UK Defence & Security Exports

Transport Security

An introduction to UK capability

Part of

Department for Business & Trade

Contents

Ministerial Introductions

I am pleased to be able to share this brochure with you. It is vital to ensure that transport networks, whether air, rail, road or maritime are secure so that citizens can move around freely without concerns for their safety, and that economic prosperity is maintained through the continued free flow of legitimate goods. These factors matter to countries around the world, and both the public and private sectors are looking for solutions to potential threats in a security landscape that is rapidly changing.

The UK's security sector has a world-class reputation for knowledge, capability and expertise. Based on years of experience, the UK Government works closely with operators and the wider industry to design, manufacture and sell best-in-class solutions of the highest standard in quality, reliability and durability. Our businesses also offer world-leading consultancy and services to support good practice and effective planning.

Throughout the 2023 refresh of our Integrated Review of security, defence, development and foreign policy we recognise that continued investment in science and technology is essential in keeping the UK at the forefront of research, development and innovation, and this brochure is a simple but valuable tool in showcasing the many unique and innovative capabilities available from the UK that will help your efforts to keep sites safe and secure.

The UK Defence & Security Exports team, in collaboration with the UK Government's international network of staff based around the world, is committed to connecting businesses directly is our trusted UK companies. They have the products and services necessary to address the urgent issues of today, while also preparing for the challenges of tomorrow.

I would strongly recommend that our overseas customers contact the UK Defence & Security Exports team in London or your local British Embassy or Consulate. They will be able to provide you with more information on how the UK can help to support your ambitions for improved security outcomes.

Lord Johnson of Lainston CBE
Minister of State
Department for Business & Trade

Transport connects people and places, increasing prosperity and enabling a better quality of life. It is therefore vital that the transport network remains secure and resilient, and the UK has an exemplary record of improving the safety and security of the network we all rely so heavily on to travel and trade.

Robust and proportionate laws are bolstered by the use of products and services developed in the UK which help strengthen safety and security around the globe. As security threats evolve, the UK innovates to meet new challenges. We have seen this in aviation with changes to screening requirements, and over the coming months most major airports will introduce cutting-edge systems into their security checkpoints, ushering in a new era of improved security and passenger experience when going through departures. Not only will it mean greater convenience for travellers – as people will no longer need to spend time taking items out of their bags – but it will also enhance passenger safety, as security staff will have more detailed images of what people are carrying.

Our capabilities reach far beyond aviation. UK manufactured products are known for their quality, reliability and safety and are a trusted choice for both facility operators and consumers around the world. Our innovative approach means the UK also offers sophisticated solutions from Automatic Number Plate Recognition systems that can track stolen vehicles, through to the latest millimetre-wave scanning systems capable of detecting concealed weapons and contraband materials potentially carried by people passing through passenger terminals, without the need for physical searches.

I would encourage you to contact our UK Government staff who can help to connect you with the Department for Business & Trade and with our domestic companies who will gladly provide you with the support that you need to help strengthen the security of your transport hubs and networks.

Baroness Vere of Norbiton
Parliamentary Under Secretary of State
Department for Transport


Departures
Arrivals

Executive Summary

Safe and secure transport networks are key to both the safety of citizens and the free flow of goods.

For airports, security is a key element in preventing terrorism, as well as reducing smuggling and other criminal activity which can threaten the safety of passengers, aircraft and terminals. On the roads, in most countries these networks carry the majority of passenger and freight traffic, so ensuring their smooth and safe operation is key not only for citizens but also to ensure economic prosperity. For rail systems, which are increasingly busy and complex, the communications systems they rely on to control and monitor trains, signals and stations need to be protected against intrusion. The vulnerabilities in stations and across networks also need to be addressed, as they can be subject to criminal activity such as theft, vandalism and trespassers and the ever-present threat of terrorism.

UK industry can help overseas customers, both public and private, to address all of these concerns, and this brochure aims to introduce you to the broad range of solutions that are available to help secure transport networks and hubs across the fields of aviation, rail and road networks and ports, as follows:

- Perimeter Security – physical and electronic systems that protect the environs of key locations such as airports and railway stations and other transport hubs.
- Search & Screening – preventing dangerous and illicit materials from entering areas that might threaten passenger safety, as well as ensuring the smooth functioning of supply chains in order to bolster national security and economic prosperity.
- Preparedness & Situational Awareness – Gathering information and intelligence to enable detection and mitigation of threats, and ensuring that robust plans are in place to deal effectively with any incidents
- Command, Control & Communication – The tools that enable the effective coordination of operations to detect, deter and prevent criminal activity and security incidents.
- Cyber Security – Ensuring that information technology systems are secured against attacks that seek to interrupt their smooth operation or to gain unauthorised access to sensitive information.

Each capability area is matched with case studies that provide examples of the range of products and services that can be employed to protect transport hubs and networks. At the end of this brochure, you will find further information that sets out how UK Defence & Security Exports can link you to appropriate UK expertise, including resources and contact details.

A Forward Look – The Industry Perspective

The British Aviation Group is the leading representative body for British companies involved in aviation and airport development and operations, providing expertise to airports worldwide to enable them to connect to the full spectrum of British aviation expertise, delivering solutions for airports large and small.

By its very nature, aviation is the most global of industries, and only by collaborating internationally can we manage malicious risks such as terrorism and crime which target our sector.

In the UK we have long experience in managing these security risks and our businesses rightly have a reputation for developing innovative, cost-effective solutions to protect and mitigate threats, while enabling secure, sustainable growth.

We are all aware that our industry provides both a target and a threat vector for those that seek to create disruption and harm others, achieving high media impact, causing mass casualty, significant economic impact and creating public anxiety. As global economies begin to recover, so does our industry and we are once again seeing major infrastructure projects in the aviation sector take off. It is more important now than ever that we work together to identify the best solutions for this fast-moving industry which relies on efficiency and positive passenger experience to succeed.

The attack on flight PA103, just over 30 years ago, brought about a step change in aviation security in the UK with the advent of hold baggage screening, cargo security and enhanced access control measures for passengers and staff. In more recent years the terrible attack at the Manchester Arena also resulted in new thinking around the critical functions of risk assessment, corporate responsibility and managing 'grey space'. This is all learning which feeds into our experience and helps us develop and deliver effective and proportionate security to protect our passengers, staff, assets, and industry.

Aviation Security - Frequently Asked Questions

Question: *How should I assess and manage threats in the aviation security sector?*

Answer: Having a clear understanding of the threat is crucial to inform the development of a risk-based and proportionate security response. This process requires a robust and tested methodology and, conducted properly, will establish risk tolerance, and provide the basis for collaborative engagement and stakeholder buy-in. Work with security professionals who can advise on the best methodologies and develop a scenario-based approach to assessment, so that the likelihood of a threat is assessed based on intent and capability, together with the worst-case consequences. Going through this process will also involve identifying critical assets, and will provide an understanding ofcritical assets and will provide an understanding of inherent mitigations and, most importantly, the residual risks.

Understanding these residual risks is critical to the development of the mitigation strategy, for business-as-usual scenarios, or in the case of new facilities, to form the basis of design, ultimately protecting the airport and the business.

A professionally conducted threat, vulnerability and risk assessment should be part of every airport development project. It will not only provide clarity for the required mitigations – whether these are operational or design-based - but will also guide capital and operating expenditure, ensuring that the investment is targeted where it is needed most.

Question: *How can I influence major investment programmes at my airport to take account of security?*

Answer: One of the biggest challenges facing any security manager when it comes to design projects is the engagement of the security department with the project team at an early enough phase to influence the design. Given the tactical and operational demands of the role, the security manager may be one of the last to hear about this capital expenditure programme. You may

be made aware of the existence of projects only when external consultants engage with you to seek input, or a member of the project team asks for advice on some technical issue, often at a very late stage of the design. So, the first important step is for the security manager to engage with the programme manager to get early sight of planned project investments. To avoid abortive spend, security input is needed from the very earliest stage of planning, including when deciding on the location for any new build facility – planners and design teams may be unaware of the location of critical assets and other sensitive installations, security of which could be compromised by a new facility in the same area.

When security is designed into the project at the outset, it provides the opportunity for risk-based, proportionate and cost-effective security measures to be unobtrusively embedded into the design, achieving security outcomes in line with the client's risk tolerance and enhancing passenger or user experience.

Without the right corporate security culture, security managers should never assume that they will be informed of projects that design teams consider have no security input and therefore have a responsibility to keep abreast with all capital projects taking place at their site. Engaging with capital infrastructure projects and design teams should be a critical part of every security manager's role. Proactively working with programme and project teams will not only ensure the best security outcomes, but it will also optimise investment and avoid expensive retrofit which is often the result of late security engagement.

