidelines and procedures need to be developed for reporting the unusual, dealing with the reports and then analysing for trends.

Anomalies

When your facilities, especially areas like bridges and tunnels, are checked, this needs to be done with people who know what they are looking for – what is out of place. Clearly, a tidy system – with trackside rubbish and left-over engineering materials removed regularly – will assist with emergency inspections by reducing the number of hiding places.

Training in the recognition of abnormal behaviour targets non-standard passengers – those who do not fit the pattern of those normally travelling or are suffering from undue stress.

There is a reasonable predictability about many different types of passenger – the business traveller, the back-packer, the package holiday-maker, the student. They dress, behave and interact with others in reasonably standard ways and when they do this, do not arouse suspicion. Those who do arouse suspicion are not behaving as most passengers do: they are acting outside of these norms.

People wearing bulky or heavy clothing on a hot day, passengers with clenched fists, and people obviously agitated are suspicious.

Staff need to be trained to recognise the signs and how to deal with them – in exactly the same way as Customs officials are trained to recognise people likely to be acting illegally. They need to be able to check their suspicions without alarming potential attackers. One element of this is to encourage staff to make eye contact with passengers. Another is to encourage them to develop non-threatening lines of questioning to assess the suspect individual. This is nothing more than casual chat, to ascertain where a passenger is going and why: only the really unpleasant passenger will react badly to a friendly approach.

There are good reasons why someone might wear clothing different to that of your regular passengers – they might be dressing comfortably for a long flight or for their destination, they might be conforming to their own religious or cultural norms. Passengers on long haul flights with no bags might have sent them in advance, or they might be making a quick trip and therefore need less baggage than usual. They might be wearing bulky clothing to conceal obesity, pregnancy or a deformity.

They might be perspiring or nervous because of illness or stress – and going on a long journey can be very stressful to some.

Nonetheless these signs need to be watched for: staff need to look for the unusual. Moreover having found it, they need to follow it up (which needs training) and be backed up in doing so. A diligent member of staff who reports something suspicious and finds that nothing happens, no-one cares, is unlikely to do it again.

Innocent travellers doing something out of the ordinary are unlikely to react adversely if approached by someone in authority to be asked if they need help. People taking photographs are unlikely to resent being asked what they are doing – and will probably have a genuine explanation. Terrorists or their accomplices, if approached, will probably have thought out a reasonable reason for what they are doing – but the act of being approached will warn them that this may not be a soft target.

Case study - Heathrow Express

Shortly after Heathrow Express staff had been trained in dealing with of abnormal behaviour, two of them, using their training, approached a couple of people acting abnormally at Heathrow's Central Terminal Area station. The couple turned out to be illegal immigrants.

Television-based security systems

CCTV is useful around depots and other major facilities as well as on stations and trains.

Proper installation is important.

- A good level of lighting is necessary for it to be really effective.
- Installation needs to be properly done, or high winds will cause poles to sway and you may lose some of the images.
- Areas where passengers are most vulnerable need most surveillance.
- Cameras should be sited where people cannot avoid or damage them.
- They should also be positioned where they cannot be obscured – maliciously or by growing vegetation.
- Coverage should extend into the surrounding area.

Experience has shown that CCTV alone is ineffective: it needs to be combined with police patrols and prompt responses to problems.

Intelligent CCTV systems are being developed to detect unusual behaviour.

- Normal patterns of crowd flow, crowd speed and congestion are predictable: exceptions can be flagged up.

- Unusual activity like loitering can trigger closer examination by CCTV: images can be examined closely at leisure and if the activity is repeated or leads to an incident, used for detection.

- The same images can be put into a face recognition database, to alert security officers to a repeat appearance: face recognition techniques, to permit intelligent CCTV to recognise known terrorists, are being developed.

- Motion prediction software in CCTV systems can also be used to detect unattended parcels.

- Some systems can also detect when a bag and a passenger become separated, and flag this up for investigation.

Case study: Tokyo Metro

In October 2005, the Japanese Ministry of Transport announced plans for a 3-month test of a facial recognition system on the Tokyo Metro. The system, developed jointly by NTT and an American company, was to be installed at the ticket gates at Kasumigaseki station (near the seat of government in the city) in April 2006.

It is designed to analyse the facial characteristics of passengers and compare them with a database of 1000 terrorist suspects, and alert the police when a match is found.

The system can check 1000 people a second.

Also available are video security software products, some of which use a combination of video and microwave motion technology. This can, for example, highlight people going the wrong way in sensitive areas (using the exits to effect an entrance), people throwing objects over a fence, tailgating (two people using an entrance when only one has been authorised) and loitering.

Case study: Boston Logan airport

Massport plans to use CCTV and sensors in combination to monitor the waterfront perimeter of the airport. When abnormal movements are detected by sensors, cameras are automatically focussed on the area involved and security staff are warned of a possible intrusion. The software can "learn" what is normal – birds and aircraft – and the cameras work in conditions of low visibility.

Similarly, CCTV can be combined with thermal imaging for perimeter security. The sensors will detect and flag up abnormal heat sources – possibly intruders.

Case study: Airtrain JFK

Airtrain JFK, the elevated railway connecting the terminals at New York's John F. Kennedy International Airport with the New York subway and the MTA Long Island RailRoad, selected Verint Systems Inc. as supplier for a networked video solution to enhance system security.

The system uses intelligent software to monitor the output from the CCTV cameras in lifts, on passenger platforms and on key sections of the track. The software analyses what it is seeing – evaluating both real-time and stored data - to assess behaviour patterns. Anything abnormal is flagged up for investigation.

Intelligent CCTV may help detect pick-pockets and car thieves as well as terrorists. It can also deter the vandal and the graffiti artist.

However one major issue is retrieval of data after the event – how easy is this? After the 7/7/05 attacks on London, downloading images from hard drives was a long, expensive and frustrating business. This needs to be discussed with system suppliers.

Another issue is the number of false warnings given – this can normally be found out by a limited scale test. See page 30.

Case study: First North Western.

The UK train operator First North Western installed CCTV in a new fleet of trains. Cameras were fitted both in the passenger compartments and also facing forwards to detect people on the track. The equipment was supplied by Faiveley.

Random searches – or the threat of random searches – of passengers or bags or both can be a deterrent.

The ability to search passengers in particular is restricted by law in some places, so the legal aspects of this need to be watched (see page 36 and, for US views, TRB's Legal Research Digest 22: the Case for Searches on Public Transportation).

CCTV too is seen in some places as an intrusion on privacy, and installation needs to be tactfully bundled with good passenger communications. Whether or not required by local legislation, it is good practice (and reassurance) to warn people that there are cameras around. The message, "Smile, you are on TV" was used by one UK train operator.

3. Deter and delay

Introduction

Terrorists will probably have a range of targets in mind for their attack. These targets will be reconnoitred to help them decide on priorities and preferences. How much damage could an attack do in each of the possible locations? How easy will it be to undertake – and, maybe, to escape afterwards?

Your deter and delay policies need to persuade them that you are the wrong target – that it's all too difficult.

Security by design

Ideally security should be built into systems: it should be part of the design. The concept of Crime Prevention Through Environmental Design (CPTED), which was developed by the British Transport Police in response to the IRA attacks on London in the last century, may be useful here.

Retro-fitting security may not be easy with legacy infrastructure, but it needs to be considered.

Priorities for surveillance devices and intrusion alarms should be based on an assessment of risk.

Your protection systems need to increase the effort, to increase the risk involved in an attack. Easy targets will be chosen in preference to hard ones. The kinds of CCTV protection described in the previous section (see page 13) are evidence to the potential terrorist that this is a hard target: they are all part of a deterrence strategy.

