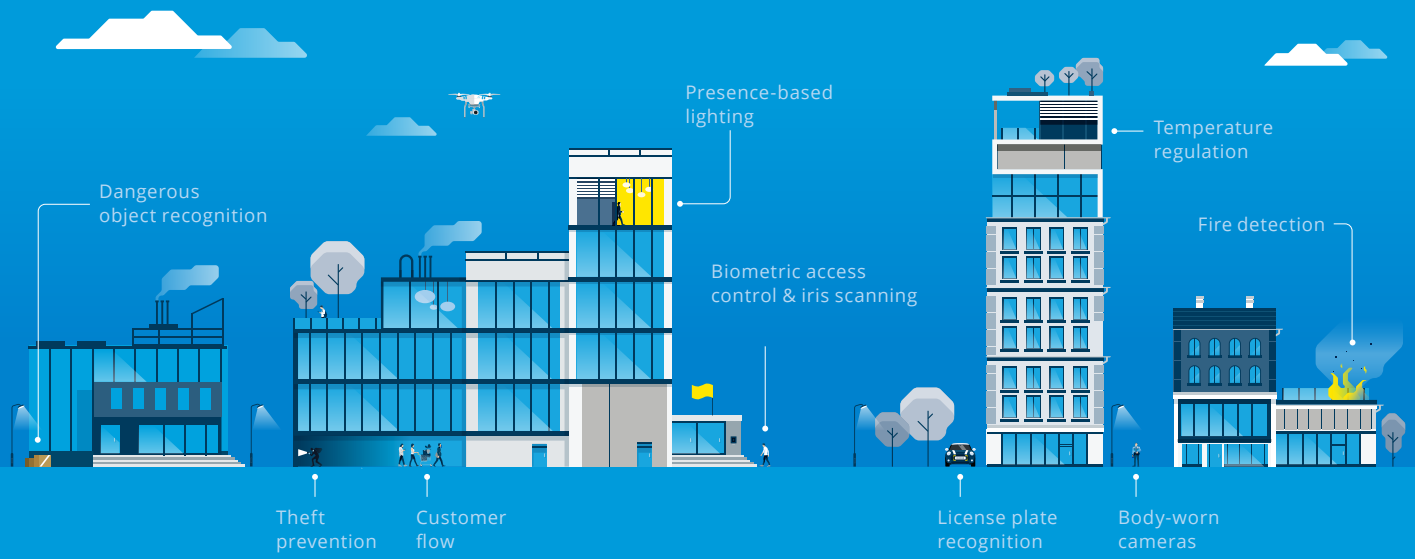
Public transport security in the age of smart cities

Challenges and solutions for European bus, metro and rail companies

MAKE THE WORLD SEE



WELCOME TO THE AGE OF SMART CITIES

A new era of public transportation security
According to the European Parliament, 240 European cities have made progress towards becoming smart. All cities in Nordic countries are smart, and most cities with populations over 100,000 in Italy, Austria and the Netherlands are smart, as well as half of British, Spanish and French cities.[1]

What makes a city smart?
The European Commission defines a smart city as a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and businesses.

But a smart city goes beyond the use of smart communication technologies to focus on better resource use and less emissions. This means upgraded water supply and waste disposal, more efficient ways to light and heat buildings and smarter urban transport networks. It also means more interactive and responsive city administration and safer public spaces.

Improving transportation in smart cities
Many smart cities use technology to improve their public transport systems. With the goal of reducing reliance on private cars to reduce emissions, pollution and congestion, improve public spaces and boost convenience for citizens, they are using information systems that collect data about traffic, vehicles and usage of different modes of transports. This helps cities make public transport more efficient and accessible, which is drawing more people, especially the younger generation, to using it.[2]

But what does the smart-city movement mean for security in public transport? What effect does an increase in passengers have on security risks and threats? What does the explosion of data mean for cyber-security and data privacy? And how can security professionals work closer with law enforcement and city officials to proactively mitigate security threats?

In this e-book, we answer these questions and more by taking a helicopter view of smart cities and analyzing their impact on public transportation. We'll explore four key areas:

- **Part 1** – Six trends affecting public transportation in smart cities
- **Part 2** – Four key security challenges in public transportation
- **Part 3** – How to heighten proactive security with an open video surveillance platform

We hope you find this information useful. To discuss anything of the advice in this e-book, please get in touch.