Question: *If I need security products, should I just buy from a catalogue?*

Answer: It is always best to conduct due diligence and involve security professionals when procuring equipment. For example, deployment of Hostile Vehicle Mitigation (HVM) solutions without consulting experts and conducting a Vehicle Dynamics Assessment could mean that the wrong product is deployed, and this may not perform as required in the event of an incident. It is far more secure and efficient to find this out before procuring a particular product! Consulting with security professionals will also open up opportunities to use other features, such as road layouts and landscaping design to mitigate the risks and ensure that the product procured meets expectations and will mitigate the risk.

The same applies to CCTV and video surveillance equipment where this needs to be deployed. Understanding the performance requirements and taking account of operational requirements will ensure the final deployments provide the coverage you need. It is too late after an incident to find out that the coverage or quality of the CCTV system did not match expectations. The message is, if you do not have the direct expertise needed within your team, look for consultants who can help. The UK Government promotes high standards working with bodies such as the British Aviation Group, the Register of Chartered Security Professionals, the Security Institute and the Register of Security Engineers and Specialists (RSES).

Question: *What is the future for Aviation Security and Automation?*

Answer: As the need for improved security at airports grows so does the need to find faster, more accurate systems that support and integrate with the passenger journey. Screening systems, management of data and supporting technology are all growing with pace. The appropriate use of Artificial Intelligence (AI) in this environment is becoming more and more common and UK technical suppliers are pushing technological advancements in order to support airports which often struggle to maintain staffing level at peak times. These novel solutions aim to improve the quality, speed and safety of passenger journeys and increase the security of airports. For example, machine learning that aids operations by automating accurate decision-making on the screening of passengers' bags and behaviours will also speed the throughput of check in and screening processes in the future, while not compromising security.

The UK has a strong track record in supporting and delivering aviation security expert advice, services, and products, from advice on risk management and the security principles of design, to physical and electronic security equipment, to expert analysis from our broad range of security professionals. We are highly experienced in offering proportionate, cost effective, risk-based security solutions which enhance passenger experience whilst delivering effective security outcomes.

A Forward Look – The Policing Perspective

Lucy D'Orsi CVO QPM is the Chief Constable of the British Transport Police. This UK police service is responsible for policing the rail network and several urban rail systems networks in Britain including the London Underground and the Midland Metro tram system.

As Chief Constable of British Transport Police (BTP) I have the privilege of leading a force of dedicated and highly specialised officers and staff who consistently go above and beyond to fulfil our mission as Guardians of the Railway. We are one of the world's oldest police forces and our history tells us that being courageously innovative yields significant benefits for example: BTP were also the first to Police Force to use police dogs. Our unique status in UK policing, as an arm's length body of the Department for Transport, means that we are continually testing the art of the possible. Under my leadership we will continue to be bold and embrace innovative technological solutions to ensure that we can get passengers to their destination safely and on time. I believe that a single guiding mind for security across the UK rail network, which makes use of integrated systems and is bold in its use of data would deliver security more effectively and efficiently for passengers.

Our work at BTP is centred around keeping the public and those who work on the railway safe, minimising disruption, and creating a hostile environment for crime. I am proud to lead a force which is forward-thinking, committed to taking bold measures to prevent crime and deliver the best outcomes for our passengers and industry partners – because everyone has the right to travel without fear of violence, intimidation, or harassment. We strive to be better every day and we are always looking for ways to enhance the service we deliver on the railway. A key part of my role is to build strong partnerships with industry leaders to explore the benefits of emerging technologies and to ensure that our resources are deployed effectively.

BTP already operate in a data-rich environment with over 100,000 CCTV cameras in operation across 20,000 miles of track in England, Scotland, and Wales. We know CCTV is an invaluable tool in policing, particularly as a deterrent. That is why I believe that improving our access to CCTV will enable us to respond to incidents more quickly and effectively. A good example of this is the work that train operator Northern began in 2022 to align their on-board CCTV systems with BTP. This will allow us to monitor security incidents and threats to public safety in real-time and make informed deployment decisions.

I am a firm advocate of drones - a brilliant example of new technologies that can be put to good use in policing the railways. I understand the importance of using drones beyond visible line of sight in detecting crime and minimising disruption. Drones provide essential situational awareness to officers on the ground, and they are crucial tools in monitoring incidents and containing threats until the right resources arrive. They also play a vital role in our Disruption Strategy, with our dedicated disruption teams working tirelessly to reduce the impact of disruption on the rail network. A rapidly deployed drone can quickly scan the line for trespassers, which might take officers on foot a lot longer. The evidence shows that BTP's drones have had a positive impact, contributing to faster journeys and shorter delays on the rail network. However, we must continue to work closely with industry partners to ensure that this technology is deployed consistently across the network.

CCTV and data gathered by new technologies are underused on the railway. In the future I believe it must be used proportionately to identify anomalous behaviour to inform a targeted policing response. We must be bold and 'Dare2Share' information and data across agencies, and in building new partnerships. For example, we have recently trialled some Integrated Security and Policing Pilots to make better use of non-police resourcing at 5 major railway hubs. Data can be used to identify someone who is vulnerable, potentially a pickpocket or even a predatory sex offender and we owe it to the public to make use of that.

As the technological landscape continues to evolve, I will ensure that BTP and our partners remain at the forefront of innovation in this space.

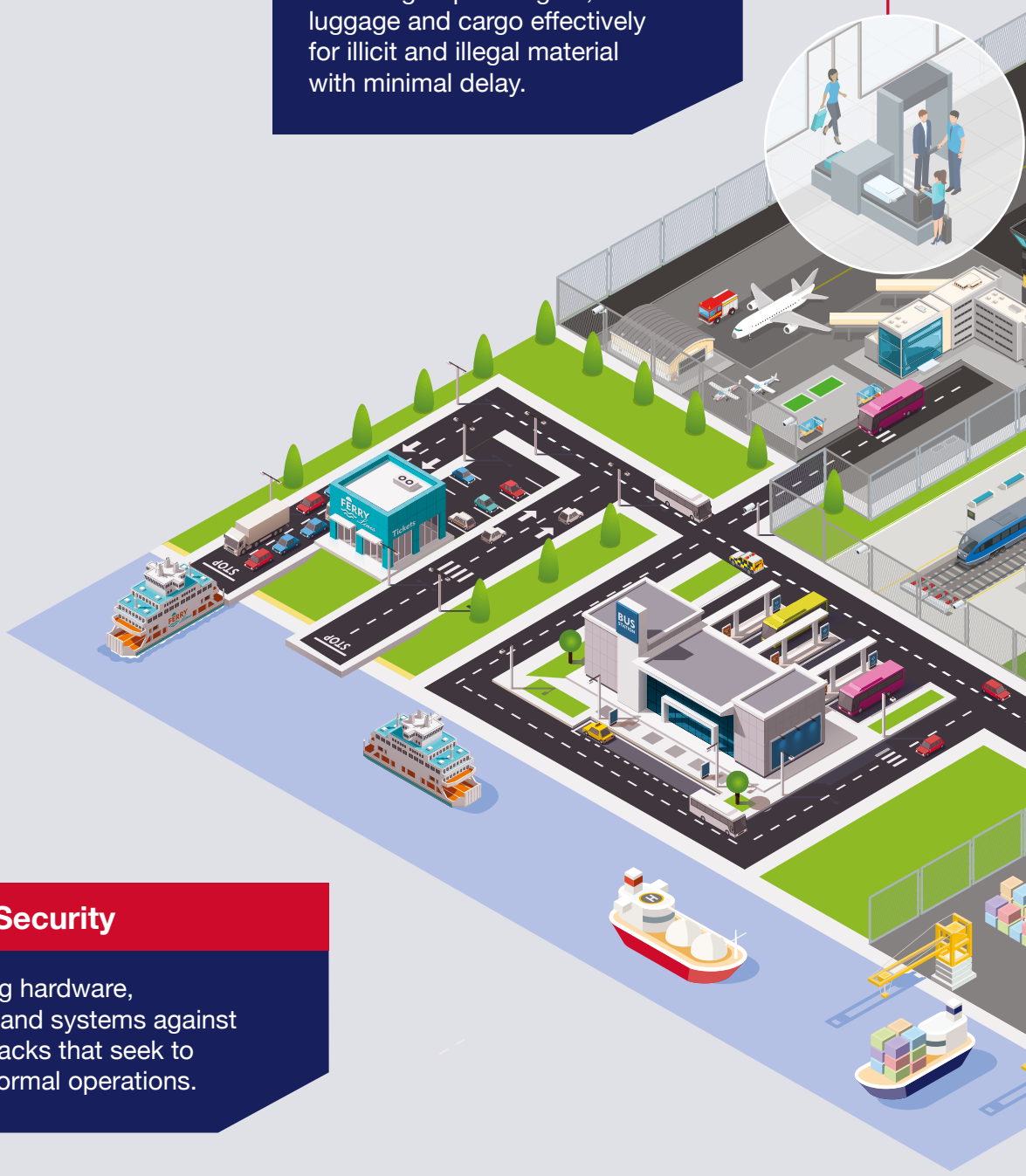
Security of the Transport Network

Search & Screening

Scanning of passengers, luggage and cargo effectively for illicit and illegal material with minimal delay.

