eurotransport

SECURITY SUPPLEMENT

Photo Source: TfL
Photographer: Ian Bell

SECUR-ED: providing a set of tools to improve urban transport security

Jan Steinkohl and Yves Perreal, SECUR-ED Project Coordinators

CCTV in public transport: no longer a nice to have!

Dave Gorshkov CEng FIET, Chair, APTA Technical Standards Working Group CCTV & VCA Standards and *Eurotransport* Editorial Board Member

SMRT's security and emergency planning philosophy and initiatives

Maurice Tan and Vaswani Anand Lachman, Security & Emergency Planning, SMRT Trains Ltd

Jan Steinkohl and Yves Perreal
SECUR-ED Project Coordinators

SECUR-ED: providing a set of tools to improve urban transport security

Despite high profile attacks on public transport systems in 2003 in Madrid and in 2005 in London, public transport is a very secure means of transport. However, public transport operators in Europe strive to increase the security of their systems even further, living up to their responsibility of protecting passengers, staff and assets as well as the reputation of their network from security threats.

Potential security threats arise from low-probability but high impact criminal acts like terrorism, as well as from everyday operational security problems such as disorder, vandalism, graffiti or assaults on passengers and staff. Public transport systems are particularly vulnerable to such threats, not only because they transport an enormous amount of passengers, but more importantly because in order to provide efficient transport services to such a large amount of customers, public transport systems must be open, uncontrolled systems. Being in possession of a ticket is enough to access the network and travel anonymously without prior reservation or security screening during the time of booking, or at stations and stops. This characteristic in public transport in Europe must be maintained. Given the complexity of critical infrastructure in public transport systems, this requirement poses a real challenge to public transport operators.

SECUR-ED
SECured URban transportation - European Demonstration

The SECUR-ED project

SECUR-ED is a €40 million research project financed by the EU's FP7 programme and brings together 40 partners from public transport operators, industry and research institutions to try and find solutions to this challenge. The project, led by Thales, aims at improving mass transportation security in Europe through the development of packaged modular solutions that can be used in large and medium-size cities in Europe. Based on best practices, SECUR-ED will integrate a consistent, interoperable mix of technologies and processes that cover a wide variety of aspects – from risk assessment to complete training packages, while also considering societal and legal concerns related to some solutions, such as CCTV and video analytics. The solutions presented by SECUR-ED will reflect the diverse environment of mass transportation. The project ensures that these solutions will not only exist on paper by integrating them in existing public transport networks where they will be put to test and validated in so-called demonstrations. In order to ensure the transferability of our solutions, they will be tested in both large and small public transport networks.

Taking a wider approach

When thinking of security enhancing solutions, most people think of technologies such as CCTV cameras or metal detectors. However, SECUR-ED takes a wider approach, also considering the contribution that a culture of security can make to a public transport operator, and other pillars of a sound security regime. These include, for instance, manpower that is available for carrying out security activities, such as security staff, security service providers, and forces that may be called in to assist such as police and firemen, but also front line staff that could be involved in security-related incidents like cleaning staff, for instance. All of these can be trained and educated to be able to increase the security of a public transport system and to be able to detect and handle security risks. Procedures are also important for increasing security. Standard operating procedures and methods, such as searching of facilities and rolling stock or checking procedures for passengers, are as important as emergency operating procedures to be prepared in the case of a crisis. Of course, a good security regime also includes technological solutions, such as communications and security systems that include public information systems, threat detection systems and command, control systems, and appropriate vehicles for mobile teams. A security system can also include design criteria that are applied to infrastructure and rolling stock in order to prepare them for access control or crowd management. SECUR-ED analyses effective security regimes and recommends certain safeguards to public operators in order to increase security. SECUR-ED also develops training modules for the staff of public transport operators to put the procedures in place.

Addressing new developments

Of course, SECUR-ED also analyses technological solutions, assessing existing technology that can be integrated into security systems rather than at the development of new, untested technologies. If a gap exists in the proposed solutions, SECUR-ED will make sure that any new development can be addressed by the adaptation of off-the-shelf, available technology that can be integrated in public transport networks. When suggesting possible technological solutions, SECUR-ED will make sure that best practices from the railway and the bus markets are taken into account and that state-of-the-art technologies coming from other related industries such as telecom, IT, security and others are considered. These solutions are carefully analysed to evaluate their suitability for application in public transportation. This broad approach should help overcome the fact that today many technologies are deployed in silos.

Analysing a wide range of technologies

SECUR-ED analyses a very wide range of technologies, such as CCTV and video analytics, chemical, biological, radiological, nuclear, and explosives sensors, cyber security technology and telecommunications that are installed for security purposes. The work of the project also includes dual use systems, i.e. systems that do not only serve security purposes but also additional purposes such as communication, safety systems, such as traffic management systems and video systems that serve operational and safety needs, fire detection systems, building management systems, access control, ticketing, and HVAG and SCADA, as well as passenger service systems. In addition to the complexity of integrating them technologically, they require extra attention because in organisational terms they are generally not under the control of the security division of public transport operators.

However, each mass transportation system has a unique set of risks and vulnerabilities and it is therefore impossible to create 'one-size-fits-all' solutions. Yet, when analysing solutions, it is important to identify communalities in the needs and the technologies and suggest a series of solutions to provide a selection of proven solutions to public transport operators. However, this is not an easy task because highly complex systems exist, each with their own technological needs, with countless legacy systems, most of them basically analogue with some digital supplements. Additionally, different cultures, disciplines, operational models, business structures, and perceived threats exist among different public transport operators. In this environment, SECUR-ED aims to ensure interoperability between systems. This should be done through a service oriented architecture and a system-of-systems approach and the development of standard interfaces. The aforementioned solutions, such as training, procedures, as well as hardware and software, are selected and packaged with interoperable interfaces, hopefully ready to be integrated in different public transport networks.

The SECUR-ED demonstration test in Berlin will show the importance of staff training to be ready to react and manage any kind of security incident

Copyright: Paolo Margari/paolomargari.it

Large-scale demonstrations

In order to ensure that the principal capacities developed in SECUR-ED will work in real life, tests in large-scale demonstrations in Madrid, Paris, Milan, and Berlin will take place.

Madrid

The test in Madrid will show how to manage different kinds of transportation systems, such as metro and bus, with a unique security and incident management system controlled by the Madrid transport authority, CRTM. Ground and on-board cameras will support each security operation in conjunction with a complex integrated control system. The security operator from the control centre will be able to have a complete overview of transportation systems, receive alarms and manage all tasks to support and solve the emergency: all buses and metros will be monitored on a map, alert messages from staff will be visualised and processed.

SECUR-ED demonstration tests will take place in Paris among RATP and authorities to underline the importance of coordination and fast reaction

Copyright: RATP/Denis Sutton

SECUR-ED PARTNERS

- Alstom: www.alstom.com
- Ansaldo STS: www.ansaldo-sts.com
- ATM: www.atm-mi.it
- Axis Communications: www.axis.com
- Bombardier: www.bombardier.com
- CEA: www.cea.fr
- CRTM: www.ctm-madrid.es
- DB: www.bahn.com
- EDISOFT: www.edisoft.pt
- EMEF: www.emef.pt
- EMT Madrid: www.emtmadrid.es
- EOS: www.eos-eu.com
- FNM: www.ferrovienord.it
- FOI: www.foi.se
- Fraunhofer: www.fraunhofer.de
- Gteam Security: www.gteamsecurity.com
- Hamburg-Consult: www.hamburg-consult.de
- ICCA: www.iccaweb.com
- Ineco: www.ineco.es
- INOV: www.inov.pt
- JRC: www.ec.europa.eu/dgs/jrc
- MIVB/STIB: www.stib.be
- MTRS: www.mtrs3.com
- NICE: www.nice.com
- RATB: www.ratb.ro
- RATP: www.ratp.fr
- Morpho: www.morpho.com
- SELEX Elsag: www.selexelsag.com
- SNCF: www.sncf.com
- University of Würburg: www.uni-wuerzburg.de
- Ministère de L'Intérieur: www.interieur.gouv.fr
- TCDD: www.tcdd.gov.tr
- Technical University of Dresden: www.tu-dresden.de
- Thales: www.thalesgroup.com
- TNO: www.tno-managementconsultants.nl
- UITP: www.uitp.org
- UNIFE: www.unife.org
- University of Paderborn: www.uni-paderborn.de
- University of Stavanger: www.uis.no
- VTT: www.vtt.fi

Paris

The test in Paris will show new technologies, from chemical, biological, radioactive, nuclear and explosive detectors, to new algorithms for video analysis. In this demo a strong cooperation is foreseen among the operator, RATP, and authorities to underline the importance of coordination and fast reaction. The challenge is to control a crowded open area, without interfering with passenger flow.