Even signs warning people of the presence of CCTV surveillance measures may help deter.

Intrusion detectors (including motion sensors) and alarms are needed, both for buildings (offices, signal-boxes, control rooms) and sites (depots, key points of vulnerable infrastructure).

An increased visible police presence, including frequent security patrols, is a reassurance to passengers as well as being valuable in deterring attacks.

Public and private areas

There needs to be a clear boundary between public areas and private areas. The latter need to be protected by access control systems (keypad or card activated doors, for example) so that in the event of a bomb warning, they are lower priority areas for search.

"Tailgating" – holding a door open for a person following you in – is basic courtesy. But if you need a key-code or swipe-card to access a building, that courtesy is misplaced. See page 14 for a possible defence.

Staff need to be briefed in security measures for private areas – they need to be told to challenge the unusual, for example.

Public areas need surveillance and patrolling to ensure their security.

Infrastructure

The entrances to important bridges, viaducts and tunnels (and potential access points like ventilation shafts and emergency exits) need protecting with perimeter protection systems like security fencing, intrusion detectors, motion sensors and CCTV.

Fencing can be a neglected element of security. It can delay attacks, and define where illegal entry starts.

There are places where the railway is used as a short-cut by local residents and the fencing is damaged so frequently that no-one bothers to report or repair it any more. The dangers of this approach are obvious, but people can be reluctant to continue to spend when they know that damage will recur almost immediately. However, it is clearly a serious issue – the innocent and the not-so-innocent should not have access to the tracks – and action needs to be taken. This can range from a regular police presence to warn trespassers to consultation with local people to try to get a formal safe crossing point installed where it is necessary. It should be noted that the IRA bomb attacks on England in the last century sometimes used access points created by trespass.

Some railways have iconic structures – features which almost define the railway. In the UK, the Forth Bridge, the Ribblehead Viaduct and St. Pancras station are known nationally as is the Flåm line in Norway and the Øresund fixed crossing between Denmark and Sweden. Here, it is probably worth installing alarms and intrusion detection devices on the fences. The Channel Tunnel Rail Link is well protected for a variety of reasons: the level of protection here is probably excessive for the average airport railway but an example of what can be seen as necessary.

Being alert to cars waiting with no obvious purpose is a deterrent. People waiting with good reason will not mind being challenged. The same car waiting in the same spot on more than one occasion is clearly a suspicious event.

Layouts which maximise visibility and minimise the number of hiding places are optimal both for security and for reducing opportunities for casual vandalism, assault and theft.

Transparent waiting shelters remove places to hide.

Good lighting helps too. It needs to be positioned to

- highlight anyone approaching,
- conceal security guards and
- enhance the performance of surveillance cameras.

Major stations

Protecting major stations is always a compromise between the needs of the travelling public and the need for security.

There may be a case for testing or modelling the air flow through major stations especially if they are sub-surface or underground. If toxins or poison gases were released, where would they go? In case of fire, where would the smoke go? In the light of the outcome, escape and evacuation routes may need to be changed to avoid danger.

What is feasible?

Creation of safe zones like the airside part of an airport is unlikely to be possible. There are too many access points, and too much need for immediate access. So you can only deter: you cannot totally protect by allowing access only to those who have been searched and screened.

The IRA bombing campaigns in the UK exploited simple gaps in security – gaps in fences allowing access, poor lighting allowing activity to be concealed, litter bins and blind corners allowing bombs to be left un-noticed. Lessons learnt were as follows.

- Keep fences repaired, especially those near roads. Bombs placed on railways tend to be brought to the site by car.

- Improve lighting – to deter attacks and to improve observation. This needs to be done carefully – in some places, lighting outside rather than inside a perimeter fence is necessary, to illuminate attackers rather than defenders.

- Devise credible rubbish policies. Blast-proof bins are fine but expensive. “Take your litter home” publicity campaigns can work reasonably well, depending on the culture of the country: they may need to be combined with regular litter-sweeps, to collect things which always will get left lying around. Transparent plastic sacks, regularly emptied, can be useful: they can be inspected quickly.

- CCTV is valuable for protection and for the capture of offenders.

- Raise awareness by publicity.

- Train employees to report suspicious activity, and to identify suspect packages.

- Improve evacuation and emergency plans.

- Use all means of communications to advise on threats, service disruptions and alternative routes available.

- Prepare for hoaxes and false alarms.

- If a system is vulnerable, it will be a prime target for attack.

4. Prevent

Security plan and threat assessment

A security plan is a good start point for prevention.

Your system needs a thorough risk assessment to see where the vulnerable points are, where the high-profile targets are, where the threats are or might be. Which parts of the system are particularly important? Where is there

- high potential for loss of life
- the likelihood of serious impacts on the functioning of the area
- potentially a high level of environmental damage or
- somewhere where recovery or replacement will be very costly or difficult?

This assessment needs to be coupled with a parallel assessment of your security measures and programmes, and those of other bodies like the police.

Case study – MATRA

Following a 2002 report on aviation security, the UK government set up a Multi-Agency Threat and Risk Assessment process at UK airports. Under this, all those with an interest in aviation security at that airport worked together to agree a risk register, and to identify actions required to mitigate risks to an acceptable level.

The process was supported by a secretariat which promoted best practice and monitored progress.

Threat assessment models are available from places like the American Society for Industrial Security and Sandia National Laboratories (see page 48, Resources available).

Both suggest a similar sequence of steps.

- Describe what is there – the facility and its major functions.
- Identify critical assets needing protection – key points (including control points and IT centres) and people.
- Evaluate the iconic status of the facility – in national, social or economic terms.
- Evaluate its proximity to places of iconic status – could an attack on a nearby building of national significance impact on the railway?
- List the major vulnerabilities and evaluate the likelihood, the probability of an attack.
- Evaluate existing security systems and assess their adequacy.

- Set out a list of mitigating measures to reduce the potential for harm to your organisation if the vulnerable points were attacked.

Fencing

Transportation facilities are only vulnerable if they can be reached. Controlling access is a vital part of security, of attack prevention.

Railways, by their nature, occupy long thin stretches of land. Some countries make it the responsibility of the operator to fence the railway: in other places, it is either voluntary, obscure, or an obligation of a neighbour. Inevitably there are gaps: are they where it really matters? This is where the vulnerability analysis referred to on page 7 is useful. The priorities – where high-quality fencing, regularly inspected, is necessary - are the high profile and the high value targets.

Some railways are obstacles, severing communities or separating trip-ends: some people ignore bridges and underpasses in favour of unauthorised crossing points, deliberately damaging fencing in order to use them. The 2-metre high palisade fence is favoured by some railways, but this is very vulnerable to someone with a crowbar removing one of the uprights to create a way through.

These unauthorised routes need to be dealt with – both because of general public safety issues and because of the potential for terrorist access.

Perimeters can be protected by lighting and cameras, and by sensors or radar systems which can differentiate between animals and people.

Intrusion detection sensor technology has improved and come down in cost with improvements in IT – in particular, in digital signal processing. Available technologies include the following.

- Active infra-red sensors. This technology uses a beam from an infra-red emitter (usually a light-emitting diode) to a receiver at the other end of the detection zone. If the beam is broken – perhaps by an intruder – a warning is given.

- Electric field wires. Parallel insulated sensor wires are installed, on their own or on stand-offs on an ordinary fence. Movement of or between the wires is detected by a change in electrical capacitance.

- Electrified barrier – the classic electrified fence, giving a non-lethal shock to an intruder (and, usually, raising an alarm).

- Fence disturbance sensors. Vibration, motion, and acoustic sensors can be built into a normal fence so that attempts to cut or climb it can be detected.