Prep
Situ

Effec
provi
passe
and r

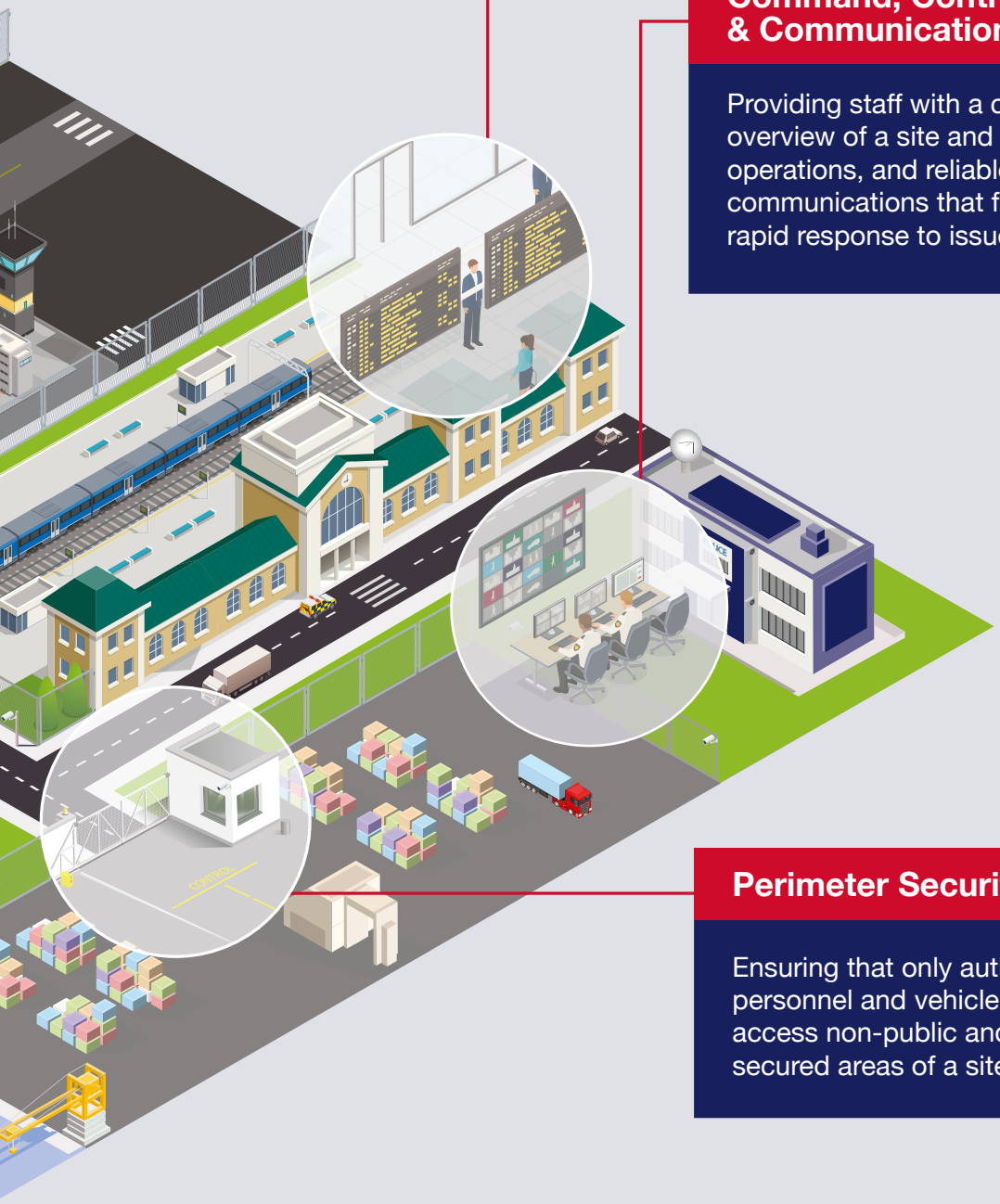


Cyber Security

Protecting hardware, software and systems against cyber-attacks that seek to disrupt normal operations.

paredness & ational Awareness

tive monitoring of traffic flows, ding essential information to engers and sharing information modelling to mitigate risk.

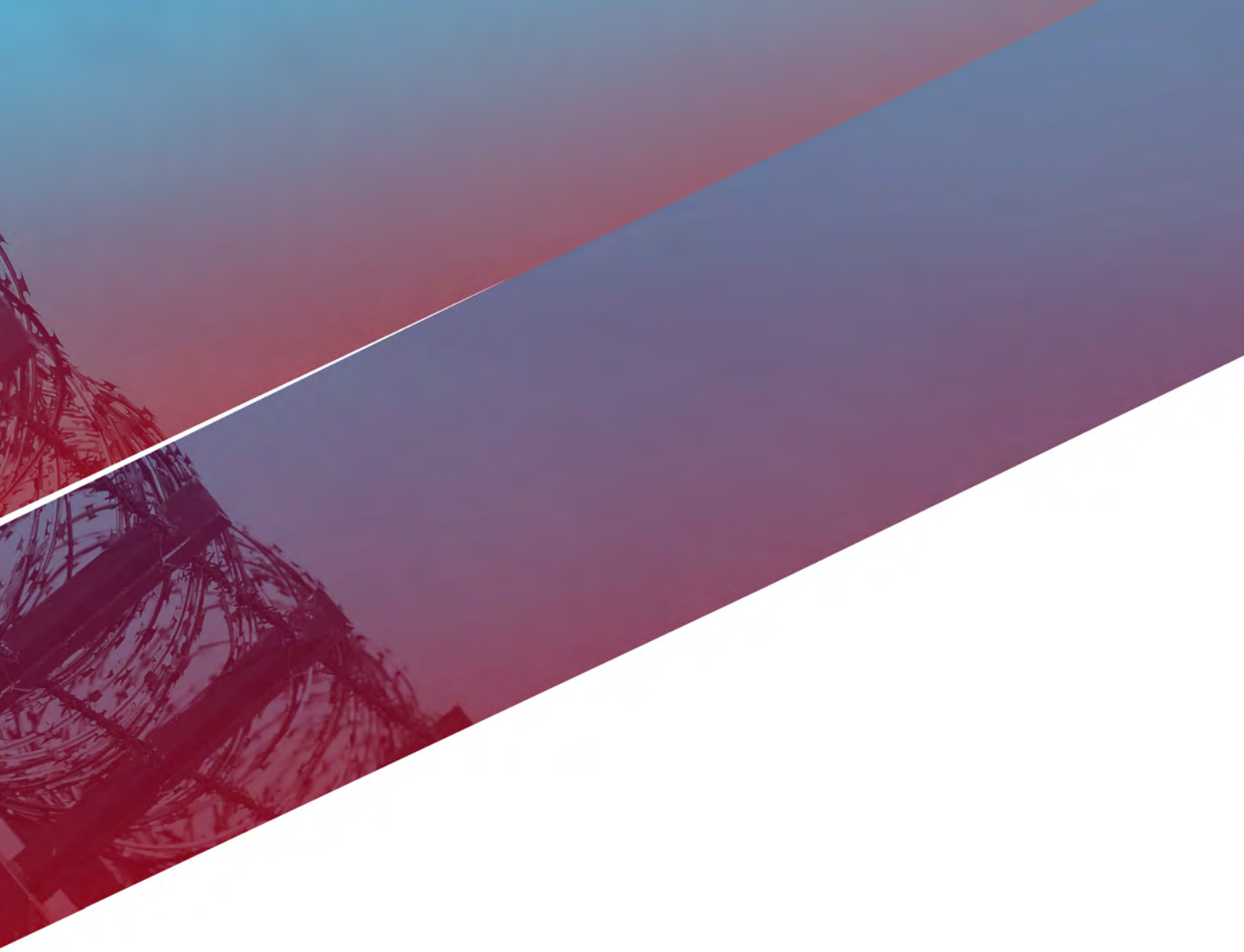


Command, Control & Communications

Providing staff with a complete overview of a site and its operations, and reliable and robust communications that facilitate a rapid response to issues.