Milan

The test in Milan will show how it is possible to trace a suspect person during his transit through the public transport system and using services of different operators. It will start with an alert to the police with the aim to prevent an attack. On a video wall, all cameras will show dynamically the areas where the suspect is detected. Here also the train depot and yard is considered vulnerable, therefore a security system to prevent intrusions and damages to trains and facilities will be tested.

Berlin

The test in Berlin will show the importance of staff training to be ready to react and manage any kind of security incident. The training will be done using advanced simulation tools.

In order to make sure that the results are transferable to other cities, the solutions will also be put to test in smaller networks.

There is a lot of challenging work involved with the SECUR-ED project. For further information please visit the project website at www.secur-ed.eu. A SECUR-ED presentation will also be given at this year's InnoTrans on Stand 120 in Hall 4 on 18 September from 12h30 to 13h45.

BIOGRAPHY

Jan Steinkohl is Public Affairs Manager at UNIFE. As part of his responsibilities he works on the two FP7 projects SECUR-ED and PROTECTRAIL. Prior to joining UNIFE he gained experience in the Directorate General for Transport and Mobility of the European Commission.

BIOGRAPHY

Dr Yves Perreal has a PhD in Applied Mathematics from Ecole Centrale in Lyon. He joined Thales in 1990, and after 10 years in the Thales Central Research Laboratory, he moved to the Aeronautical Division in 2000 to work as Programme Manager of big avionics systems, then as Programme Department Director. In 2005, Yves became CSO of European Satellite Navigation Industries, the company responsible of the Galileo IOV phase. In 2008, Yves became Director of ThereSIS, a Thales Innovation Centre, and in summer 2009 moved to the Transport and Security entity to take the lead of the SECUR-ED project.

Dave Gorshkov CEng FIET
Chair, APTA Technical Standards Working Group
CCTV & VCA Standards and *Eurotransport*
Editorial Board Member

CCTV in public transport: no longer a nice to have!

As we move past the London Olympics and reflect on the various measures taken to provide 'security' to the transport network, what have we learned and how do these lessons measure up with existing 'legacy' systems and technology changes that will affect future surveillance systems?

Over the past 20 years, various solutions for CCTV have emerged that have been predominantly based around analogue camera or CCD (Charge-Coupled Device) sensor technologies. The CCD has been a reliable stalwart of the security industry and remains the most widespread solution currently in use to meet the surveillance needs of the transport industry. But times are changing!

CMOS (Complementary Metal-Oxide-Semiconductor) based solutions first started appearing in mainstream CCTV solutions about 17 years ago, although these were not as robust, very expensive and relatively complex to use compared to their modern day cousins. Things have moved on significantly and depending on who's reports you read (even we have one available from Digital Grape!) the migration to IP CMOS based camera technology is well underway and soon – within the next 2-4 years, maybe sooner, we will see more IP CMOS cameras being purchased than Analogue CCD devices. Consequently, migrating existing legacy surveillance systems to IP is providing a major opportunity to introduce new features and capabilities to existing security and surveillance systems.

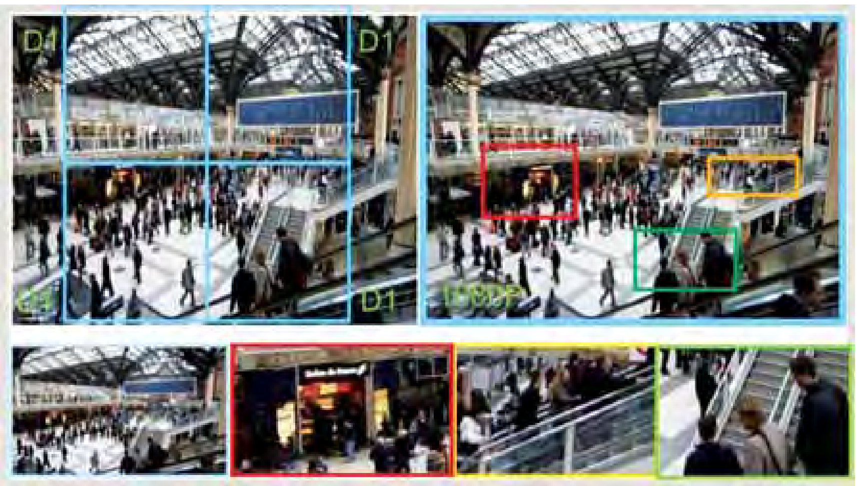


Figure 1: Boxes on the above image shows difference in 4 x D1 images vs. 1 x 1080P HD image and how 'areas' of the image can be zoomed in on from any terminal

But why all the excitement now rather than a few years ago when 'Hybrid' CCD based solutions were all the rage? Well, costs, complexity and sensitivity are the major answers in reality.

Until recently we have not really had the technical performance vs. cost benefit from CMOS based sensors and systems to justify the move CCTV designers to specify these solutions. That has very much changed now with improved quality of performance in low light conditions and the ability for IP HD (High-Definition) cameras to replace Analogue SD (Standard Definition) cameras at a ratio of at least 2:1 if not 4:1 thereby putting greater pressure on removing the issue of the higher costs of CMOS vs. CCD based solutions. And since most of the cost associated with CCTV cameras is involved with the installation, this replacement ratio is a significant advantage going forward.

Combine this with the most recent

advances in Control-room Management Software (CMS) or Station Management Software (SMS) now available, and coupled with improved public broadband networks that are able to move CCTV images around and through 'external' networks, and you can see that we are now entering a new phase of implementation of IP based surveillance solutions.

The thought of throwing away the billions of £, $ or € worth of existing CCTV installations does not sit well with property managers in the public sector, let alone the private sector, as these systems are still doing a good job in most cases. However, most new-build projects are now moving forward with all IP systems. Take the new state-of-the-art Network Rail development at Reading, UK, in which the station is all IP – the first of Network Rail's 2,500+ stations to go that way – and according to Network Rail's own engineering teams that presented at IFSEC 2012; from 2013 they do not envisage using any new CCD (analogue) based solutions in any new upgrades and will be looking at using 'qualified' CMOS IP based solutions.

But Network Rail is not the only transport agency looking to move to new technology solutions. Major networks across Europe, Asia and the U.S. are all now starting to roll out projects to move to IP based technology and bring CCTV into a higher level of integrated systems management software, thereby enabling greater use to be made of the information provided by security solutions.