- Magnetic sensors. These are buried wire loops or coils, sensitive to the movement of ferrous metal (which induces a current to raise an alarm).

- Microwave sensors. Bi-static radar is normally used in perimeter fencing. It uses two antennæ – one to transmit, one to receive – to detect motion. It works between two inter-visible points.

- Passive infra-red sensors. These can detect the movement of heat sources (like people).

- Ported coax (also known as guided radar or leaky cable). This relies on disturbances to an electromagnetic field around a buried coaxial cable.

- Pressure sensors are buried pressure-sensitive devices (tubes of pressurised liquid connected to pressure sensors, or sensitive fibre-optic cable). They detect the presence of an intruder by means of changes in pressure.

- Seismic sensors. These are buried sensors capable of detecting the presence of an intruder by the sound and vibration of their approach.

- Surface wave sensors. An electro-magnetic field is created around a pair of parallel wires supported by non-conducting poles. An alarm is raised when the field is interrupted.

- Taut wire sensors. Parallel wires in tension are connected to sensors (switches, piezo-electronic sensors or strain gauges). When they are displaced, an alarm is given.

- Video motion detectors (VMDs) process video signals from CCTV cameras, and report changes in contrast in specific zones.

Case Study: Washington DC

A pilot smart detection system is being established on a 12 km north-south freight corridor through Washington DC – a route which goes close to a number of sensitive areas, including National Airport.

Freight wagons entering the corridor will be tested automatically for chemical leaks. Sensors will detect the presence of intruders and simultaneously warn them off and alert the police.

Partly this responds to concerns about hazardous materials passing through the nation's capital: it also provides more security and tests equipment in the real world.

Protecting installations

Among the key targets could be the major signal boxes (interlockings) and the control rooms. These need access control measures to ensure that only authorised people are allowed in. There will be a hierarchy of lines of defence – operators will not wish to keep interested professionals from studying their facilities, but will certainly wish to keep the casual passer-by away.

Biometric access control systems are more effective than keypads or card readers, but more difficult and more expensive to use: they should be installed in the highest profile locations. Such systems can give a false sense of security – the assumption that they are foolproof – but at all four stages (enrolment, data storage, data acquisition and matching) there is scope for people to circumvent the system (see "Biometrics at the frontiers: assessing the impact on society" in the Resources section, page 49).

Turnstiles – of the manual or electronic variety – are more secure than keypads or badge-based systems. It is human nature to hold a door open for someone following close behind: the follower may not be an authorised person.

Intrusion alarms and motion sensors, possibly linked to CCTV, should also be used in high profile targets.

CCTV is a valuable deterrent. However the problems of monitoring need careful consideration – there are limits to human attention. Intelligent systems which flag up unexpected movement are particularly useful (see page 13).

Security guards and police patrols are valuable deterrents. Again, prioritisation is necessary to ensure that the high-value targets are best protected. Those involved do need to know what they are looking for – what is out-of-place – so guards will need training or escorting by professionals.

Bridges and tunnels are vulnerable targets. This is partly because they are difficult to replace, and partly because an emergency in a bridge or tunnel is more difficult to handle because of access issues. Access points need to be protected by fencing and CCTV, and communications need to be checked regularly for adequacy.

Case study – New York

The MTA Long Island RailRoad has installed clearly-marked emergency telephones at regular (125 metre) intervals in the East River Tunnels in New York. Fire protection systems (a tunnel standpipe system and wall-mounted chemical extinguishers) have also been fitted.

Tunnel ventilation is an issue linked to general safety concerns. Fans to clear and direct smoke are common in new tunnels: retro-fitting into old tunnels may need consideration. Modern systems (as in the Channel Tunnel between England and France) are designed to blow smoke away from passengers: passengers find safety by walking towards the wind.

Other general safety measures in tunnels – again, common in new ones – include evacuation walkways, handrails, signage and ladders. These can be difficult to retro-fit to old installations, but nonetheless evacuation plans need to be developed in case of an emergency.

At times of high security, overbridges may need to be patrolled or inspected underneath – from the water, if over waterways.

Protecting trains

London Underground and the London rail network generally was hit by a number of bomb threats in the 1970s.

One response was to make tampering with seats obvious. This was done by a system of brightly-coloured security tags: if the seat cushion was lifted to put a bomb underneath, the tag broke and the break was easy to spot.

Another response was remove litter bins – good places to leave bombs. This illustrates the compromises necessary – people will leave litter (more in some cultures than others) and there are limits to the effectiveness of "Take your trash home" publicity. The expensive way of resolving this is blast-proof bins: the low-cost way is transparent bags which make inspection of the contents easy (especially if emptied regularly). There are limitations on the effectiveness of blast-proof bins: the bombs used on 7 July in London are reported to have contained around 4 kg of explosives, which is an amount which can be easily carried.

Routine inspections of trains as they leave depots for the first services of the day may be valuable, especially at times of high risk.

Some – but not all - railways have found ticket barriers effective, not just for revenue protection but for deterring casual crime. If a ticket is necessary to access a station platform, it deters some vandalism. Some airport railways try to avoid having barriers (because they are difficult for people with baggage to negotiate) but they do have their advantages.

While airport-style individual processing of passengers through x-ray and screening portals may not be practicable on most railways, technological developments need to be watched. Explosives detection devices and millimetre-wave imagers may help to monitor passengers to detect the suicide bomber.

On an Airport Express, it may be possible to scan bags using standard airport equipment (this is done on Eurostar and on the maglev to Shanghai Pudong airport). Airport security people will be able to advise on practicalities like space requirements, throughput and staffing needs.

Case study – combined millimetre wave and video

A system developed by Brijot Imaging Systems in Florida combines imaging systems to reduce the public disquiet at the intrusiveness of millimetre wave scanners.

If the millimetre wave detector finds a weapon, this is flagged up on a conventional video picture of the carrier, telling security staff where the gun or knife is hidden.

The company propose the use of this in a narrow passage (or possibly a set of parallel passages – like ticket barriers, for example) where passengers have to pass through one at a time. Most passengers would pass straight through: suspects would be diverted for further examination.

An alternative on railways with a higher throughput may be explosives detection devices. Technical developments in these may make them possible in places like ticket machines, ticket barriers and on escalators. This is covered in the next section.

As ever, there is a need to be alert to future developments.

Mobile phones.

It should be noted that the Madrid bombs were triggered by mobile phones.

These were however just used as timing devices, not communications devices. Therefore the idea of making train windows impervious to radio waves would not have prevented the Madrid bombs.

5. Explosives.

General

Systems for detecting explosives need to be considered, especially following the bomb attacks on the Madrid suburban system in March 2004, the London Underground in July 2005 and the many suicide bombings in the Middle East.

A range of trials was conducted in the US in 2004 on rail systems: these are described below.

Transit and Rail Inspection Pilot

The pilot screening programme, known as TRIP – Transit and Rail Inspection Pilot, has had three phases.

In the first, in May 2004, tests were conducted at New Carrollton station, in Maryland, to check passengers and their bags for explosives before they were allowed to board trains in the morning and evening. The station is an interchange point served by both Amtrak and the Washington Metro.

The baggage screener used in the trial – by L-3 Communications, using multi-view tomography - was capable of scanning 1800 bags an hour automatically: it had a high-speed conveyor and large tunnel to accommodate large items.

Passengers were asked to enter a portal where they had to stand for a few seconds while air was puffed over them before being asked to leave. The air was checked for traces of explosives.

It reportedly took 12 seconds to check each passenger. Testing took place 8 hours a day over 30 days, and was supplemented with random screening by sniffer dogs.

Throughput would be adequate for most airport railways - Heathrow Express has about 1500 passengers in a peak hour, and not all have baggage.