Perimeter Security

Ensuring that only authorised personnel and vehicles can access non-public and secured areas of a site.



Perimeter Security

Perimeter Security

Transport hubs are diverse, highly active environments with people and goods constantly moving. The challenge for security professionals is balancing the need for easy access and the free movement of the public and goods while maintaining a secure environment and protecting sensitive areas from intrusion.

As well as ensuring the security of those travelling, behind the scenes, transport hubs also require sophisticated access control requirements to protect those working in a location as well as the goods being moved. To do this, a layered access system is required, protecting the different zones within a hub. It must be sophisticated enough to differentiate between visitors, contractors and staff, to prevent unauthorised access while maintaining efficient operations.

Straightforward and well-established physical security measures play a key role in protecting the transport network. Many British security products are designed to meet international standards including LPS1175. This Loss Prevention Standard was introduced to provide independent testing and certification of physical security products. Products are tested for their resistance to force-based entry using the types of tools and methods assailants might employ to gain entry. LPS1175 assumes intruders have full knowledge of a security product and their willingness to take proportionate steps to overcome that product. More importantly, the standard considers the entrepreneurial tactics criminals and terrorists are willing to invest. The threat levels and tools to define this standard reflect guidance from UK Government, the National Protective Security Authority (NPSA) and the National Counter Terrorism Security Office (NaCTSO) along with Subject Matter Experts and industry from across the security sector.

Establishing such standards as LPS1175 and testing products can offer effective deterrence as well as limiting a range of terrorist threats and criminal activity such as theft, vandalism and accidental damage. Deterrence often plays a significant role in physical security, where the co-ordinated, intelligent promotion of security leads a hostile actor to perceive or assess that their reconnaissance or attack will fail. Often CCTV alone does not provide a deterrent, but effectively combined with other measures such as fencing, access control or locks, and the combined effect communicated via a poster or audible message can often deter a hostile actor from their intention altogether. Transport hubs such as airports often cover large areas and encompass multiple sites, linking these together will often require fencing, secured gates and numerous points of access that need to be secured against unauthorised access.

The increased use of Uncrewed Aerial Vehicles (UAVs) has the potential to bring many benefits to the transport network, including rapid threat detection while flying overhead, providing aerial images and live footage. This enables security staff to assess the threat level and the appropriate response. However, the malicious use of UAV's poses a new risk to airports and other transport hubs requiring perimeter security considerations to take into account the airspace above such sites as well. Addressing these threats requires sophisticated solutions that provide accurate detection, tracking and identification as well as the deployment of effective countermeasures. As an example of the impact this technology can have, in a 2018 incident at Gatwick airport, thousands of flights were cancelled or grounded due to suspected drone use in the airport's controlled airspace., This affected the flights of 140,000 passengers and resulted in costs of approximately fifty to seventy five million pounds for the airport operator and airlines.

Innovative UK companies, regulators and airport operators have worked closely to develop commercially available solutions which are already in operation at several UK and international airports. UK industry has a track record of providing tried and tested solutions to ensure site security, and is at the leading edge of new innovation to address evolving and novel threats. Working closely with UK Government, agencies including the Connected Places Catapult have enabled collaboration between operators, agencies and industry leading to deeper sector knowledge, along with new products and services to remedy real-time challenges.

Secure Room Case Study

Storage facilities for high-value goods in transit need to be very secure in order to protect these assets from potential theft.

A UK airport engaged Securiclad to assist in the retro-fit of a secure cargo room following a review by a UK police counter-terrorism security adviser which identified that the facilities and method of storage for highly sensitive products at the airport did not achieve the necessary standards for such material.

The solution chosen used the company's security wall and ceiling panels, rated to LPS1175 SR4 standards, to provide a primary barrier which enclosed a second structure. When completed, this installation formed a safe and secure environment in which to store sensitive materials, reducing the risks associated with exposure to them.

The secure area installed by Securiclad needed to have a robust and durable finish, with the wall panels fitted to concrete slabs and the ceiling panels supported by an integrated steel framework. The company also worked with an approved door manufacturer to provide easy access to enable day to day operations in the area to be undertaken. The finished installation also needed to be hygienic as well as low maintenance. The work was carried out by personnel cleared to the appropriate security level to allow them to work unsupervised 'air side' and the appropriate certification was also provided to the airport by Securiclad and its approved installers.

Based in Monmouth, South Wales, Securiclad products enable companies and government bodies to adequately protect facilities such as data centres, utility company control rooms and nuclear sites both domestically and overseas. They work across a broad range of sectors to help organisations secure high value assets including currency, hazardous materials, pharmaceutical products, IT infrastructure and much more.

Counter-Drone Case Study

Commercial airports need to maintain the highest levels of safety and security for aircraft, passengers and the thousands of people who work or live in the vicinity of the complex. For London's Heathrow airport in particular, which is used by 89 different airlines and covers 1227 hectares with a perimeter of ten kilometres in length, accurate and constant situational awareness is an essential requirement.

Operational Solutions Ltd worked alongside a range of multi-disciplinary teams at Heathrow to design and establish a highly effective layered solution to address the threats posed by potential drone incursions. Whether intentional or accidental, drones could potentially introduce flight and operational disruption, cause damage to aircraft or endanger passengers and staff.

The company had to take into account the many challenges that an airport environment presents, including the use of radars covering all approaches to the airport while compensating for return signals from other moving objects and building reflections, as well as solving the problem of distinguishing drone radio transmissions from the vast and complex frequency environment across the airport. The complexities of providing different levels of actionable intelligence to multiple security teams across the site also had to be addressed.

These issues were solved by deploying multiple types of radio frequency sensors, radars and cameras, each with their own programming aimed at identifying as many types of drones as possible. These were all brought together under Operational Solutions' proprietary FACE™ software platform, which displays all available data in one responsive platform to allow rapid identification, tracking and response to drone threats.

Founded in 2010 Operational Solutions Ltd is dedicated to supplying and integrating innovative systems that create safer spaces globally for all. They have a wide range of solutions designed to offer comprehensive situational awareness in the face of risks both on the ground and in the air.

Secure Design Case Study

In order to remain secure, the physical elements of a layered security system need to be protected from intrusion and interference, Crime and Fire Defence Systems Ltd are currently delivering a project aimed at ensuring that the IT assets of a corporate network are protected from an insider threat. Full traceability is achieved by both physical security, including CCTV integrated with full access control at each security authorisation point of entry that incorporates visual and audio approval as well as a PIN, which are then checked at a command-and-control centre in real time. and through software, which together provide full visibility and measured checks with operational responses.

The cyber engineering approach the company has adopted uses Assured Physical Protection System (CAPPS) products which are tested and accredited, and offer protection from penetration or unauthorised plug in. All data and cabling on the site is also mechanically protected with physical access security measures locking down fittings and fixings from unauthorised access or physical attack.

Reducing insider threats and cyber-attack Crime and Fire Defence Systems Ltd offer full security engineering design for all perimeter areas and assets, plus cyber protection for organisations across Critical National Infrastructure sectors. These ensure that operational requirements are met, and risks are minimised.

Search & Screening

Search & Screening

The September 11th (9/11) attacks in the US changed the face of security screening/security at transport hubs across the globe. The threat had evolved, security regimes including search had to adapt quickly, with travellers asked to remove belts and take certain items from bags to be scanned separately, and sharp objects were no longer permitted in the cabin.

Following a later incident involving an attempted 'shoe bombing' on an international flight, passengers were asked to remove footwear so these items could be individually scanned. Following Operation Overt, which uncovered a terrorist plot to use explosive liquids disguised in drinks bottles on transatlantic flights, passengers must empty containers with more than 100ml of liquid at security checkpoints. Each new requirement increased queue times and created a longer screening process as well as increasing costs for airports and carriers. Aviation security has continued to evolve to become one of the most regulated sectors in the world.

In response, the UK Government quickly introduced restrictions while airport authorities worked with regulators, Government laboratories, subject matter experts and industry to develop innovative new screening measures. Passenger security remained a high priority and had to be balanced between the effective level of screening and the speed of processing passengers. These included the installation of walk-through metal detectors to identify weapons and other devices hidden on a person and the introduction of trace detection to identify explosives and harmful substances. To carry out more in-depth searches and to identify suspect behaviours, training regimes for security staff were also enhanced with regulators including mandatory certified training for Transport Security Officers (TSO), establishing a training framework which is periodically updated to maintain relevance with the latest threats and a group of certified trainers to deliver courses. Alongside this, TSO training was also updated to include modules to identify suspect behaviours and isolating suspect individuals in crowds, for example screening checkpoints, to minimise disruption to other passengers and contain a possible threat.