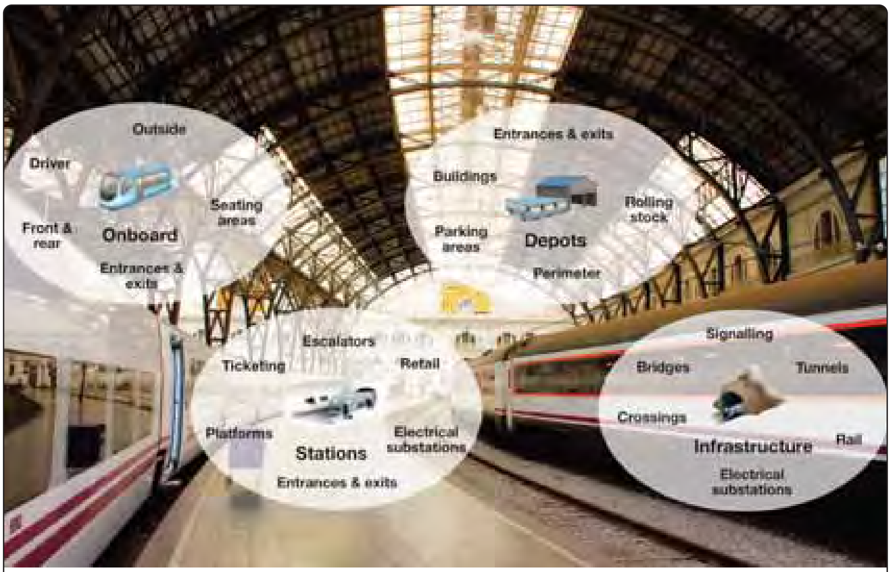


Figure 2: Rail control rooms have increasing numbers of data sources as illustrated above

The current lead supplier and the main developer of the IP based camera technologies are AXIS, a Swedish-based camera maker. IP solutions are starting to be deployed globally across major transport networks, and as opportunities to upgrade occur, such as new projects or refurbishment projects, then these are moving to IP solutions either in part or on mass.

TABLE 1 CCTV format Transmission budget table (24hrs operation)

Stream	Res	FPS	TX	Store
MJPEG	CIF	1	156Kbs	3.4GB
	CIF	25	2.9Mbs	84GB
H264	CIF	1	11.2Kbs	0.24GB
	CIF	25	279Kbs	6GB
MJPEG	**4CIF/D1/480P**	**25**	**12Mbs**	**260GB**
H264	4CIF/D1	25	860Kbs	19GB
H264	1MP	25	2.8Mbs	60GB
H264	**2MP/ 1080P**	**25**	**5.6Mbs**	**120GB**
MPEG2	1MP	25	8Mbs	170GB
H264	3MP	25	6.7Mbs	146GB
MJPEG	3MP	25	95Mbs	2.1TB

Some of the transport networks[1] that have started IP camera integration projects and deploying thousands of cameras include: NSB in Oslo; SL in Stockholm; Moscow Metro; SBB in Zurich; and EMT in Madrid, plus many others.

So why are transport networks around the world moving from their reliable and well-understood analogue solutions to introduce new state-of-the-art IP based CMOS solutions? The answer is not an easy one and varies between operators, whether bus, rail, light-rail or metro. However, the results and benefits are now becoming clear.

As my own standards committee (U.S. based APTA CCTV Standards Group TSWG1) is moving forward with a new IP camera addendum to add to our existing CCTV standards, published in June 2011, I can clearly see the areas that are of most benefit to our community.

One of the problems associated with high bandwidth CCTV data, and often the cause of much problem, is the backhaul communications networks. As anyone will know, when they try to download a video clip over a cellular network, unless you have a high performance 3G or 4G (broadband) connection, that image will take an age to store and eventually play out. The same is true of CCTV only more so. CCTV images are not intended for entertainment and some of the technical 'tricks' that broadcasters use for entrainment-based images are not applicable to CCTV, hence caution must be used when using very high order compression systems to make sure that you design your system architecture to meet not only the 'observation' needs of a control room, but also the needs of any potential need to submit imagery for legal or post-event analysis needs. It's easy to compress away your image resolution or frame rates, but once it's gone there is no way to get it back. Hence there is the need to ensure that you design your CCTV system and associated communications networks and storage requirements accordingly. **Table 1** provides looks at transmission and storage overheads, which then needs to be matched to any 'link budget' of the communications networks. If you have fibre, you

> ***Modern control centres are now routinely looking at not only CCTV feeds, but also Access Control, SCADA based alarms and alerts, communications as well as HVAC and building services making control rooms highly integrated nerve centres of modern transport networks***

have the luxury of being able to use the strands to transmit relatively high-resolution images. (Cautionary note; if you rent your fibre links, you may want to be clear on your network's overall annual rental costs per MB which can be very high in some regions). If you use third party RF based networks (2G, 2.5G, 3G or the latest 4G networks) then you will want to ensure that any compression and storage architectures take account of any network transmission limitations or coverage issues. Bear in mind that if you are using a single 1080P IP camera, it can need up to 5Mb/s or more of transmission bandwidth (upload) even with H264 compression and 120GB of storage required for a single 24hrs (25FPS) worth or recording (see **Table 1** opposite). Start multiplying your cameras to 100 or 1,000 and you can see why Tera Byte's (TB) or even Peta Bytes (PB) of storage per day are commonly referred to (see **Table 2**).

While we are discussing transmission, bear in mind that most IP cameras will give you the option of two, or even three, outputs at the camera head. In this way you can chose to store locally (at the edge) a high-resolution image and then only send back to the control room a compressed image suitable for presentation that can then be 'squeezed' using H264 or even the new H265 (coming soon) to better suit the network capabilities, if this is an issue.

TABLE 2 Data capacity and transmission terminology

kilo-	k or K	10^3
mega-	M	10^6
giga-	G	10^9
tera-	T	10^{12}
peta-	P	10^{15}
exa-	E	10^{18}*

** Not generally used to express data speed*

Some IP cameras also feature SD card storage but are clear that you have enough capability in the card and understand any lifecycle restrictions on such cards. The current CCTV standard for transit systems requires that 31 days of recording be retained without any frame reduction and this could be a challenge if you are storing 120GB per day! An SDXC card is available in 128GB and this could give you one day of flat out operation. If they ever make the 1TB or 2TB versions then this will change that to almost a month. With consideration for a reduced operating 'day' or reducing stored FPS to less than full frame rate, you could squeeze 31 days into this card so distributed storage at the edge 'could' be an option as long as you understand how to get the full resolution image should you need it for evidence reasons. However, bear in mind the cost of these cards and how many read write cycles they will support and network attached storage (NAS) may be a more cost effective option.

The improved performance of CMOS sensors enables previous light sensitivity issues to be overcome, certainly in current 720P technology and also with high quality 1080P sensors (full HD), which is where we shall be setting our minimum resolution requirement in the new addendum. The introduction of 16:9 aspect ratio enables four current 4:3 aspect ratio cameras to be replaced with a single IP camera enabling a greater field of view and also offering up the 'potential' for a virtual PTZ capability overcoming a common issue of ownership of the PTZ joystick control often seen between control rooms of different authorities!

The benefits don't end there. As we see control room software becoming more integrated due to the use of IP based technologies, greater use can be made of integrated control centres allowing increased control over areas that only a few years ago would not have been able to be integrated in the way that we can now.

Modern control centres are now routinely looking at not only CCTV feeds, but also Access Control, SCADA based alarms and alerts, communications as well as HVAC and building services making control rooms highly integrated nerve centres of modern transport networks. Advanced Video Analytics are also playing an increasing part in reducing workload in the control rooms as these algorithms become more reliable. Depending on the type of functions monitored by Video Content Analytics (VCA), these can be carried out either at the camera head or via server based software in the control centre. One increasing area of potential use of VCA is in tunnel and portal protection where monitoring of access to tunnels is critical for both safety as well as security. Existing 2D analytics are being replaced in some cases by 3D analytics using two cameras to provide a reliable depth of field element making the system more reliable to detect people entering tunnels alongside moving or stationary trains. Guideway protection for high-speed lines is also an increasing requirement for reliable VCA to detect intrusions to the track and in the stations some agencies are using VCA to monitor lines at ticket booths to improve productivity and customer service.