The conclusion was that it was suitable for use at some locations likely to be terrorist targets, but not those with a high throughput.

Phase II, at Washington Union station, tested equipment for screening checked baggage and cargo before it was loaded onto Amtrak trains, and also screened unclaimed baggage and temporarily stored items at the station.

Screeners from the TSA inspected luggage, along with temporarily stored personal items and cargo.

This built on the earlier test. According to a statement released by DHS, "TRIP Phase II is expected to yield important data on the effectiveness of screening equipment in a non-climate controlled environment, cost, and impact on Amtrak operations."

Boarding passengers were checked for explosives using detection equipment similar to that employed at New Carrollton. The TSA required everyone to enter their train through a single door in the rear car. After examination, each person had to take their carry-on baggage up a narrow stairway to the second level and walk through all or part of the train, then downstairs to luggage storage bins, then to their seat – not the most user-friendly system possible.

The equipment worked, but its bulk and expense made it unsuitable for system-wide implementation.

Phase III – testing the feasibility of on-board x-ray screening of passengers and their bags for explosives on a moving train – started in July 2004 at New Haven station, on the North East Corridor (and one of the places to which Continental Airlines code-shares with Amtrak).

This phase used a Shore Line East commuter car normally running between New Haven and New London. The equipment fitted into ordinary railway carriages without extensive modifications, and testing did not disrupt normal rail operations and logistics for boarding passengers. TSA staff were present up to 11.00 and from 16:00 to 21:30. Hand baggage was screened for explosives, as were tickets (and this test showed whether explosives had been handled recently). Secondary follow-up checks were carried out as necessary, and police were also at the station in case firearms or drugs were discovered during the checks.

Testing tickets for explosives residues was not infallible. Many systems are using contactless smart cards: these do not make enough contact for the residues to be detected. Moreover, the carrier may not have actually handled explosives: they could just have been given a back-pack containing them. In that case, there would be no residues to detect.

An alternative may be to test samples of the ambient air, but these detectors too have their limitations. Certain perfumes can cause false alarms: they give a similar reaction to some home-made explosives. Re-configuring detectors to react only to commercially-available explosives would mean that they would not detect the home-made explosives.

Then what?

Technology is being developed by General Electric and Cubic to detect explosives residues from a finger touch as a passenger buys a ticket at a vending machine. If explosives are detected, an alarm is activated and a digital camera immediately transmits a photo of the purchaser to the police. The ticket is encoded so that it does not activate the barriers. This is likely to be commercially available from 2008.

Screening on a moving train may be efficient in terms of passenger loading and throughput, but it does raise issues about what to do if explosives are detected. How would passengers carrying them be dealt with?

The same issue (and need for planning) arises at stations. If testing equipment at a station gave an alarm, what would happen? Plans for this – an immediate alert to the police, probably a warning to train drivers not to stop at the station – need to be devised and rehearsed.

Alternative methods of screening at stations

An alternative technology is the explosives trace portal (ETP), as used in Phase I of the TRIP project described above. This is structurally similar to the airport metal detector, but blows several puffs of air at individual passengers and analyses the air for explosive materials.

At some of the busiest airports, this is used in conjunction with an x-ray backscatter system, which creates photo-like images which can reveal weapons or explosives. This is unlikely to be suitable for frequent train services, since the time taken for an inspection is likely to be long.

Structures

Structures need to be protected against explosives – bombs and suicide bombers. The improvised explosive device (IED) is a popular weapon among terrorists.

An explosion is a rapid chemical reaction, producing a very hot high pressure gas virtually instantaneously. This will create strong blast waves in the surrounding air: these will move outwards from the source, gradually reducing in strength and velocity. These waves will impose loads on structures significantly higher than the design loads: these will be of short duration, causing local failure possibly leading to progressive collapse.

The first points to suffer will be the windows. Windows and glazed areas can be fitted with blast film (to prevent glass from shattering and shards flying around the room, turning windows into weapons) or anti-blast curtains (tight-mesh curtains, with a lot of material weighted at the bottom, to retain glass fragments). The windows themselves need to be strong enough to resist the blast – the frames, particularly in exposed spots on lower floors, need to be secure against a bomb.

Keeping explosives away from structures is an obvious precaution. Bollards can prevent vehicles approaching a building – but they need to be fit for purpose, and not merely decorative. Features like planting, low walls (possibly incorporating benches) and steel fencing can be more than decorative – they can help attenuate the blast.

Ideally lower walls of vulnerable buildings should have few windows (although they can be covered with a curtain wall, to look as if they are completely glazed): these areas will be closest and most vulnerable to the blast.

It can be valuable to identify Bomb Shelter Areas in buildings likely to be damaged by a bomb. If evacuation was unwise (because of a car bomb outside, for example), people could assemble in the designated area. This needs to be identified by a structural engineer. It will be away from external walls, doors and windows, and surrounded by masonry or concrete walls. It should not be connected to external doors, so stairwells to the ground floor often cannot safely be used for this purpose.

A mortar attack can be improvised from the back of a lorry (as was done some years ago at Heathrow Airport) or from a suitable area of flat ground. Potential mortar launching points can be identified and included in routes to be patrolled at times of particularly high security.

Trains

Trains in confined spaces – like tunnels - are more vulnerable than those in the open. This is because in a tunnel, the blast cannot escape, cannot be diffused into the open air: all of its force is spent on the train and its contents.

The potential for panic is also greater underground.

Signs

A suicide bomber will generally wear the bomb under clothing – so a heavy bulky jacket or voluminous garments are necessary. These stand out on warm days. A smell of chemicals, or dangling wires, are other suspicious indicators. A clenched fist may be holding a detonator. Agitation or tension is natural.

None of these are proof positive of a bomber, but they are all indicators of the possibility, and need to be watched for by staff. Staff need to be trained in what to look for and how to deal with it – see page 12.

Intelligence

The police and security forces will monitor general threats to the best of their ability: transport organisations need to work closely with them to ensure that intelligence is quickly passed on. This will help when developing a tiered level of security, for example (see page 43).

Dogs

Specially trained sniffer dogs – sometimes known as K-9 teams, especially in North America – can be effective against explosives. They can detect minute traces. They can also be trained to detect guns, or people buried in rubble.

They are usually trained to chase and subdue a carrier, rather than to attack.

They are expensive – to train and maintain – but a good deterrent and a valuable reassurance to passengers.

False negatives and false positives

When equipment gives a warning that something is wrong, there are four possibilities illustrated in the diagram below. The diagram is set in the context of explosives detection, but the same argument holds for any warning device.

		The real situation	
		Explosive present	Explosive not present
The warning equipment says	Explosive present	True positive	False positive
	Explosive not present	False negative	True negative

A False negative is the worst possible result – the equipment wrongly indicates safety. But too many false positives will lead to unnecessary delays and disruption, and possibly bring the whole system into disrepute so that people ignore it.

Systems need to be tested on a small scale before full implementation to see whether the level of false results is acceptable.

6. Chemical, radiological and biological threats

Detection and alert systems are needed for these so that communication of the nature of the problem can be done as quickly as possible. Protective clothing (for example gas masks), and training in its use, may be needed by first responders, or they could add to the casualty count. Decontamination systems for stations and rolling stock will be needed so that services can be quickly restored.

Chemical

"A chemical attack is the spreading of toxic chemicals with the intent to do harm" ("Chemical attack – warfare agents, industrial chemicals, and toxins" fact-sheet from the US National Academies and the Department of Homeland Security).

Harmful chemicals include military chemical weapons, toxic industrial and commercial chemicals, and toxins of biological origin like ricin.