The most favoured transport routes into the UK are via air and sea, therefore the UK has overseen the development of many high-profile solutions to the challenges affecting search and detection, especially around our airports, sea ports and the domestic railway network. UK sea ports process the most international cargo, with 72.1m tonnes of freight passing through them in 2022. Annually, domestic ports handle over 65 million tonnes of containerised freight and lead the way in screening loads for illicit goods such as narcotics, firearms, explosives, radiological & nuclear devices.

Measures include the use of highly detailed X-ray scanners, designed to scan the contents of a container in just a few minutes as it passes through a piece of equipment similar to the metal detectors passengers walk through at airports. This technology has led to significant disruption to the transit of illegal goods. Sea container screening also includes sniffer dogs and some trace detection on outer container surfaces. The UK Government, via the Home Office has also developed significant cooperation between multiple agencies, including Border Force, the National Crime Agency, and European authorities, designed to identify vehicles and containers which are likely to contain illegal goods. In response to the growing worldwide trade in people smuggling, authorities also use non-intrusive measures such as carbon dioxide sampling and human presence detection systems to identify and deter this practice.

In order to minimise delays to passengers and to increase the throughput of luggage and cargo, transport operators continue to work with leading industry providers to develop enhanced screening methods that maximise throughput while maintaining the high level of screening required. For example, the UK is pioneering the use of 3D Computed Tomography (CT) and bottle scanners, providing enhanced image resolution of the contents This will significantly enhance security outcomes whilst also enabling passengers to carry their electronic items and larger liquids in their cabin baggage.

The UK leads on collaboration between the public and private sectors, directly linking industry to challenges, innovating and designing solutions. This includes innovation competitions supported through the Defence and Security Accelerator (DASA, part of the UK Ministry of Defence) aimed at SME's developing novel techniques to resolve challenges across a number of sectors including transport. In support of these innovations, the UK Government via the Department for Transport (DfT) and the Home Office, have funded the Future Aviation Security Solutions (FASS) programme, investing £25.5 million over five years to improve aviation security through science and technology innovations. The programme has been developed to improve the ability to identify and prevent terrorist attacks on aviation and have a positive impact on passenger experience.

Search and Screening Case Study

Search and detection capabilities are used to screen thousands of passengers, luggage and cargo with minimal delay and the devices to support this are being constantly improved to increase throughput.

3DX-RAY's systems combine high image quality with ease of use. Portable systems are offered to meet a wide range of inspection needs and our quality management system has been independently certified as meeting the requirements of ISO 9001:2015.

The 3DX-RAY Threat Scan®-LSC is a portable x-ray inspection system that includes two panels: the large format LS1 panel and the compact LS3 panel. The LS1 panel has a large imaging area of 600mm x 460mm to scan typical bags and packages in one scan yet is still remarkably lightweight and incredibly thin. The LS3 panel is more compact with an imaging area of 305mm x 256mm, for use where access to suspect packages is limited or under vans, for example.

This combination system is powerful and can penetrate steel up to 40mm at 120kV and up to 60mm at 150kV. It also produces high quality, sub-millimetre resolution images. The ThreatScan® range is suitable for use in suspect bag and package inspection in locations such as mass transit rail and bus stations, shopping malls, airports, stadia and sports arenas. The system is also used for general security inspection by first responders such as Police, Military and Private and Government Security agencies.

3DX-RAY Ltd is a global market and technology leader in line-scan x-ray imaging systems for security inspection, with a track record of innovation and success. Established in 1996, the company has supplied systems worldwide directly and through partners, agents and distributors.

Screening Systems Integration Case Study

RHEINBERRY

Airport security screening systems have traditionally been poorly integrated, and data has been siloed, which can allow banned objects and substances to slip through. The adoption of open architecture reduces OEM lock-in and improves efficiencies in terms of security operations and procurement.

Customers in the airport, regulatory and OEM worlds have worked with Rheinberry to start the journey towards the interoperability offered by open architecture. This is achieved via the adoption of Digital Imaging and Communications in Security (DICOS), Open Platform Software Library (OPSL) and Aviation Community Recommended Information Services (ACRIS) international standards which provide common screening result data formats, interfaces and data models, all built on solid concepts of accountability and cyber security.

Rheinberry are a unique consultancy, providing open architecture guidance and technical governance across the airport security systems domain, where they have been active since 2019. One of the company's co-founders is an author of ACI EUROPE's Open Architecture for Airport Security Systems document, which is currently changing the face of aviation security:

Rheinberry is currently working with several airports across the UK and Europe, regulators in North America and the Asia Pacific region and several OEMs and specialist third party software providers.


50

Preparedness & Situational Awareness

Preparedness & Situational Awareness

Transport networks are complex environments. To run efficiently, safely and securely, operators must understand the landscape they are trying to protect. This can be achieved by bringing together multiple sources of intelligence and modelling possible outcomes for every eventuality. This approach includes the adoption of robust security doctrines, novel surveillance technology and comprehensive multi-agency training and exercises.

In the wake of the 1995 chemical agent attack on Tokyo's transport network the emergency services were criticised for a lack of coordination between the relevant agencies, including the absence of a critical link between the transport operator and medical services. Nations across the world reviewed their own processes in response to this incident, this was the start of an increased focus on interoperability. A decade later, there was a similar terrorist attack in London on the bus and underground networks.

The UK emergency services had been carrying out inter-agency exercises and training for several decades to maximise the preservation of life at significant incidents or terrorist actions on transport networks. Soon after the attacks in London, the UK formally began the development of the Joint Emergency Service Interoperability Programme (JESIP). This framework is now used by all domestic emergency services when responding to large-scale security incident, to ensure that there is a rapid and coordinated response, leading to a reduction in casualties. JESIP has already been introduced to several international agencies keen to develop a similar structure of coordination for their emergency services.

The effective use of surveillance in busy transport hubs such as bus terminals or railway stations is essential, due to the limited scope for search and screening measures in these high-throughput environments. They rely on visual monitoring through CCTV systems and behavioural analytics to identify potential threats and to enable a coordinated response from security staff and law enforcement agencies. Comprehensive surveillance of a location also encompasses the routine security risks associated with site maintenance, construction work or other activities. Recently developed Artificial Intelligence (AI) is also used for facial recognition and to highlight suspicious behaviour, such as loitering or an individual returning to the same location repeatedly.

On the road networks, Automatic Number Plate Recognition (ANPR) systems are also used extensively in the UK. They are an effective tool, supporting the identification and tracking of vehicles suspected of being associated with unlawful activity. ANPR also provides law enforcement officials in a control room with the situational awareness to direct the appropriate response by officers on the ground.

The sharing of intelligence and information between organisations responsible for security is also a crucial factor in disrupting would-be bad actors from carrying out criminal or terror-related activities. Techniques including detection, analytics and intelligence all play a key role in security, and so should be managed under a coherent doctrine. For example, sources of intelligence and data are often diverse and so rely on the establishment of strong strategic partnerships that promote information exchange.

These inputs, including weather forecasting, CCTV feeds and criminal databases, are all vital elements of the intelligence picture for any transport hub. While some sources may have more relevance to particular sites, all inputs of data and information are an important aid in decision-making.

For operators and staff, multidisciplinary training programmes provide the skills and techniques necessary to identify and intervene in a potential threat situation. While classroom training is available from the UK, several facilities also offer fully immersive simulated exercises that place staff under the same conditions as a real incident. These have the benefit of ensuring that those responding to threats are aware of the role that they play and how they should respond effectively.

During particularly busy periods, transport hubs can be placed under immense pressure. Significant numbers of passengers can pose risks to both safety and security. In such circumstances effective digital signage and public address systems can help to improve throughput and reduce congestion on station concourses, and where the public can be rerouted towards dispersal points should an incident occur.

Training Case Study

State 21 were approached by a number of ports and asked to enhance staff training for those managing port security and enforcing by-laws. The company developed and delivered a bespoke course for each port, addressing their specific needs with teaching methods ranging from classroom input to role play and table-top exercises, allowing participants to be fully immersed in the training experience.

One port felt there was increased risk of either protest or direct action, due to a connection to fossil fuel trade (although the wider port is more focussed on renewables). They also identified that they needed to consider how to deal best with waterborne activity. State 21 were able to deliver a bespoke course to the port, augmented by the skills of the Company Ambassador, who was previously the Head of a Police Marine Unit. A major focus of the course was 'Facilitating Peaceful Protest', with a keen eye on the media. Just a few weeks after this course was delivered the port was subject to organised protest and this training enabled the port to respond to the protest in a way that allowed freedom of speech, whilst protecting both the Port operation and its reputation.