Whether you call this a PSIM, an extended VMS (Video Management System) or a CMS/SMS, the trend is clear. Many more designs for new and existing transport networks are using the benefits of improved IP capabilities to much greater extent.

From a number of recent projects I have been involved with, designing the availability of cost effective and reliable CCTV based IP technology is now having a beneficial impact on systems capabilities. Quality of imagery in new, as well as refurbishment projects, has increased significantly by use of HD grade cameras where needed and having the ability to re-use existing legacy analogue cameras within a new CMS architecture will only increase the deployment of these systems as greater integration of IP based systems find their way into the control room!

Reference

1. Information provided by AXIS Communications Ltd

BIOGRAPHY

Dave Gorshkov is a professional business developer and entrepreneur with extensive 'hands on' commercial experience, combined with technical engineering credentials, in the international high technology market place. He has specific experience of developing businesses in the semi-conductor, wireless communications, surveillance and intelligent transport systems global markets. With over 25 years of experience in managing and developing international businesses, 15 years of which has been at board level, Dave is well accustomed to reviewing business operations of both 'Turn Around' and 'New Ventures' and understands the specific requirements of high technology channel development for both hardware and software solutions across a wide range of international market opportunities. With proven business skills in the identification of both commercial and technical goals, Dave's expertise in the area of high technology business development has been recognised by the UK Government's department of Trade and Investment (UKTI) who have retained him for the past three years to support FDI activities globally for UK PLC. Dave is now concentrating on developing his own projects with high technology companies globally considering Foreign Direct Investment (FDI) in the overseas technology markets. His consulting company, Digital Grape Business Services, is also a founding member of the www.UKInvestment.org. Dave's technical expertise has also been recognised in his appointment, for a second term, as Chairman of the Technical Standards Working Group (TSWG1) in the U.S., where he has been responsible for the development of the recently published standards for CCTV & VCA systems used in the critical area of public transport. With numerous articles and Business Intelligence reports to his credit, Dave uses his commercial and technical experiences to contribute to a number of technical and business publications in the UK and U.S. Dave is also a Chartered Engineer (CEng) and Fellow of the IET.

Patrik Anderson
Director Business Development Transportation,
Axis Communications

Public transport security goes digital

As Reading becomes the first railway station in the UK to install IP-based security cameras, this article examines the benefits of IP surveillance and why more and more transport operators in Europe rely on this technology.

IP-based surveillance is fast becoming the technology of choice for transport operators looking for ways to enhance passenger and staff security and improve operational efficiency. Reading train station recently became the first railway station in the UK to announce that it is installing HDTV quality IP-based surveillance cameras. Once rollout is complete in April 2013, the station will have one of the most sophisticated surveillance systems in the UK's transportation sector.

The new surveillance system is currently being implemented as part of a complete station redevelopment programme to accommodate more trains, new platforms, fewer delays and a much improved train station. It will significantly improve CCTV coverage at the station, give Network Rail real-time access to live and recorded videos in HDTV quality, and provide a safer environment for rail staff and passengers.

Many transport operators in Europe already benefit from the advantages offered by IP surveillance cameras. In addition to providing real-time footage that can be viewed by numerous stakeholders, the HD quality images guarantee sharp and crisp pictures that we are now used to from our home high-definition televisions.

Central surveillance in real-time

Instead of only using surveillance video forensically, transit authorities can now connect all security cameras – from stations, depots, buses, trains and tunnels – to one or a few security centres. Operators can view live video from any IP camera at any time and share them with response resources, police and authorities via portable computers, PDAs or mobile phones. This enables efficient detection, prioritisation, response and investigation of the many and diverse incidents that occur every day. From vandalism to robbery and violence, incidents can be detected at an early stage, evaluated in the security centre with live video as they develop, and responded to with the appropriate resources. And even if several incidents happen at the same time, a network video solution provides the real-time video images needed to get a complete view of the situation.

In the past, when investigating an incident on the transport network, the investigators would have to spend hours locating the right

video footage. In the digital system, they can find the relevant files almost instantly.

There are dedicated cameras for the various parts or the transit system on the market, as the requirements differ depending on the setting – whether the camera is installed on-board buses and trains, at stations, terminals and rail yards, or along the infrastructure.

Products available include vibration-resistant on-board cameras and recorders, plus vandal-proof indoor and outdoor cameras. And with IP cameras on offer that include thermal and low-light cameras, it is even possible to detect people and vehicles in complete darkness, so the cameras become important tools against trespassing, metal theft and graffiti.

The market's leading cameras make the most efficient use of bandwidth and storage capacities, and the ease of installation and repositioning also reduces the total life-cycle cost. Finally, one HDTV camera can cover a larger area than four analogue cameras, so fewer cameras are needed compared to an analogue CCTV installation.

Reading train station is set to become the first station in the UK to benefit from HDTV quality IP-based surveillance. The station's new IP-based security surveillance system is currently being rolled out as part of a complete station redevelopment programme to accommodate more trains, new platforms, fewer delays and a much improved train station.

IP-based surveillance proven in some of the busiest transit systems in Europe

In the case of Reading station, as one of the busiest stations in the UK outside of London with more than 14 million passengers travelling through annually, Network Rail was keen to improve the overall coverage of the entire site by using megapixel cameras to enable larger scenes to be monitored than had previously been possible with analogue solutions. An initial trial clearly demonstrated the benefits of IP cameras. As Raul Marquez, a Senior Project Engineer for Network Rail explains: "We analysed footage of customers passing through the ticket barriers and very quickly realised that by using just two megapixel cameras we were able to see far wider coverage of the station."

"The cameras are also extremely easy to install which in a station is a real plus point as cameras can be relocated very quickly and easily if the need arises," adds Raul. "These cameras are also a greener option as they use less power than our previous analogue CCTV system and are simpler to maintain."

The applications of IP-based surveillance can range from enhancing security at just one station to covering whole fleets to multi-site implementations with many thousands of cameras. Several of the larger urban transit systems in Europe have already made the switch to IP-based surveillance.

For example, La Empresa Municipal de Transportes de Madrid equipped the entire bus fleet of Madrid with approximately 8,000 security cameras. Münchner Verkehrsgesellschaft installed a digital surveillance system in close to 450 underground trains and street cars in the Munich metro system. And in Stockholm, after a recent installation on more than 400 buses, there are now more than 18,000 IP cameras on stations, buses and underground trains.

All these operators have benefited from increased actual and perceived security in their transit systems. The IP surveillance systems have helped them to attract more passengers, minimise service disruptions and lower the costs of dealing with vandalism and metal theft. Millions of passengers travel through the largest transport systems every day, with hundreds of incidents happening. With real-time surveillance, it is now possible to make an informed decision on how to respond appropriately to each incident, and ultimately to make passengers and staff feel safe.

Intelligent video applications will provide even greater benefits in the years to come. While some are still at a development stage, there are already several reliable intelligent applications available today, including motion detection, license plate recognition and tampering alarms. With motion detection, a camera can automatically detect and alert for activity in areas where there is not supposed to be any activity. This makes it easier to detect, for example, graffiti artists at depots, tunnel trespassers or suspect activity along the rail infrastructure.

Decades ago, the transportation sector was one of the early adopters of CCTV surveillance as security plays such an important role in making public transportation the preferred choice for commuters. Now, transport operators can again lead the way in the shift from analogue to digital surveillance technology. To keep their systems running smoothly, with as few interruptions as possible, they need to know what is happening at all times, whether at stations, on board individual trains or along the transit infrastructure. And as some operators have already discovered, IP video can make all the difference.