This is probably the most serious type of attack of this kind – transportation of harmful materials is relatively easy, and results are instant and long-lasting.

The fact-sheet quoted gives extensive and valuable advice on usage, symptoms and protective measures, as well as a list of web-sites with more information.

Case study - Los Angeles MTA

When the subway system in Los Angeles was built, there was concern about leakage of methane gas into the tunnels, so sensors were installed in critical places.

These are now being upgraded to detect other chemicals which might be used by terrorists.

Case study – MBTA Boston

MBTA Police use mobile chemical detection equipment to test passenger luggage for traces of explosives or other dangerous material.

Radiological

"A radiological attack is the spreading of radioactive material with the intent to do harm" ("Radiological attack – dirty bombs and other devices" fact-sheet from the US National Academies and the Department of Homeland Security).

This is relatively easy way of exposing many people to physical damage.

This fact-sheet gives extensive and valuable advice on usage, dangers, protective measures and long-term consequences, as well as a list of web-sites with more information.

Biological

"A biological attack is the intentional release of a pathogen (disease causing agent) or biotoxin (poisonous substance produced by a living organism) against humans, plants or animals" ("Biological attack – human pathogens biotoxins and agricultural threats" fact-sheet from the US National Academies and the Department of Homeland Security).

This kind of attack is particularly serious because its effects may not be detected for some days after the attack – by which time carriers could have spread the material widely.

The fact-sheet quoted gives extensive and valuable advice on the impact, danger and protective measures, as well as a list of web-sites with more information.

Case study: WMATA

At the end of 2005, Washington Metropolitan Transit Authority went into a partnership with the Lawrence Livermore National Laboratory to evaluate options for response and recovery after a biological or chemical attack.

The 6-month project built on the system's chemical detection system. It involves collaboration with police, safety and emergency operations officials to develop a plan to identify and clarify roles and responsibilities at all levels in responding to a release of chemical or biological material on the transit system.

The team will also look at clean-up and decontamination issues.

Precautions

In the event of an attack, employees may be required to stay inside a building for an extended period of time - for example, if there is external radioactive contamination. Internal areas need to be designated and equipped so that people can remain there for a minimum of three hours while the surroundings are assessed and cleared. Toilets, water, snacks and adequate seating need to be available.

Spare clothing may also be necessary. If people have been exposed to contaminants, they will need to remove exposed clothing – partly to avoid contaminating others, and partly so that the clothing can be used to assess the dosage received.

Isolation or evacuation (or both) of affected people – passengers, staff and anyone else involved - may be necessary. Train services may need to be stopped to prevent spread of hazardous materials, as may ventilation systems in buildings.

Air-tight containers and liquid sealant may be necessary as part of the emergency equipment to collect or make harmless suspect packages or fluids.

The US Department of Homeland Security has conducted tests with non-toxic traceable gas in New York's Grand Central station to assess how dangerous gases might flow through the station. This was to help develop emergency plans, assess escape routes, and decide where ventilation systems needed improvements.

Clearly, this is a sensible test to make, although computer modelling techniques may well be adequate to obviate the necessity for the release of real gas in a real station. These would also check the value and adequacy of equipment like ventilation fans, which properly used might be able to contain harmful materials.

7. Fear

Disruption, fear and panic are powerful weapons. During the Iraq war, there were people who, quite rationally, would not use the London Underground: being caught in London in a terror attack would be bad enough, but being trapped underground was seen as far worse. The media, by their policy of emphasising the bad news, exacerbate this kind of reaction.

Research published in August 2004 by Group 4 Securicor said that 36% of those who were now more afraid to travel attributed this fear to the threat of terrorism.

If you have a strong public awareness campaign, if you are obviously prepared for attacks, this can reassure passengers. An attack on any part of the public transport system can raise fears about the next target: if your system is obviously a hard target, ready, vigilant and alert, it will reassure your passengers as well as deterring the attack in the first place.

Signage about unattended parcels needs to be monitored regularly – is it all up to date and all visible?

Even more important is signage for emergency evacuation routes – is this immediately visible? A natural reaction among people is to try to escape using the way they came in – which may not be the quickest way. You need to ensure that emergency egress points are obvious (and, for the prevention of false alarms, that exits which are only for use in emergency are clearly identified).

Your staff are essential in convincing passengers that there is a real emergency and in reducing panic. If they know what to do, are obviously doing it and are communicating this to passengers, it helps. Staff on the ground at the site of an incident will, of course, need to be reinforced as quickly as possible.

8. Fire

The use of fire as a means of attack can be countered by methods used by railways to inhibit fire generally.

Fire detection systems, especially in enclosed spaces, are valuable. Air-sampling smoke detection systems are currently considered the most reliable.

Materials used in trains and on stations needs to be highly fire resistant. It also should not give off toxic fumes when heated.

Case study – the Royal Navy

The adverse reaction of materials under stress has been noted in "The rules of the game" by Andrew Gordon.

In the Battle of Jutland, the work of the fire-and-repair parties was hindered by the fact that lead-coated copper wires were fixed above the main passage-ways. The copper conducted heat from flames some distance away, melting the lead which dripped onto the heads of people using the passage-ways.

In the Falklands Conflict, it was found that the laminated panelling used in some ships splintered into lethal shards as a result of the shock and heat of an explosion nearby.

Prompt removal of rubbish, and standards for materials on sale in underground station retail and catering outlets, also help reduce the risk of fire.

Systems for extracting smoke – especially fans in tunnels – need to be investigated. However, it is probably more valuable to ensure that well-signed evacuation systems are in place, so that vulnerable passengers can be removed from the system as quickly as possible.

This was certainly true in investigations at London's Victoria station in the 1990s. A significant part of the station is underneath a commercial development with a low roof. Increasing the number of emergency exits and improving the signage was far more effective and significantly cheaper than a smoke extraction system; and it also met the needs of the fire service (who wanted all passengers evacuated so that they could deal with the fire without worrying about anyone in the way). It was relatively easy to develop new emergency exits, by adding creatively to what was already there.

Equipment which might start a fire should where possible be contained in services rooms, equipped with sprinkler, fire detection or fire suppressant systems.

Arson has been used against Japan's Narita Express, probably by people opposed to expansion of the airport.

9. Baggage.

Baggage can be used as a carrier for many means of attack – explosives, biological, chemical and radiological weapons, and fire. Most items of baggage will be innocent, fortunately: the problem is finding that which is not.

Specially trained dogs – canine or K-9 teams – can be useful for checking baggage for explosives, as well as for routine patrols of trains and stations.

Random searches are a valuable deterrent, and most people will cooperate with reasonable requests especially if they are dealt with sensitively.

Some US transit authorities insist that passengers make their bags available for search: passengers not willing to allow this are not allowed to travel. The British Transport Police tell passengers that they may be asked to submit to a search: if they are, they will be given information about their legal rights. A clear and reasonable policy – possibly risk-based – needs to be developed here, based on local laws and conditions. Staff need to be trained and briefed accordingly.

It can be a valuable reassurance to passengers to ask them to identify bags in overhead racks and in luggage stacks. It is usually not difficult to put a bag on a train and either not ride it or alight without the bag at an intermediate station – this was done in the attacks on the Madrid suburban railway system.

In-town check-in is a special case. Typically bags are checked in, usually by airline or ground handling staff: passengers are asked the standard security questions, documentation is checked and a boarding card issued. Bags are then usually carried in a dedicated secure area of the train (or occasionally by road): they can be loose loaded or containerised. Heathrow Express used fire-proof containers, with special locks to ensure that any attempt at tampering was obvious. However they are transported to the airport, once there they are treated as transfer bags and screened for illegal contents.

Is this adequate for an airport railway?