State 21 Ltd has been trading for over 8 years. Their wealth of policing expertise allows them to provide services relating to major incident/ emergency planning and exercising, along with command and control and security training.

What the customer said:

'State 21 delivered a highly topical, relevant and comprehensive course on areas that are becoming increasingly important to ports and harbours in the UK. We operate in a fast-changing world, and we need to provide our people with the proper tools to meet new challenges and risks. This course certainly provided food for thought, as well as practical and workable solutions. The high-level of engagement from my colleagues was maintained primarily down to the style of course delivery and the obvious experience both the trainers.'

Detector & Sensor Integration Case Study

Since the 1990s and in the wake of several attacks against transport hubs involving chemical and biological substances, detection and response has become a primary focus in the evolution of terrorism against transport networks worldwide.

PELA Systems' PELAmesh platform uses AI & enhanced integration with a wide range of detectors to provide real-time monitoring & alerts to CBRN (Chemical, Biological, Radiological Nuclear) and EO (Explosive Ordnance) threats. Bringing together multiple detection sources, regardless of manufacturer, PELAmesh provides operators with live monitoring, automated alerts, and pre-programmed responses when a CBRN event is detected.

This patented solution delivers unrivalled performance compared to standalone systems and non-integrated detectors. PELAmesh connects to each detector, essentially forming an encrypted network over which the data is transmitted. The operator can view the data and act on it or use the automated protocols. Alongside CBRN detectors, PELAmesh integrates with other detectors crucial to the environment. Input from weather, thermal, movement and other detectors can be integrated to provide complete situational awareness. PELAmesh products are designed and built in the UK and work hard to make seaports, airports, and transport hubs safer.

Since 2010, PELA Systems' range of products has been providing a crucial link between substance detection and mitigating the risk, and the company continues to work directly with other manufacturers to integrate their devices into PELAmesh.

Body-Worn Camera Case Study

A prominent British transport security authority required a comprehensive, efficient, and reliable solution to address a few significant issues they were facing with their existing fleet of body cameras.

The first was the need for cameras with mobile upload capabilities for prompt and real-time response. Reveal's K7 body cameras with wireless upload capabilities aptly addressed this, allowing the authority to upload evidential data swiftly for a timely resolution. The authority had previously been using a phone app for interview recordings and evidential photos. Reveal's solution elegantly merged these needs into a single device. The camera can serve as a mobile interview recorder by manoeuvring the articulated camera head for audio-only recordings and adjusting the settings to capture high-resolution photos.

The K7 camera and DEMS 360 evidence management software can also integrate with third-party solutions to compile information from body-worn video, 999 calls and drone footage as part of a larger digital evidence management ecosystem. The challenging environment of trains also necessitated enhanced audio capability, with the direction of sound playing a crucial role. To meet this need, Reveal employed dual microphones to improve audio quality.

Over 4,000 Reveal K7 body cameras were supplied for personal issue, plus around 200 Calla cameras for covert operations. Reveal's front-facing screen, a key feature recognised for its de-escalation and deterrent effects, played a substantial role in the authority's decision to choose Reveal.

Reveal Media, with 20+ years of experience in body-worn camera solutions and digital evidence management software, has a proven track record of delivering large-scale, national projects. Today, Reveal's solutions have been adopted by security organisations, police, local governments, prisons, healthcare professionals, and flagship retailers in over 40 countries.

Capacity Building Case Study

SCJS led the delivery of a Chemical, Biological, Radiological & Nuclear (CBRN) Centre of Excellence Project to provide capability and capacity in response to CBRN-related incidents to first and second line responders in Iraq, Lebanon and Jordan.

A specific requirement from Iraq emerged towards the end of the project for a trailer mounted, secure mobile laboratory solution that met Biosafety Level (BSL) standards, partly as a result of the impact of the global pandemic.

Mobile solutions such as a BSL laboratory are bespoke and developed in consultation with the client so that a completely tailored solution is achieved. Any format can be designed from the base unit providing the best solution for research, environmental sampling, forensic investigation, CBRN site analysis or command and control by way of example. Working together with GLSI, logistics were finalised and a bespoke 20-foot mobile laboratory was prepared and then delivered safely by road in May 2023 to the Disaster & Emergency Medicine Training Centre in Baghdad.

SCJS is a not for profit, global capacity building organisation and trusted delivery partner of both the UK Government and the European Union. SCJS is an approved supplier on the Conflict, Security & Stability Fund (CSSF), International Strategy & Capabilities (ISC) and ICT frameworks. Together with its sister company GLSI, a specialist equipment provider of forensic, CBRN and mobile solutions, they provide bespoke services and products to support 'rule of law' initiatives and wider security sector needs.

Automatic Number Plate Recognition Case Study

Automatic Number Plate Recognition (ANPR) technology has become increasingly important in transport security & law enforcement across the UK. ANPR systems use cameras to capture images of number plates & offer overview images to provide evidence correlation which is collated using sophisticated ANPR software. This technology is widely used across multiple security & law enforcement systems to offer real time identification of 'hot list' vehicles or provide tracking capabilities for vehicles of interest. The adaptability & flexibility of ANPR technology also provides law enforcement with further opportunities in identifying, catching & providing evidence against criminal activities.

MAV's industry leading intelligent ANPR cameras within the Rapier, IQ & IQX ranges are used globally by Governments, Military and Police Forces across the world. The development of cutting-edge ANPR cameras has provided opportunities for vehicle behavioural analysis, safety & speed data capture as well as supporting a plethora of further multi-sector uses.

The advancement of technology, like the IQ & IQX Intelligent ANPR Cameras, provides valuable support to strengthen the defences of borders, cities, highly populated areas, critical infrastructure as well as other potential targets. MAV's design of ANPR cameras balances the need for expedient results without compromising accuracy & performance.

MAV Systems is a specialist ANPR technology provider with camera deployments, in very demanding systems, operating around the world. The company employs in-house design which spans over 30 years in the development of covert and overt ANPR, selling through a network of partners & public safety integrators based throughout the UK, Europe, Americas, Middle East, Australasia, Africa & Singapore.

The market for the company's ANPR technology has been growing steadily for many years, and this trend does not seem to be dissipating due to the importance of its inclusion in multiple systems such as traffic & emissions analysis, toll crossings, Low Emission Zones,, tax, insurance & MOT vehicle validity, spot & average speed systems plus its role in combatting counterterrorism.

ANPR technology will continue to evolve as will its use across sectors, systems & countries, and MAV systems strives to offer ANPR cameras that meet the needs of today's transport security systems, whilst offering opportunities for the advancement of solutions due to in-built potential.

Interference Monitoring & Analysis Case Study

It is well-documented that Organised Crime Groups (OCGs) use illegal jamming devices to overpower Global Navigation Satellite System (GNSS) and other mobile devices in order to carry out criminal acts, which can include armed robbery, modern day slavery, disruption of public safety and vehicle theft. It is approximated that vehicle theft alone is a billion-pound industry within the UK. OCGs deliver stolen vehicles to 'chop shops', often concealing the vehicle's location by blocking tracker signals by using GNSS jamming devices. The valuable vehicle parts are then stripped and smuggled out of the country.

Forsberg Services' GILD software provides situational awareness for operators, enabling them to detect and discriminate between interference sources and providing understanding of the complex RF environment through the analytical monitoring of GNSS bands. The product focused on identifying, classifying, and locating interference by locating jamming sources from the air or ground. Collected radio frequency data is analysed and distributed to relevant parties. GILD provides critical information such as interference frequency, interference band width, signal strength and grid location of interference source.

Currently operational in the UK, its benefits include:

- Preventing disruption - locating interference sources enables the user to mitigate the effect.
- Detecting mobile and static jamming sources before they saturate the GNSS receiver.
- Acting as platform navigation system in addition to jamming sensor – no requirement for additional hardware.
- Operating on a multiple frequencies and constellations.
- Production of data reports inform key stakeholders of incidents and trends.
- Interoperability - GILD can be integrated into current in-service situational awareness platforms.
- Stores jamming data locally for post processing and analysis.

Forsberg Services Ltd was established in 1987 by Charles Forsberg, following a career in the Royal Navy working as a navigator and hydrographic surveyor.

Command, Control & Communication

Command, Control & Communication

Transport hubs are often congested, large and complex environments, with various areas of a site separated by different levels of access levels, all vital to the overall operation. A security incident taking place in a crowded transport hub can quickly escalate, involving other passengers, potentially leading to panic and delaying the response of emergency services. To address this challenge, transport facilities in the UK deploy Command, Control and Communications elements which are scalable and integrated. These central hubs of knowledge management are critical as they function to share real-time security information with both operators and users of the transport network and direct resources appropriately.