BIOGRAPHY

Patrik Anderson joined Axis in 1997, and is focused on building the company's offering and presence in the transportation sector on a global basis. Patrik has vast experience in business development in many industry sectors as well as long leadership in product and project management.

CONTACT DETAILS

AXIS® COMMUNICATIONS

Axis Communications AB

Emdalavägen 14
SE-223 69 Lund
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30
Web: www.axis.com
Twitter: http://twitter.com/axisipvideo

OTN Systems

COMMITTED TO GET YOUR INFORMATION ACROSS

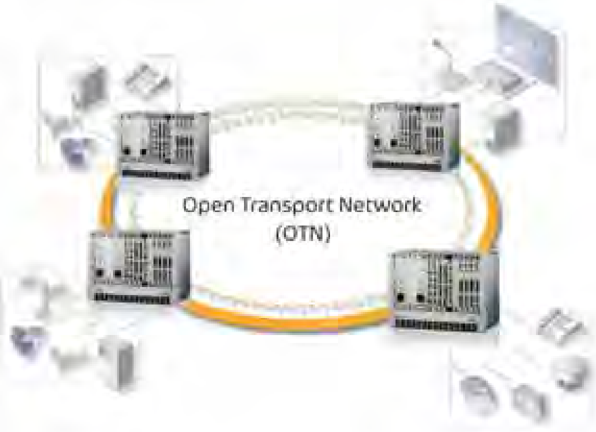
OTN Systems: Multi Service Networks for Metro & Rail

OTN Systems develops dedicated fiber optic communication networks for metros, light rail systems, people movers and railways worldwide.

The Open Transport Network (OTN) solutions are based on the latest fiber optic technology and offer you the most reliable, open and easy-to-use systems available on the market.

Connect all railway applications on a single optical backbone

OTN is a reliable and deterministic digital communication backbone for CBTC, telephony, public address, radio systems, emergency help points, passenger information systems, ticket vending, data, SCADA, LAN and CCTV that fully supports your operations. The OTN network transmits all the information between stations, track side locations and the operations control room. All applications can be connected directly to the broad range of interface cards which are configured in the modular OTN network nodes. In addition to Ethernet and IP based applications also legacy applications (analog & digital) can connect easily to the OTN network.



Features

- **Redundant** fiber optic communication provides **high capacity** and immunity to interference, even over long distances.
- OTN guarantees **bandwidth availability** to each individual application, also in worst case conditions.
- **Modular** OTN network nodes facilitate maintenance and system modifications or expansions.
- Integrated network based **Video** surveillance & recording solution exceeding 2000 cameras
- Operational **Simplicity** ensures low Cost of Ownership
- **Cyber security:** keep hackers out!
- **Future proof:** designed to have a life span of 15 years and more.

N70 node: the most reliable 10 Gbps backbone with hard QoS and advanced L3 routing capabilities

- 10 Gbps redundant optical backbone
- Dedicated bandwidth per application: 100% QoS
- Power over Ethernet (PoE+) on all ports
- Extended temperature range

You can experience OTN at leading transport authorities around the world. Please contact us to visit an existing installation in your region.

www.otnsystems.com info@otnsystems.com

Maurice Tan and Vaswani Anand Lachman
Security & Emergency Planning, SMRT Trains Ltd

SMRT's security and emergency planning philosophy and initiatives

Singapore is a small city-state with a multi-racial and multi-religious society. Being an open economy with one of the world's busiest sea and air ports, an international financial hub and a popular tourist destination, Singapore is vulnerable to potential terrorist threats that could disrupt its social fabric and economy.

Singapore – a potential target for terrorists and terrorism

Singapore has been directly targeted by terrorists since the 1970s. On 31 January 1974, members of the Japanese Red Army (JRA) and the Popular Front for the Liberation of Palestine (PFLP) attacked the Shell oil refinery complex on Pulau Bukom (a small island lying south of Singapore) and subsequently hijacked the Laju Ferry as a means of escape. On 26 March 1991, Singapore Airlines flight SQ 117 was hijacked by Pakistani terrorists. More recently, Singapore and Indonesian authorities uncovered activities by Jemaah Islamiyah terrorists who planned bombings of critical infrastructure, including two stations within the SMRT trains network.

The land public transport eco-system in Singapore

The land public transport system in Singapore comprises the Mass Rapid Transit (MRT) system, the Light Rapid Transit (LRT) system, public buses and taxis, with approximately 5.1 million passenger trips made daily. The system is built around the 'hub spoke' concept that allows for the integration of transport facilities with other facilities.

The porosity of the eco-system makes it a vulnerable target. Recent attacks across the globe on land transport systems have suggested that trains, buses and their related infrastructure in the form of stations and depots are attractive and vulnerable targets. Attacks in Madrid in March 2004, the London Underground in July 2005 and the Mumbai railway station in November 2008 prove this point. Train networks around the world remain a soft target because of their accessibility, openness and potential for mass causalities.

Dealing with security threats to the public transport system requires a multi-agency approach. In Singapore, this need is addressed by the Public Transport Security Committee (PTSC). The PTSC comprises members from the Ministry of Transport (MOT), Ministry of Home Affairs (MHA), Land Transport Authority (LTA), Singapore Police Force (SPF), Internal Security Department (ISD), Singapore Civil Defence Force (SCDF), National Security Coordination Centre (NSCC), Joint Counter Terrorism Centre, SBS Transit and SMRT Corporation Ltd. The committee provides a holistic approach to address public transport security challenges and threats. It undertakes comprehensive reviews of the security arrangements and recommends improvements to the security of the public transport system. The public transport operators, such as SMRT, remain responsible for the security of our depots and all assets.

SMRT – Singapore's premier multi-modal transport provider

SMRT has operated and maintained Singapore's first MRT system since 1987, a network comprising multiple lines totalling almost 130km, encompassing four depots, 81 stations and approximately 150 trains. Daily ridership on the train network is estimated to be roughly 2.3 million passenger trips. The rail corridor spans the entire length and breadth of the island and connects the business district and heartlands.