Logic says yes. Someone wanting to put a bomb on a train could find an easier and cheaper way than buying an airline ticket, going to the downtown check-in and checking in a bag. They are likely to want to avoid detection: presenting documentation at check-in is not the optimal way to do this.

10. The airport station – the interface

Introduction

The airport station is the interface between the railway environment and the aviation environment. Interfaces are places where particular problems can arise.

Working together

Jurisdiction is one issue. Which authority deals with crime, emergencies and security issues here – the railway authority or the airport authority? Is there a boundary issue? Can airport police deal with crime on the railway and the other way round? How good are the communications between the different organisations? How well do they work on the ground – can railway police radios talk to airport police radios? Do both work underground (if part of the airport railway is underground)?

Allied to this is regulation. Railway security and aviation security tend to come under different parts of government – even if they all come under one government department – and different inspectors can ask for different things. Reconciling the two – reaching a sensible compromise or deciding on one viewpoint or the other - is sometimes not easy.

Anecdotally, this is rarely a big problem, especially on the ground where professional people tend to work well together. It is, however, a point to be aware of, especially where a new airport link is being built.

Case study – the VIPER project.

In December 2005, air marshals in the United States started riding mass transit systems in a counter-terrorism surveillance test programme.

This used both under-cover plain clothes officers and uniformed TSA staff, usually in teams which also included a bomb detection dog team and local law enforcement officers.

The test was called VIPER – Visible Intermodal Protection and Response – and took place on Amtrak's Northeast Corridor, railway lines in the Los Angeles region, ferries in Washington State, the bus station in Houston, and mass transit lines in Atlanta, Philadelphia, Washington DC and Baltimore.

It was, apparently, an ambition of the TSA to expand their capabilities to surface transportation. The ambition was reportedly thwarted: the test was scaled back amid concerns about communications, coordination and the willingness of local officials to cooperate. Some transit authority staff claimed not to have been consulted: others were just hostile to the presence of TSA staff on their system.

There were also fears about air marshals being diverted from their primary role (although, of course, far more people ride transit than fly! – see page 8); and because a full risk assessment of the transportation system has yet to be completed, proper priorities were difficult to assign.

Another issue is standards. What are the standards for things like CCTV - including warning notices about their presence, quality of data recorded, coverage, and storage of (and access to) images?

Evacuation and closure

What happens if there is a need to close or evacuate the airport or the station or both?

There are different scenarios possible here, which all need to be thought through as part of the planning process.

An airport might need to be closed for a short period for an emergency – a small fire, a hijacking, a security threat. Liaison with the railway operator may be necessary, especially if flights are going to be diverted: passengers (including meeters and greeters) need to be warned to check the situation before they travel.

If there is in-town check-in, this will give rise to a range of issues – for example, how are bags already in transit dealt with? Passengers will want to know!

Evacuation of the airport, or closure for a period longer than a few hours, would give rise to different needs. Railways are inherently a high-capacity means of transport and can move large numbers quite quickly. This capability is not necessarily usable immediately because rolling stock and train-crew might not be available: the necessity to divert these from their normal roles would depend on the scale and nature of the problem. But even the ordinary airport service can be used to move substantial numbers in an emergency: passengers will be reasonably tolerant of crush-loading conditions if they understand that it is necessary.

If there is a need to close an airport station, intending passengers will need to be told as soon as possible – so the airport information system needs to be used extensively. Airport authorities are usually good at providing bus or coach services in an emergency: railways tend to have reasonable contacts in the bus industry for vehicles to cover things like emergency engineering work. Pre-planning where they might come from and where they might go (through to the city, or to a nearby station unaffected by the airport station's problems) will ease the situation and assist the passengers.

The issues are similar if there is a need to evacuate the airport station or the railway. Passengers need to be warned as soon as possible: this needs good communications between airport and railway. The airport authority needs to plan for unusual numbers of people unsure of what to do. In some cases - for example where the railway is in tunnel under airport property – emergency exits may lead onto the airport. Again, there needs to be adequate communications between railway and airport so that people emerging from the exits are dealt with properly.

Closure of the railway needs to be planned for too. This is more likely to be part of normal contingency planning already, especially in the case of an Airport Express where people build their day around being able to get between airport and city in a specific time. Forecasting how long the closure is likely to last (and therefore the reaction to closure) is difficult, even with experience. Railways will need to be geared up to alerting other providers of transport – buses, taxis and the like – and liaising with them to ensure that the best use is made of the capacity available and that genuine emergency cases are properly dealt with.

Case study: Washington Metro

In Washington DC, Metro passengers can volunteer for training courses which help them help others in emergencies. This covers evacuation of the system, and helping victims of an attack before first responders arrive.

11. Employees – the positive.

Employees are your eyes and ears. They know what should be around the system and what should not. They are in contact with passengers every day. They are also in the front line – they make far more trips on your system than anyone else (which can have a psychological impact, needing a serious response from management, if there is a threat or an attack). They are the people who can most easily raise the alarm if they are suspicious about anything.

They can only do this if they know how: they will only do this if they think their warnings are taken seriously and acted on. If a gap in a boundary fence is reported and no action results, people will stop reporting gaps in fences: if trackside rubbish is just allowed to accumulate, no-one will do anything about it until someone uses it to derail a train.

If properly trained, staff can watch out for and deal with abnormal behaviour. For example heavy clothing may conceal a bomb: a clenched fist may conceal a detonator. Staff need to be trained to assess and deal with this without triggering an incident. The usual method of evaluation is to attempt to initiate non-threatening lines of conversation and to make eye contact.

Staff need to be trained in making eye contact - for example when checking tickets. This does make the system more friendly, more human; and it can help detect potential wrong-doers. It is very easy for checking tickets to be seen as a routine job: it can be more, if people are shown how and are convinced of the value of it.

People need to be trained in handing threats received by telephone – how to react, how to decide whether it is genuine or a hoax – and what to do next.

People need to be trained to look for the right things (see the acronym HOT, and also material about abnormal behaviour on page 11).

They need to be told what to expect, for example after a major incident, so that they can calm passengers down as much as possible. They will be the immediate face of the transport system: they will be in charge until the emergency services arrive and their reactions are important in maintaining order and saving life. Regular refresher courses are essential, as is a recognition that you will never be able to train for everything.

Two case studies may be instructive.

Case study – 9/11

On the morning of 11 September 2001, airspace over the United States was closed. Around 4500 aircraft in the air were instructed to land: all aircraft approaching the US were turned back or landed in neighbouring countries. This was not something which had been practiced, rehearsed or even envisaged. Indeed, in the run-up to 31 December 1999 the suggestion that all aircraft be grounded because of fears about the millennium bug was rejected – one reason being uncertainty about whether there was actually room on the ground for the world's aircraft fleet! But the unthinkable order went out on 11 September and air traffic control and airport staff coped. The training, the way of thinking, the way of dealing with emergencies which they had absorbed made it possible to do this.

Case study – 7/7

On 7 July 2005 London Underground staff had to deal with numbers of shocked, injured and panicky passengers on half a dozen trains damaged by bombs in three locations. They had not been trained in dealing with traumatic injuries, in dealing with the chaos and destruction which they found. But the unthinkable happened, and they coped. The training, the way of thinking, the way of dealing with emergencies which they had absorbed made it possible to do this.

Your staff are a valuable resource. You can add to this value by good management, good motivation and good training.

12. Employees – the negative

Your staff know the system and its defences, so if they are disaffected or leave your employment dissatisfied, they are a potential source of information to terrorists and others. So a policy of debriefing people leaving the organisation can be valuable here as well as in other areas of company policy.