Emergency services are often co-located in UK transport hubs, with highly trained incident commanders working alongside control room operators. In the UK, law enforcement and preventative security operations on the railway network are closely coordinated with the British Transport Police (BTP). The BTP operates nationally across the entire rail network in Great Britain, policing over 10,000 miles of track and more than 3,000 stations and depots. BTP officers are trained to respond to security incidents unique to this mode of transport in addition to their routine law enforcement responsibilities.

Responding to an incident effectively also requires clear, concise communication to direct appropriate resources to the right location. Vital to this process is live, high-definition visual monitoring that enables operators to quickly ascertain the scale of response required to a security incident and its impact on those nearby. This represents a significant volume of data; thus, the provision of sufficient network bandwidth is a constant challenge for Command, Control and Communication systems. Through close collaboration with industry and service providers, control rooms in the UK utilise the latest in fibre optic networks alongside resilient communication using the latest 5G mobile technologies. This enables control rooms to operate seamlessly with high-definition video, voice and data communication. These networks are constantly reviewed as technology improves and when new sources of data are made available.

In addition, situation rooms and portable control rooms often rely on the mobile telecommunications network, and in the UK this is achieved through the latest 5G technology. The UK Government has invested over £40 million in integrating 5G and three UK universities have started research on the next generation 6G mobile network, with investments of more than £25 million in research and development in this area.

In the UK, transport hubs have layers of communication that facilitate secure connections to user groups based on their role. For example, communications networks will be configured so that security, law enforcement and janitorial teams are on separate channels. These are then handled via control rooms where highly trained personnel action and route communications. Dedicated procedures based on tried and tested principles have been developed over many years to provide decision makers with the skills to effectively review live information sources and direct the appropriate level of resources to tackle an incident. For example, in 2005 London was targeted by four suicide bombers across multiple public transport routes in the city, injuring more than 700 people.

The resulting multi-agency response has since been acknowledged to have saved lives in challenging circumstances. Part of its success can be attributed to the coherent message communicated to media outlets, limiting panic and disruption to other transport networks. This coordinated response and cohesive communication was the outcome of multi-agency training simulations and a clear command structure, established through cooperation between the emergency services and government agencies. This led to the creation of JESIP, the Joint Emergency Service Interoperability Programme, which today governs the way in which UK agencies cooperate in response to major incidents.

Communicating with passengers is vital to the overall safety of all transport hubs. Timely and appropriate information delivered using remotely controlled information boards, public address systems and directional signs all aid in the safe flow of passengers in congested spaces, keeping them moving and guiding them away from danger. These systems need to be hardened against intrusion to ensure that the correct information is delivered without interference external sources who might benefit from the confusion that would be caused by misinformation. To protect against this, UK transport operators and agencies follow guidance from the National Cyber Security Centre (NCSC) on emerging threats to cyber security and communication.

In London, Transport for London (TfL) uses a state-of-the-art control room to oversee the capital's complex and congested road network. The Network Management Control Centre (NMCC) manages the 360 miles of road, where it manages traffic flow including securing the movement of Government ministers, international dignitaries, and royalty. Working closely with law enforcement, the NMCC also maintains a comprehensive network of cameras enabling operators to direct resources to ongoing security incidents, and to identify where an incident might be developing. This provides much-needed information to manage and route traffic away from potential danger along with monitoring situations as they develop.

Communications Case Study

TETRA is the current established means of critical communication employed across the globe. It has been a trusted service due to its resilience, reliability, and efficiency, allowing for voice, group calls, and direct device-to-device calls. However, the system is lacking in many areas, especially regarding data sharing. On the other hand, 4G wireless standards allow large amounts of data to be shared, whilst still encompassing the capability to communicate via voice. It can also be used to communicate in-between services, allowing fire brigades, police officers, and medical teams to all connect together.

The Handsfree R5 Fixed Vehicle Device by Handsfree Group is a complete mission critical communication solution that utilises LTE to provide voice, push-to-talk (PTT), high-speed data, and integrated video. Handsfree Group is one of two approved suppliers to deliver fixed vehicle technology and accessories for the deployment of the ESN (Emergency Services Network) contract, which will eventually fully replace the current existing TETRA Airwave System. The device comprises of a control unit, user interface, and associated accessories (such as telephone handset, speakers, and antenna). The R5 is an Android™ 10 platform with Google applications installed, providing an easy-to-use interface that regular Android users will find to be familiar. It is an all-in-one, reliable device that offers interoperability between users; with superior sound quality to ensure your vital communications are crystal clear. This technology is suitable for police cars and motorcycles, fire engines, ambulances, and marine vessels, along with coast guard, mountain rescue and other mission critical users.

Over the last 15 years, Handsfree Group have supplied and installed the latest market-leading vehicle technology innovations through their UK and USA operations. Their commitment to rigorous Research and Development has led to the device being developed from initial concept to full certification in the space of two years. It is the first Fixed Vehicle Device of its kind to receive GMS (Google Mobile Services) certification and has received accommodations for its interoperability and application in public safety from the ICCA. Every single feature and benefit have been tested and approved by users in the field, with feedback from users being considered every step of the way.

Integration Case Study

Command, Control and Communication solutions are vital to safety and effective operation of an event. Alongside incident response it can also be used for planned events, integrating resources, contingency plans and workflows. During an event a suitable platform ensures that resources with the right skills, equipment, incident knowledge and experience are safely and quickly despatched to any incidents that occur within the event location whilst still managing the day-to-day response across the wider environment providing commanders with a single, common operating picture.

For over 30 years Capita have been supplying integrated Command, Control and Communication solutions to public safety agencies to support both day-to-day operations and major, planned events on a global stage.

As one example, the company's ControlWorks integrated command, control and communications solution facilitates better outcomes for the public by automatically providing detailed caller knowledge and history, ensuring that the most appropriate resource arrives as quickly as possible, and enables collaboration and interoperability through shared technology and services on a truly geographically independent, flexible and mobile platform. This solution is used by major organisations worldwide including, in the UK, the British Transport Police, the Police Service of Northern Ireland and the Highways England roads agency.

Their solutions combine secure communications, detailed mapping and intelligent searches of connected data sources with live tracking of assets, CCTV feeds, sensor-driven alarms from IoT devices and the ability to live-stream video from mobile devices to ensure full situational awareness within the control room. With a fully integrated mobile capability, responding resources can be kept fully informed as incidents unfold and can provide updates from scene as appropriate.

Cyber Security

Cyber Security

Whether used to deny service, damage equipment, steal intellectual property, impose ransomware demands or steal customer data, cyber-attacks perpetrated by hostile nation states or criminal networks are becoming increasingly frequent and more sophisticated. Therefore, over and above physically protecting equipment and systems a layered defence affords better protection and planning for the prevention and mitigation of cyber threats forms a key part of any organisation's security plan.

Recognising the fact that the threat landscape is constantly evolving, the UK Government supports operators and the public through advice, guidance and tools provided by the National Cyber Security Centre (NCSC) plus legislation contained in the Network & Information Systems Regulations (NIS). The many UK companies who provide solutions to help our domestic operators comply with these robust rules can also support operators overseas who wish to employ similar exacting standards.

As a leader in global cyber security the UK offers comprehensive solutions that can help operators to understand and mitigate a wide range of threats. These include staff training and awareness to prevent data breaches and malicious entry to essential systems, through to endpoint protection software so that computers, smartphones and IoT devices are more difficult to compromise. Next-generation firewalls to defend against attacks and systems that can alert operators to attempted breaches or unusual activity being detected on internal IT systems are also available. Services that our providers offer include vulnerability assessments and penetration testing, as well as fully managed service packages that cover all aspects of an organisation's cyber security needs.

NCSC Assured Services harness the very best of the UK's cyber security industry. As the National Technical Authority for Cyber Security, the NCSC uses its expertise to define standards for cyber security services, and its brand to differentiate the services offered by industry that meet these standards.

Through its schemes, the NCSC is creating a trusted marketplace for all sectors of the economy, particularly those of specific relevance to securing the UK Critical National Infrastructure include CHECK penetration testing, Cyber Incident Response and Cyber Risk Management & Security Architecture consultancy. As of 2023, 77 UK companies can offer these NCSC assured services.

These products and services, along with information on certified companies, can be found on the NCSC website at: https://www.ncsc.gov.uk/section/products-services/introduction

The UK Academic Perspective: Academic Centres of Excellence in Cyber Security Research (ACEs CSR) have been part of the UK Government's National Cyber Security Strategies since 2011, and continue to play a key role in helping Government make the UK more secure and resilient in cyberspace.