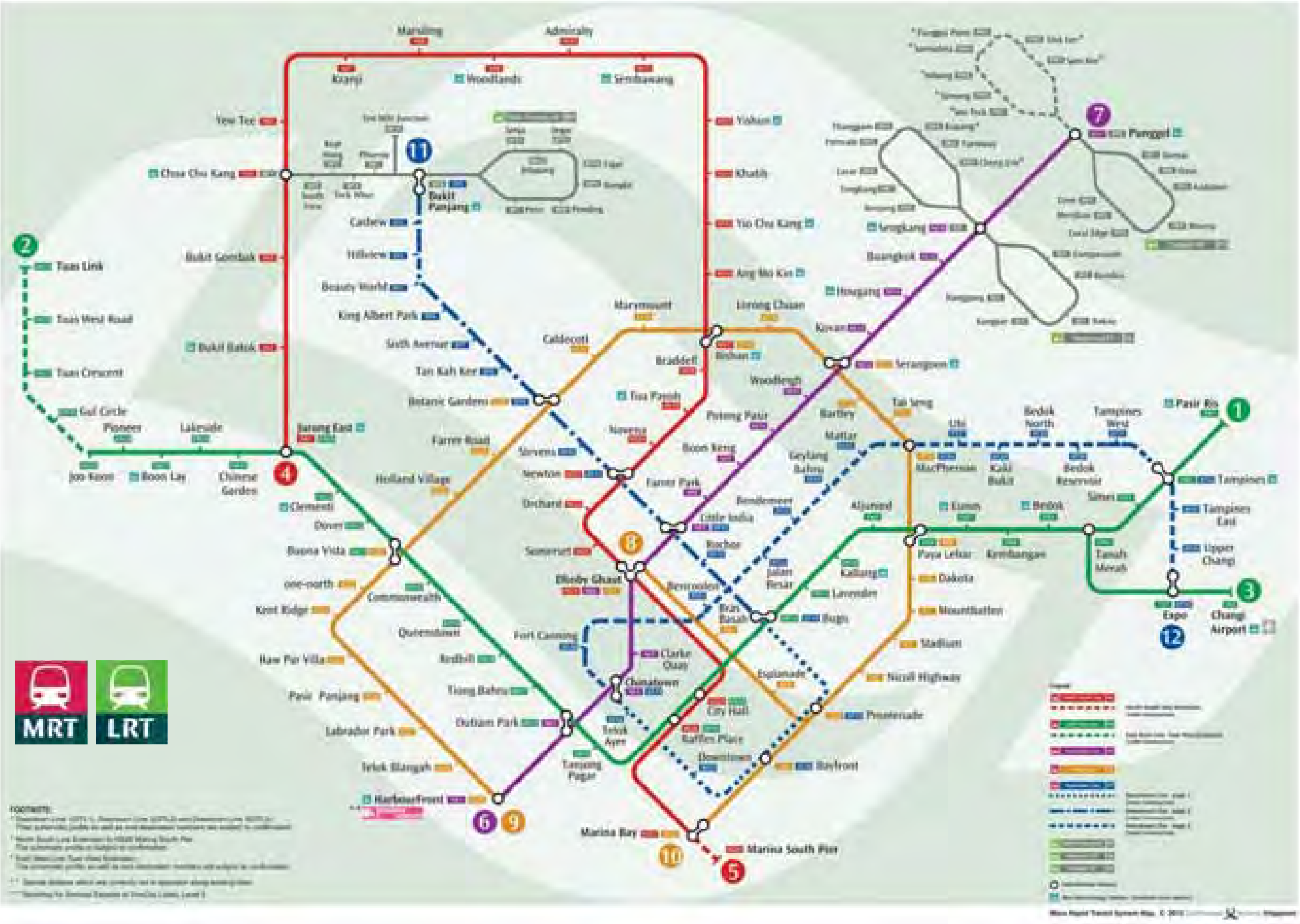


Figure 1: The MRT and LRT system map

In addition, SMRT operates Singapore's first fully automated LRT system. Within the train network, we lease approximately 34,400m^2 of commercial space. On the roads, SMRT provides 94 bus services connecting the Western and North Western areas to the rest of Singapore with a fleet of approximately 1,050 buses, and is a leading taxi operator with a fleet of 3,000 taxis.

The vulnerability of the system, and the organisation, was put under the microscope in May 2010, when two vandals cut through the perimeter fencing at SMRT's Changi Depot and spray-painted graffiti on the side of a train. Just over a year later, in August 2011, a SMRT train was again found spray-painted with graffiti. Investigations revealed that the train had been vandalised while at Bishan Depot. The two incidents raised public concerns. If untrained and unsophisticated vandals could gain access to secure facilities, it did not take a stretch of one's imagination to see that trained terrorists would be able to do the same with far greater impact than the nuisance of vandalism.

> ***'Dealing with security threats to the public transport system requires a multi-agency approach'***

The two incidents were overshadowed by a major service disruption on two days in December 2011. More than 200,000 commuters were affected by the service disruptions which saw trains immobilised within the tunnels and in some cases, commuters forced to walk the track to the nearest stations. The scale and complexity of the disruption was unprecedented, and the organisation was left with much to ponder in the wake of the incident.

These incidents served as a catalyst to reshape the organisation's approach to security and emergency planning. Increasing numbers of passengers and facilities present challenges that include higher exposure to crime and terrorism as well as a greater vulnerability to disruption which will require more sophisticated protection and preparedness capabilities. This article details the key components of our improvements so far.

SMRT's security and emergency planning philosophy

SMRT's mission is *'To be the customer's choice by providing a safe, reliable and friendly travel experience that is enhanced through convenient and innovative service'* and enshrined within this is our promise to provide our customers with a safe and hassle-free journey. As the cornerstone of the local public transport scene, our ability to fulfil this promise has major repercussions on the lives of the citizenry. The adverse impact on Singapore's image as a safe and secure city-state would also have serious repercussions on its status as a major tourist hub and financial centre.

Core to this promise is the belief that our calling is beyond protecting a train system or public transport network. Rather, it is the belief that we are protecting an essential service that is the lifeblood of our nation. This belief allows us to go beyond the 16 Security and Emergency Planning (SEP) professionals or 7,000 staff that makes up SMRT, and reach out to key national security agencies such as the Ministry of Home Affairs (MHA) as well as the population at large, who serve as volunteers on our network.

Creating a framework for security

The philosophy is well grounded in a robust and rigorous security and emergency planning management framework which covers the initial assessment of threats and vulnerabilities, prevention and protection, and response to and recovery from incidents and crises.

Assess

We adopt a three-pronged approach of threat, vulnerability and consequence assessment. This includes the examination of 'soft spots' in key installations through internal and external security audits. Internally, audits are conducted by various parties including the corporate Internal Audit Department and the Security Audit team within SEP. 'Red Teaming' activities are a constant feature that helps identify potential 'soft spots' in the system. Most of these activities are mirrored at the national level through the government agencies responsible for land transport and security, and these supplement our assessment, allowing for multiple perspectives and solutions to be considered and implemented.

> ***Recent attacks across the globe on land transport systems have suggested that trains, buses and their related infrastructure in the form of stations and depots are attractive and vulnerable targets***

Prevent

All elements of deterrence fall under this category. We aim to prevent any potential terrorist attack and thwart other threats to the public transport system. This extends from the implementation of security measures and standard operating procedures for staff to the engagement of citizens to facilitate the identification and reporting of any potential threat.

Protect

We proactively protect our critical assets through people, technology and processes.

Respond

Should deterrence and protection fail, we must effectively handle major incidents to mitigate its impact to the commuters, company and community.

Recover

The need to recover from an incident expeditiously is critical to ensuring the longer term viability of the public transport system and the company. Understanding the business and its critical functions allows for the development and implementation of operationally viable Business Continuity plans. To this end, regular exercises and collaboration with national security agencies cater for an immediate and effective response in times of need.

The framework is a recurring and continuous process because new threats will

emerge and will require fresh assessment to ascertain the adequacy of the security measures in place. The framework helps safeguard the public transportation network.

Key processes and components

The framework provides a platform through which key processes and activities are established. The key processes within the framework are (a) risk assessment, (b) risk management and (c) crisis management.

Risk assessment

The risk assessment process allows the organisation to define, determine and analyse risk. This is not a stand-alone security and emergency planning risk assessment but is administered as part of the corporate risk assessment process which also involves the identification of business, financial and operational risks. This comprehensive assessment enhances the linkage between the security and emergency planning factors and other elements within the business. Risk events such as external threats and corporate-level and business unit risks are reviewed every six months. This process also motivates the organisation to discuss top risks and emerging risks, and determine Key Risk Indicators (KRIs) and the subsequent risk mitigation and reporting activities. To ensure that security and emergency planning remain key elements of management discussions, KRIs are discussed both at Senior Management level and with the Board of Directors on a quarterly basis.

Risk management

The process of risk management can be divided into several categories. There is no scientific approach to this categorisation. Rather, a practical and operationally feasible approach is advocated to facilitate awareness and adoption by relevant parties. Key to any risk management process is the security hardware (including technology), its people and the practices or processes that complement it.

Since the breach at Bishan Depot in August 2011, SMRT has implemented a series of security improvement projects to bolster the security hardware throughout the network. Much of this was done in consultation with the government security agencies. In fact, based on operational requirements, some of this went beyond the established requirements.