Staff need to respect security policies, which they will only do if they fully understand them and the need for them - and if they are realistic. Are they seen as ineffective, unnecessary, box ticking, a lot of fuss about nothing? Or are they recognised as a part of the way an efficient transport system has to be run these days? Staff attitudes will depend on how well policies are communicated, how far they are involved, how feedback is dealt with as well as on the policies themselves (which, obviously, need to be proportional and rational).

Password policies are a particular area where it is difficult to achieve a balance. If people need to remember too many and if passwords have to be changed too often, people will write them down (and usually stick them on the computer they are supposedly protecting). But people do need to be forced to change passwords regularly, and different systems do need different protection. This is not an area which has been satisfactorily dealt with yet by the IT industry: some expectations are barely realistic, and no solutions appear to be in sight.

When staff leave, there is a need to ensure that they cannot access your computer systems – there should be a policy of immediately changing passwords and log-in codes known to that individual. The same may be true when someone is promoted within an organisation – do they still need access to the same systems as they had in their previous job?

Recruiting the wrong people can also lead to problems – are background checks made on new entrants?

Case study: a well-known European airport authority

In the aftermath of 9/11, security checks on staff revealed an unusually large number of employees with criminal records. It was then remembered that they had been deliberately recruited as part of a public service rehabilitation programme.

13. Plan, practice and learn.

A crisis response plan is necessary to set out who does what when an emergency occurs. A strong crisis response team needs to be identified, equipped and trained so that they can work effectively.

Preparation includes

- emergency response equipment (including communications equipment),
- public relations awareness (so that the organisation comes over well to the media) and
- continuity planning (so that when a key person is promoted or moves on, their role is clearly taken on by someone else).

Emergency preparedness drills are vital, to maintain awareness and to ensure effectiveness. Table-top exercises are useful: full-scale exercises involving the emergency services are much more difficult to set up but are invaluable learning tools – and excellent for raising familiarity and awareness.

Key issues include leadership and control (who is in charge at an emergency?). Effective decision-making is essential: staff and customers need to know that appropriate actions and reactions are being taken to minimise and mitigate the effects of the attack and to protect them and their future. The command centre needs to ensure that not only are decisions taken when necessary, but that communications are good – especially with the media.

Tiered security levels may be considered effective for some places, allowing an organisation to respond effectively to heightened levels of threat.

For example, at normal levels visitors could be allowed access to offices when their identity and the purpose of their visit has been verified: at a heightened level, they would only be allowed access under escort from the person they are visiting. Under the highest level of alert, they would only be allowed access if their visit was essential.

Some organisations have created a menu of responses. For example,

- At the lowest level of alert, routine measures and regular checks are necessary.
- At the next level, checks on perimeter security (to ensure that good practice is being observed by staff), checks on security systems, evacuation plans and contact lists are advisable.
- At the next level, more frequent perimeter checks, especially of priority areas, searches of high-risk areas, escorting visitors and checking access to car parks are measures which could be taken.

- At the highest level, regular patrols and searches, checks on access, and searches of baggage could be started.

Learning points need to be taken forward in a disciplined way to ensure that, if the real thing occurs, problems have been ironed out.

One lesson learnt from the fire at King's Cross underground station in London in the 1980s was the need for clear up-to-date station maps to be kept in designated accessible identifiable points for the emergency services. In the immediate aftermath of the fire, fire-fighters were struggling to reach the seat of the blaze – not realising that there was another entrance to the station, unaffected by the fire, which the ambulance service were using to evacuate the casualties.

Today, of course, these station maps can be available to first responders on the web, so that they can refresh their memories as they travel to the scene.

Another lesson from the July 2005 attacks on London was the vital need for communications. Passengers need to know what is happening to public transport services, but communications can be difficult. Mobile phone networks can be overloaded or can be giving priority to emergency services: the web can also be congested. So all means of communications – teletext, whiteboard, email – need to be brought into service. They need to be kept up to date, too, which is difficult as things change from hour to hour. Emergency phone numbers – preferably separate for passengers and for employees – can be useful, and can be manned by office staff diverted from their normal duties. External means of communications – tv and radio – also need to be kept up to date: this can be even more difficult, because broadcasters would far rather give out bad news than good.

Case study – 7/7

Late in the afternoon of 7 July 2005, a tv reporter in front of King's Cross station was asked by an interviewer about the problems people would have getting home. She was very gloomy, pessimistic and downbeat, saying that a lot of people were going to have serious problems because of the disruption caused by the four bombs which exploded that day, and she really didn't know how they would cope.

At that time – and as was being reported on the same tv channel – only three of London's main line termini were closed. True, so was the entire underground network and the bus network in the central area. But getting home was an matter of ingenuity, using the services available and where necessary by walking.

People faced problems – but not nearly as severe as was being reported.

A lesson from the 9/11 attacks was that the inconceivable, the unimaginable, can happen.

Two related possible eventualities for an airport railway are closure or evacuation of the airport. Contingency plans for these need to be discussed with airport security staff. Clearly, the railway could be very useful for emergency evacuation, but it would need a rapid response. And if the airport was closed, passengers would need to be warned as early as possible in their journey. Passengers already at the airport would make their own decisions on what to do: this could well involve large numbers of people heading for the city centre, alternative railway stations or alternative airports. See page 38 for a discussion of Evacuation and closure issues.

14. Precursor events – the warning signs.

What signs should worry you – what shows that something is likely to happen?

These can be difficult to see and difficult to interpret, but some guidelines are given.

Attackers need to know the territory. They need to see what the target looks like, they sometimes need to do a dry run to evaluate possibilities and check security arrangements. This, it is understood, applies particularly with suicide bombers: for their training they need a clear picture of where they are going to trigger their device. It can be the bomber who makes the reconnaissance visit: alternatively it can be a colleague with a camera, taking back photos to be examined at leisure.

Targets tend to be high profile. The planes used in the 9/11 attacks were owned by major flagship US airlines and aimed at iconic buildings.

They also tend to be associated with high profile events – the Madrid train bombings were timed to influence elections in the country, and the 7/7/05 attacks on London coincided with a G8 summit in the UK.

So some places and some times tend to be more likely to be the subject of an attack: this should be recognised in your security arrangements.

But these generalisations do not necessarily apply. It depends to a degree on the objective of the perpetrator. Do they want to create disruption, damage or death?

For example, those behind the bombing attacks on railways in England in the 1980s wanted to disrupt the working of the UK, but not to kill – especially not to kill civilians – to avoid too much revulsion and loss of public sympathy while generating maximum publicity. So coded warnings were phoned through – to the press, to the police, to other authorities. These had varying degrees of effectiveness: sometimes they were deliberately vague, making it difficult to respond effectively. But the bombings successfully disrupted commuting into London on numerous occasions.

Conversely, the suicide attacks in Israel seem to be aimed at killing large numbers of civilians. Therefore they tend to take place on crowded buses in crowded streets, causing maximum numbers of casualties.

Spotting someone who is on a reconnaissance trip can be difficult: they might not look out of place, and your normal customer base may be so diverse that someone may not stand out as being different anyway.

There are plenty of reasons why someone might wish to take photographs your facilities – enthusiasts, students of photography, art, planning or architecture, or people planning to build something similar.

People using mobile phones to take photographs can be very inconspicuous – much more so than the enthusiast with a camera.

See page 12 for more information about detection of abnormal behaviour.

15. Resources available

There are many further resources available to help tackle security threats – many from North America, many from the aviation industry. There is much about on-going research on the Transportation Research Board's web-site. Contact saparker@nas.edu for an updated list, or see http://gulliver.trb.org/publications/dva/CRP-SecurityResearch.pdf for a monthly report on the research. Some are books and CDs, but a number of periodicals deal with the issues. The following are mainly English language publications.