The ACEs CSR are based at UK universities which have been recognised as having an established critical mass and pedigree of good quality cyber security research. The initiative is led by the National Cyber Security Centre (NCSC), which is a part of GCHQ and is the UK's Technical Authority for cyber security, and the Engineering and Physical Sciences Research Council (EPSRC), which is a part of UK Research and Innovation (UKRI). The community of ACEs CSR has now grown to 19 universities which meet, hold conferences, collaborate, challenge and support one another. In partnership with public and private sector organisations our aim is to build and maintain a flourishing community of commissioners, producers and consumers of internationally-leading research where everyone works together for the common good.

By recognising these ACEs CSR the UK Government's aim is to:

- Enhance the quality and scale of academic cyber security research and postgraduate training undertaken in the UK.
- Make it easier for potential users of research to identify the best cyber security research and postgraduate training that the UK has to offer.
- Develop a shared vision and objectives among all those involved in cyber security research in the UK.
- Showcase UK academia's internationally leading research expertise.
- Further details on this area can be found online at: https://www.ncsc.gov.uk/section/education-skills/research-and-academia

Threat Detection Case Study

A company's Cyber Operations unit required a number of security use cases to be designed and expanded to meet additional detection control requirements.

The Cyber Operations Unit was made up of multiple teams each with designated Stakeholders and specific security use case requirements.

Somerford Associates utilised the Splunk Enterprise Security (ES) technology of the Splunk Security Stack solution, which was already present within the customer's environment, enabling them to leverage the search and discovery, machine learning, reporting & analytical features of the Splunk solution. This provides multiple frameworks to search for, detect and respond to security threats, including correlated and machine learning based detective controls as well as auditing, reporting and triage features for Incident Management.

Since the number of use cases was significant, the implementation was conducted by multiple of Somerford's fully trained Splunk engineers with a very high level of security expertise. The company's project manager controlled the project lifecycle, managing the customers' multiple stakeholders. Utilising a qualified project manager kept costs under control and on track throughout.

Somerford Associates was founded in 2001 by Andy Davies as a privately owned SME and is based in Gloucestershire UK. The Company has doubled growth year on year with 2022 revenue of over £20 Million ($23M) with 64 employees. Somerford trades in UK Pounds, US Dollars and EU Euro in Commercial and Government/Public Sector markets. The company offers end-to-end services as a licence reseller, including expert-level support from pre-sales to post-implementation, ensuring that projects are managed seamlessly.

With specialist knowledge, skills and experience derived from supporting a broad range of FTSE 100, central government, defence and intelligence companies Somerford Associates have a strong reputation for enabling digital transformation at scale, at pace and on budget. Somerford strives to always improve and continue to deliver success in line with our operating procedures and principles.

Vehicle Protection Case Study

Over recent years, automotive cyber security has gained prominence due to vehicles becoming more connected, increasing their attack surface. This has not gone unnoticed by the hacker community, and it can result in costly vehicle recalls or loss of vehicle consequences for owners.

A European OEM (vehicle manufacturer) wanted to ascertain the security posture of the connectivity within a new SUV in their range. The opportunity to engage NCC Group in addressing the issue allowed the company to inform its development teams with a technical risk analysis. Hence, they would be able to remedy any vulnerabilities that could be taken advantage of by any would-be hacker.

NCC Group provided three key areas of support for the company;

- A Web Application Test: Typically used by customers to register their vehicle for connected services. NCC Group investigated high risk areas in their web app security, such as authentication bypass, account traversal, privilege escalation, and data extraction.
- Infrastructure Assessment: Analysing the Mobile Backend so information on identification and software type or version was researched and collated. Where appropriate, attempts were made to exploit the systems.

- Mobile Application Assessment: This identified security vulnerabilities that could compromise user data on the device or be accessed via a remote server using a web service or other network interface.

As a result of NCC Group's work the company received a comprehensive technical report highlighting individual risks with a rating associated with each vulnerability and the real-world impact of exploitation. The report also contained an executive summary, which detailed business impact and technical remediation actions to enable them to improve the cyber posture of the connected vehicle.

UK headquartered cyber security specialists, NCC Group, works with 60% of the automotive companies globally, delivering technical and risk-based security assessments. Its methodologies cover all of the ISO21434 risks as well as web application security risks. They have a dedicated global automotive team led by industry specialists and backed up by the largest cyber security assurance team in the world, and have in-house dedicated hardware security labs, test tracks and specialised testing environments.

Network Protection Case Study

Northern Rail, previously Arriva Rail North, operate across the UK and recently procured digital fleets with franchises Alstom, and Construcciones y Auxiliar de Ferrocarriles (CAF). In 2018, following new cyber security regulations, Northern approached RazorSecure to secure the systems of 300 trainsets across 2 fleets.

As Northern Rail realised that they would be accepting not only the operation of the new train fleet, but also the risk attached to the connected systems onboard these trains, they saw a challenge that would need to be addressed. In addition, the new NIS Regulations set out strict compliance obligations for Operators of Essential Services to ensure they take appropriate and proportionate measures to manage the risks posed to the security of network and information systems. As their existing stock and the additional 101 new CAF trainsets were being upgraded to Icomera systems, a vulnerability analysis highlighted the need to install an Intrusion Detection System (IDS) on the Icomera Mobile Communications Gateway (MCG).

Following an extensive vendor selection, RazorSecure was chosen and partnered with Icomera to deliver the project. After the initial integration process, RazorSecure Delta was installed on the Icomera X6 MCG with reporting capability fully integrated into the Icomera support function. The RazorSecure service provides alerts, reports, and access to the dashboard for both Icomera and Northern. It is installed across 300 trains, monitoring and protecting passenger journeys and has integrated reporting capability, providing alerts, reports and secure remote access to a threat dashboard. Systems also protect the trains' control & monitoring systems (TCMS) onboard.

RazorSecure was founded in 2015 and offers products and services to enhance railway cyber security, by protecting and monitoring networks and key systems. We deliver this through our flexible approach to cyber security, designed specifically for rolling stock, signalling and infrastructure systems. Their focus is to provide the best protection against cyber-attacks and ever-evolving cyber risks, by staying ahead of a rapidly evolving threat landscape with new innovations. Their solutions are installed on over 3200 vehicles globally, making RazorSecure the leader in rolling stock cyber security.

About Us

As part of the Department for Business & Trade, UK Defence & Security Exports' role is to help the UK's defence and security companies to export, and to provide the specialist advice and practical help that overseas buyers need.

We do this by building close relationships with industry and with overseas governments as well as working closely with our own Government departments including the Home Office, the Ministry of Defence and the Department for Transport.

In addition to the military, security, fire and resilience specialists in the Department we work through a network of over 3,000 trade staff based in our Embassies and Consulates around the world. We also support the major trade shows for the defence, security and cyber security sectors that take place in the UK and overseas.

Next Steps

This brochure, which focuses on UK industry's expertise in providing security for transport networks, represents the combined expertise of companies from across the sector. It contains case studies that give a snapshot of the world-class solutions the UK can offer, but the list is not exhaustive.

If you are interested in any of the capabilities presented here, our security industry stands ready to help. The depth of knowledge and expertise that companies in the UK provide can help you to keep your next major event safe and secure from threats.

For further information, please contact the UK Defence & Security Exports staff in your local British Embassy or the team in London. We are ready to help.

UK Defence &
Security Exports

London address:

Old Admiralty Building
Admiralty Place
London
SW1A 2DY

www.gov.uk/government/organisations/uk-defence-and-security-exports

securityexports@businessandtrade.gov.uk

About Our Contributors

The British Aviation Group is the leading representative body for British companies involved in aviation and airport development and operations, providing expertise to airports worldwide to enable them to connect to the full spectrum of British aviation expertise, delivering solutions for airports large and small.

As an organisation they aim to help members sell their products and services in the UK and overseas, and internationally offer a solution for governments and organisations looking to source UK expertise for airport development projects Member companies can be searched by capability and/or market to find a supplier. BAG is a representative body that operates under the ADS Group Ltd umbrella and is open to both ADS Members and non-ADS members.

Lucy D'Orsi CVO QPM is the Chief Constable of the British Transport Police, which is responsible for policing railways and several urban rail networks in Britain including the London Underground and the Midland Metro tram system.

In her previous role, Lucy was the Deputy Assistant Commissioner for Specialist Operations in London's Metropolitan Police Service, and she continues to serve as National Police lead for Taser and Counter Drone UK capabilities.

The Department for Business & Trade would also like to thank PELA Systems Ltd, the UK Security & Resilience Industry Suppliers Community (RISC) and its constituent trade associations, including ADS and the British Security Industry Association, for their support in the production of this brochure.

This document is also available on our website at
www.gov.uk/government/organisations/uk-defence-and-security-exports

UK Defence &
Security Exports

Part of

Department for
Business & Trade