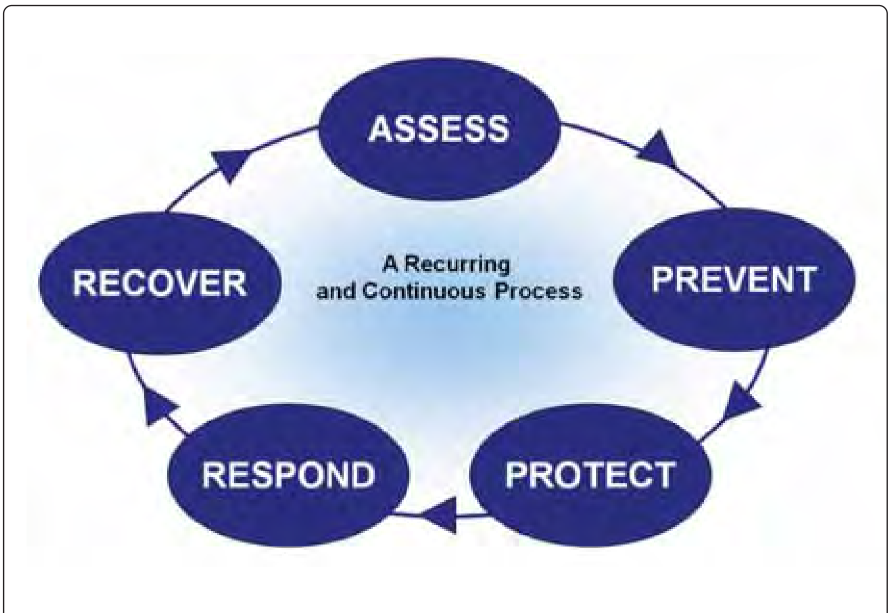


Figure 2: Security and Emergency Planning Management Framework

> *SMRT has operated and maintained Singapore's first MRT system since 1987, a network comprising multiple lines totalling almost 130km*

For example, regulations dictate that the security infrastructure at train depots be improved by strengthening the fencing, installing CCTV and enhancing the lighting around the perimeter. Given the vast space that each depot occupies, coupled with the manpower constraints faced by the domestic security industry, SMRT invested in a Fence Intrusion Detection System (FIDS). This technological leverage allows us to safeguard Bishan Depot, which sits on 300,000m^2 of land and has a 9.5km perimeter in a densely populated public housing environment, with an optimum number of security staff. Synergising this technology with the traditional manpower patrols has significantly improved our deterrence and detection capabilities.

Other hardware and technological improvements include the establishment of crisis management and emergency response rooms, which will allow real-time views of the situation and communication with the people on the ground. It also brings together other pertinent information such as national and international news broadcasts, and connectivity to regulators and national security agencies. This will undoubtedly improve our response to incidents by providing decision-makers with up-to-date information and the capability to reach out to all our staff spread across the network in a timely manner.

Multiple factors are considered when determining and implementing our security hardware. Cost is an inescapable feature, as is the effectiveness of the hardware in deterring or detecting threats. But equally important is the feasibility and practicality of implementation in our operational environment. Trains and buses must remain readily accessible, convenient, and inexpensive. The deployment of metal detectors, X-ray machines, explosive sniffers, and armed guards, which have become features of the landscape at airports, cannot be transferred easily to stations or bus stops. The delays would be enormous and the costs extortionate – public transportation would effectively be shut down[1].

Manpower is a critical aspect of any security management framework. One of the most important threat reduction measures in any system is the continued vigilance of the staff, their awareness of anything out of the ordinary, and their prompt communication of that information to the organisation's security team or management[2]. To this end, the security mindset is instilled into all staff from the onset at the point of orientation. This is reinforced through awareness programmes that must be conducted within their first year of service. The programme integrates security theory with on-site learning and a practical detrainment exercise, ensuring all SMRT staff are aware and capable of executing fundamental emergency responses should the situation arise. Regular reinforcement of the security mind-set is

Singapore's MRT network comprises multiple lines totalling almost 130km, encompasses four depots, 81 stations and approximately 150 trains

Copyright: kentoh / Shutterstock

ensured through annual 'e-quizzes' and regular 'Red Teaming' exercises.

Employees working in front-line service roles – including all station staff, train officers and bus drivers – have additional security training elements built into their technical training programmes. Administrative and support function staff who play various roles during an incident are also put through relevant training programmes. For example, administrative staff that form a customer service team are put through a one-day customer service workshop that addresses topics such as crowd control and dealing with difficult customers.

To further strengthen security ownership, the organisation introduced the 'Premises Manager Programme' which empowers line managers to assume primary responsibility for security matters at their workplace. The oversight function has also been tightened with the formation of Security Committees at the depots which report to a Security Steering Committee.

> ***'Should deterrence and protection fail, we must effectively handle major incidents to mitigate its impact to the commuters, company and community'***

Most recently, we reviewed the provision of security services at our facilities. In recent history, this service has generally been outsourced to private security firms. Moving forward, SMRT has taken back some command and control elements on the ground. This is possible through the implementation of a 'hybrid security services model' in which the line supervisors are staff of the organisation while the security officers are employees of the private contractor. This collaboration allows for both organisations to specialise in our areas of comparative advantage and allows SMRT to reap the benefits of this synergy. For example, the security partner is able to provide for a 24-hour central command centre and additional security resources that SMRT may deploy on a pay-per-use basis.

The third essential component of the risk management process is that of policies, processes and practices. This component allows for an element of standardisation and consistency in adoption and application.

Five key documents serve as security and emergency planning reference points within the organisation. The 'Security and Emergency Training Policy', the 'Security Audit Charter', Security Policy Statement, BCM Policy

Statement, and the 'Emergency Management Plan' serve as a reference guide for all security and emergency planning matters within the organisation. These documents are easily accessible to all staff through the intranet and major revisions or updates are disseminated to all via Security and Emergency Planning Circulars.

Our security practices have also evolved through the years taking into account the changing business and technological landscape. As detailed above, perimeter patrols are now complemented by the use of CCTV and FIDS. The same applies to the checks on trains prior to service.

Following the August 2011 breach, SMRT installed CCTV cameras at train launch points. These cameras allow for the SMRT Operations Control Centre (OCC) staff to monitor the exterior of the train prior to its launch for revenue service ensuring that the train is free of graffiti. Trains are also equipped with on-board cameras to deter and detect potential threats while in service. Stations and bus interchanges have significant CCTV infrastructure and are also protected with Access Control Management Systems (ACMS) to prevent unauthorised entry into sensitive areas.

> ***'Regular exercises and collaboration with national security agencies cater for an immediate and effective response in times of need'***

As with the hardware and manpower, the processes and practices are regularly tested through 'Red Teaming' exercises. Audits are also regularly conducted to ensure appropriate compliance with the established processes.

Crisis management

The December 2011 service disruption served as a painful lesson to the inadequacy of the Crisis Management process. Two key improvements were immediately implemented. First of all, we have realigned the organisation's incident management plans with the government service disruption plans. This will improve synergy between corresponding agencies in dealing with a crisis. Secondly, we have streamlined the organisation's Crisis Management and Emergency Response structures and plans to more effectively deal with a range of incidents and crises such as prolonged service disruptions.

SMRT maintains a constant state of preparedness through regular internal and external exercises. External exercises usually involve the government agencies such as the SCDF, SPF and LTA.

SMRT maintains a robust BCM system that ensures we remain resilient in the face of adversity. Our BCM strategy establishes processes that enable us to respond, recover and resume critical business functions efficiently and effectively. SMRT has been certified with the British (BS 25999) and Singapore (SS540:2008) standards, and is currently working towards certification with the new ISO 22301 BCM standards.