Publications

There are two major reports dealing with security related research.

One is TCRP Report 86. At the time of writing, the following volumes are available.

Volume 1 – Communication of threats: a guide

Volume 2 – K-9 units in transportation: a guide for decision makers

Volume 3 – Robotic devices: a guide for the transit environment

Volume 4 – Intrusion detection for public transportation facilities handbook

Volume 5 – Security related customer communications and training for public transportation providers

Volume 6 – Applicability of portable explosive detection devices in transit environments

Volume 7 - Public transportation emergency mobilisation and emergency operations guide

Volume 8 – Continuity of operations planning: guidelines for transportation agencies (published jointly with NCHRP)

The other is NCHRP report 525, "Surface transportation security", aimed more at highway organisations than public transport companies. Currently 8 volumes are available:

Volume 1 – Responding to threats: a field personnel manual

Volume 2 – Information sharing and analysis centers: overview and supporting software features

Volume 3 – Incorporating security into the transportation planning process

Volume 4 – A self-study course on terrorism related risk management of highway infrastructure

Volume 5 – Guidance for transportation agencies on managing sensitive information

Volume 6 – Guide for emergency transportation operations

Volume 7 – System security awareness for transportation employees

Volume 8 – Continuity of operations planning: guidelines for transportation agencies (published jointly with TCRP)

In addition, the US FEMA has published a series on risk management: these are especially aimed at defending buildings from terrorist attack. See http://www.fema.gov/fima/rmsp.shtm for details.

Other publications.

Biological attack – human pathogens biotoxins and agricultural threats. A fact-sheet from the US National Academies and the Department of Homeland Security (http://trb.org/news/blurb_detail.asp?ID=4991)

Biometrics at the frontiers: assessing the impact on society. European Commission Joint Research Centre, 3/05.

Chemical attack – warfare agents, industrial chemicals, and toxins. A fact-sheet from the US National Academies and the Department of Homeland Security (http://trb.org/news/blurb_detail.asp?ID=4991)

Draft outlook opinion of the Committee of the Regions on the safety of all modes of transport, including the issue of financing. European Union Committee of the Regions 10 October 2005.

Green paper on a European programme for critical infrastructure protection. COM (2005) 576 final. European Commission 17 November 2005.

Grey House Transportation Security Directory & Handbook. Details of American regulatory authorities and legislation, information resources, sample security plans, service providers and equipment and product information. www.greyhouse.com

Legal Research Digest 22: the Case for Searches on Public Transportation. TRB

Proceedings of the First Security Conference on anti-terrorism security in public transport. UITP 2005

Protecting public surface transportation against terrorism and serious crime: continuing research on best security practices. Brian Michael Jenkins and Larry N. Gersten, Mineta Transportation Institute, College of Business, San Jose State University, San Jose, Ca 95192-0219. http://transweb.sjsu.edu/publications/terrorism_final.htm, September 2001.

Radiological attack – dirty bombs and other devices. A fact-sheet from the US National Academies and the Department of Homeland Security (http://trb.org/news/blurb_detail.asp?ID=4991)

Report on station security. UITP 2005

Summary report on the 2002 APTA/FTA security roundtables. APTA

Survey on public transport security. UITP 2005

TCRP research results digest 59: a guide to public transportation security resources

TCRP Synthesis 21: Improving transit security

TCRP Synthesis 27: Emergency preparedness for transit terrorism

Terrorism risk insurance in OECD countries. OECD 2005

Terrorism, transit and public safety, evaluating the risks. Litman Tod, Victoria Transport Policy Institute, 2005

Trace chemical sensing of explosives. Editor Ronald L Woodfin

Transit Security Design Considerations Final Report. Volpe Center for FTA, November 2004. *Note that this is for a targeted audience, and not available for general distribution. If you think you qualify, contact Matthew Rabkin, rabkin@volpe.dot.gov.*

Transit security handbook. FTA

Transit system security program planning guide. FTA

Urban public transport and anti-terrorism security, synthesis and conclusions. Expert round table held in Brussels, 11-12 December 2004. Available from UITP

UK transport security – preliminary report. First report of the session 2005-06. House of Commons Transport Committee.

Vandalism, terrorism and security in urban public passenger transport. ECMT Round Table 123. 2003.

Some useful periodicals

AC&SS magazine (Access Control & Security Systems)

Aviation Security International

Borderpol Journal (covering international terrorism and homeland security)

Cargo Security International

CCTV Image (CCTV Users Group magazine)

TransSec e-newsletter

Some useful web-sites

http://trb.org

http://govtsecurity.com

https://a1.ecom01.com/aw_marketdatacenter Homeland security & defence – part of the Aviation Week Intelligence Network.

www.aps-expo.com

www.asi-mag.com Aviation Security International magazine

www.asisonline.org American Society for Industrial Security

www.borderpol.org

www.bsia.co.uk – British Security Industry Association

www.cargosecurityinternational.com

www.cctvusergroup.com

www.computersecuritynow.com deals with the international standard for risk management, ISO 17799

www.dhs.gov/dhspublic/display?theme=43&content=3377&print=true

www.fema.gov/fima/rmsp.shtm (see publications section above)

www.globalsecasia.com

www.intsi.org

www.llnl.gov Lawrence Livermore National Laboratory

www.nasscorp.com New Age Security Solutions

www.sandia.gov Sandia National Laboratories

www.sandia.gov/scada SCADA protection issues

www.securityworldhotel.com

www.selex-sas.com

www.siaonline.org – Security Industry Organisation (USA)

www.terminalsolutions.info

www.tkb.org

www.worldsecurityindex.com (multi-lingual global security directory)

IARO's Air/Rail conferences and workshops

Copies of the published reports of the earlier workshops are available price £250 (free to IARO members). Papers presented at more recent workshops are available on CD-ROM at the same price.

Workshops are very focused, dealing in detail with a restricted number of key issues, and complement the regular Air Rail Conferences. Workshops and conferences (with site visits) have been held as follows.

1993 - Zürich

1994 - Paris

1996 - London (Heathrow Express, Stansted Express)

1997 - Oslo (Airport Express Train)

1998 - Hong Kong (Airport Express Line)

- Frankfurt (with the AIRail station and the Cargo Sprinter)

1999 - Workshop 1: Berlin (the Schönefeld link)

- Copenhagen (the Øresund Link)

2000 - Workshop 2: Milan (Malpensa Express)

- Paris (plans for CDG Express)

- Washington (Baltimore-Washington International Airport)

2001 - Zürich airport: Air rail links - improving the partnership

- Workshop 3: Madrid (and its airport rail links)

- London Heathrow (Heathrow Express)

2002 - Workshop 4: Amsterdam, for railways serving airports but not as their main job - "Help - there's an airport on my railway".

- New York (the Airtrain projects)

2003 – Workshop 5: Barcelona. Today's design and funding issues for airport railways

Frankfurt (The AIRail project)

Workshop 6: Newark. Practical air rail intermodality

2004 – Workshop 7: Oslo. Leisure passengers – a market for airport railways.

2004 - Brussels (Thalys:Air France code-share)

2005 – Chicago (Chicago's future in an era of successful air-rail intermodality)

Shanghai study tour

Workshop 8: Edinburgh. Security on airport railways.

Planned workshops and conferences

2006 – Workshop 9: Baltimore. Security on airport railways.

- Düsseldorf: e-air-rail conference on Marketing and ticketing innovations

2007 - San Francisco or Vancouver?

Details are available from IARO, or on www.iaro.com: you can sign up for details of future events in different parts of the world on www.iaro.com/events.htm

Future plans are, of course, subject to change.