As a provider of an 'essential service', SMRT is clear that relying on our staff alone is insufficient. Collaborating with and engaging the larger community to be more proactive in safeguarding the public transport eco-system is critical. To this end, SMRT launched the SMRT Community and Emergency Preparedness (SCEP) programme in December 2006. The programme aims to develop a community that is better prepared for and able to respond to acts of terrorism and major train service disruptions. Developed in consultation with MHA and LTA, more than 15,000 participants have attended the programme.

SMRT moving forward – building societal security and psychological resilience[3]

The public transport infrastructure in Singapore is fast expanding. The rail network is expected to grow from 128.6km to 278km by 2020. Travel demand is also expected to grow from 8.9 million journeys a day to 14.3 million journeys a day by 2020[4]. With rising affluence, the expectations of the average commuter will continue to increase. On the other hand, the ageing public transport infrastructure, its heavy utilisation and the constant external menace posed by terrorism are serious challenges to our ability to deliver a safe, reliable and friendly travel experience.

While much has been done since the security breaches and the service disruption of 2011, SMRT maintains that a more proactive citizenry and a comprehensive emergency response plan that integrates the collective capabilities of the national emergency response agencies as well as our community of volunteers will go a long way to enhancing the resilience of the public transport network in the face of any potential threat.

While we will continually strive to improve our software and hardware to keep our network secure, we realise that major improvements can only happen when we effectively integrate ourselves into the wider national security eco-system and tapping on the social infrastructure. We stand by our motto: 'Security is Everyone's Responsibility'.

References

1. Jenkins, B.M, April 2004, Terrorism and the Security of Public Surface Transportation
2. U.S. Department of Transportation, January 2003, The Public Transportation System Security and Emergency Preparedness Planning Guide
3. Ramakrishna, K., 6 Sep 2011, The SMRT Security Breach: Strategic Implications in the Post 9/11 Era, RSIS Commentaries, NO. 128/2011
4. Land Transport Authority, 2008, Land Transport Masterplan

BIOGRAPHY

Vaswani Anand Lachman is Deputy Director of Security & Emergency Planning at SMRT Trains Ltd. Prior to his current appointment, Vaswani Anand Lachman helmed portfolios relating to Learning & Development, Talent Management, Employee Engagement and Performance Management at SMRT. He has also served in various capacities at the Singapore Workforce Development Agency (WDA) and the Ministry of Home Affairs (MHA). His portfolios at MHA included organisational excellence at the Singapore Prison Service and International Affairs at the Ministry Headquarters. Vaswani Anand Lachman holds a Masters in Business Administration (Strategic Management) from Nanyang Technological University (NTU).

BIOGRAPHY

Maurice Tan is currently Manager of Security & Emergency Planning at SMRT Trains Ltd, but used to serve in the Singapore Police Force and was previously with Suntec City Management (a mega mixed-used complex comprising of five office towers and a shopping mall) serving as Deputy Head overseeing and managing the Crisis Management & Security Services in Suntec City. Maurice has qualifications and experiences in management, security management and fire safety management. He is trained in crime prevention, security, business continuity, project management and fire safety management.

Maurice's past experiences include security training, community engagement, crisis management and management of security projects. His past project references at SMRT include being actively involved in the implementation of Asset Protection, Threat Mitigation Profiling Training and Covert Auditing, which he successfully helped implement in-house as course developer and trainer.

He has built up a good network of crisis management and security professionals from Singapore and overseas through visits, courses and conferences. He is currently working on various security projects to enhance the security environment in SMRT.

7th Annual Conference

Rail & Public Transport Safety and Security 2012

Where Safety Meets Security

20-21 November 2012

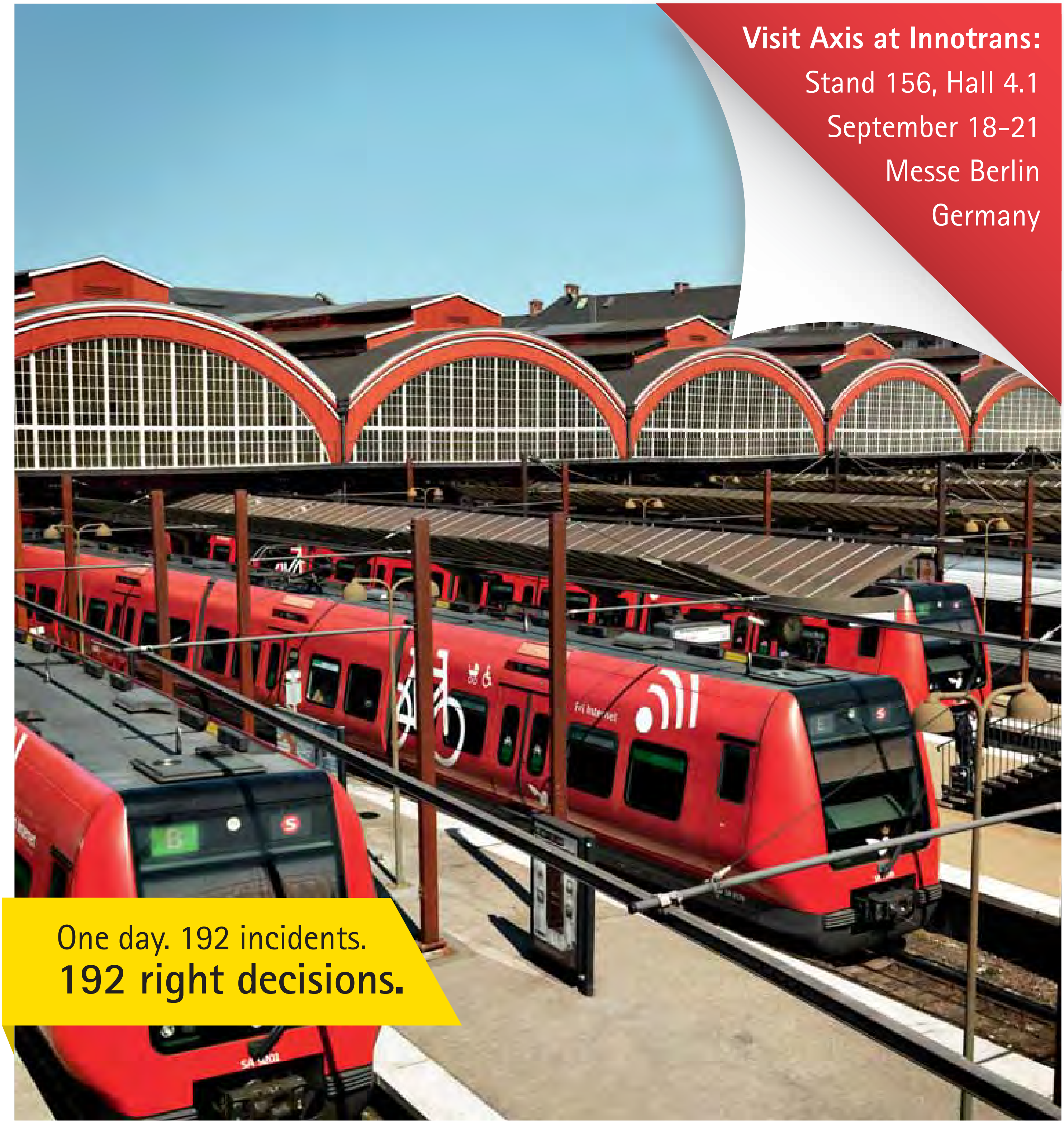
The London Hilton
Canary Wharf Hotel

www.eurotransportmagazine.com/rptss

Organised by

european railway review
Europe's leading rail industry journal

eurotransport
Europe's leading transport industry journal



HDTV
NETWORK VIDEO