[1] European Parliament. How many smart cities are there in Europe?
[2] European Commission (2017). Smart Mobility and services, Expert group report

Part 1

Six trends affecting public transportation in smart cities

Understanding trends helps determine future security solutions

Based on our collaborative work with security professionals across European public transport hubs, at Milestone, we've identified six trends that are affecting public transportation in smart cities. By analyzing these trends, we become armed with knowledge that helps us work closely with our clients in smart cities to identify security solutions that best suit their needs. Here they are in no particular order.

1. Urbanization

Over the past few decades, more and more of the world's population has been moving into urban areas creating denser cities. Today, nearly 54.5% of the world's population lives in cities, and it's expected to grow to 70% by 2050.[3] This is a key driver affecting transportation challenges and the aggressive movement towards smart cities and Intelligent Transportation Systems – and sets the scene for many of the following trends.

2. Internet of Things (IoT)

The number of physical objects that are connected to and communicating over the Internet is growing exponentially – that's what the IoT trend is all about. IoT is enabled by the shrinking size and falling cost of sensors that can be attached to almost anything, which enables new ways of tracking and coordinating a variety of processes, changing the way security teams, city officials and police departments access data.

Between 2017 and 2030, the European IoT market is expected to grow at CAGR of 18.32%. It is estimated that the transportation and logistics segment will capture 23% of total IoT revenue in Europe.[4]

3. Acceleration and complexity

Change across Europe is happening faster than ever before, and this increases complexity – both in terms of public transportation environments and societies in general. For security professionals, this brings challenges of keeping ahead of technology, cultural and behavioral changes before they have the potential to disrupt public transport systems.

4. Personal safety and security

With news of people falling victim to breaches of personal data security, growing reports of physical violence and harassment, and most recently, worries of illness spreading in public spaces, personal safety and security is top of mind for European travelers and commuters. It has become the mandate of security professionals and IT managers in public transport organizations, in collaboration with city officials and law enforcement, to create an environment where passengers feel safe and secure while in transit.

5. Sustainability

A sharper focus on climate change and resource scarcity is driving passengers towards managing their environmental footprint to a greater extent than before. At the same time, the European Commission is supporting 100 European cities in their transformation towards climate neutrality by 2030. With the transport sector making up 14% of global greenhouse gas emissions, it makes sense for European smart cities to continue to offer citizens cleaner, more efficient ways to commute. This will attract increasing numbers of commuters to public transport.[5]

6. The rise of platforms

The digital age has witnessed an explosion of online platforms, which enable organizations to leverage technology to meet escalating demands for speed, interactivity, and the personal touch. Global platform businesses from Amazon and Facebook to Uber are becoming increasingly central to public and private life.

Across European smart cities, platforms are transforming key economic sectors and spheres of life, including finance, health care, education, and transportation. Platforms enable smart cities to integrate an endless range of technologies together towards building safer, more secure and more efficient public transit systems.

7. Big and open data

The increasing number of sensors in cities (and the data they collect) is critical to creating a truly connected city, monitoring almost everything in the infrastructure from lights to road conditions. In smart cities, all types of data are gathered and stored, from an individual's location to their daily activities, and it is constantly used across different organizations. However, this raises concerns around the ownership, processing, use and security of that data. Could it be exploited? How can citizens be protected – and whose responsibility is it to do so? And what about consent?

[3] UN World Urbanization Prospects, The 2014 Revision
[4] Goldstein Research (2020)
[5] European Commission. Making European cities greener, Towards clean and smart mobility, Horizon 2020

Part 2

Four key security challenges in public transportation

Safety and comfort are a top priority for city officials

City officials understand that security has the potential to influence travel behavior at every stage of a journey from pre-trip planning through the journey itself and to post-trip evaluation.

As a matter of both protecting passengers and enticing them to use public transportation more, city officials and transportation companies are placing security as a top priority of infrastructure management.[6]

However, as the technological and cultural trends of smart cities take hold, they present a growing set of challenges for security professionals responsible for the safe and efficient operation of public transportation.

Here we delve into the top four challenges for ground transportation as identified by the European Commission and offer some related advice from our own public transportation security experts.

In the UK, it was estimated that reducing fear of crime could increase public transport patronage by 3% at peak and 10% at off-peak times.[7]

[6] European Commission: Research theme analysis report: Transport security
[7] Newton, A. (2004) Crime on public transport: "Static" and "non-stack" crime events. Western Criminology Review

Part 2

Four key security challenges in public transportation

1. Threat detection and prevention

Threat and vulnerability identification and detection are the starting points of the threat-protection process. With a large number of sensors placed throughout the environment, smart cities have an advantage here. However, for bus, metro and rail networks, the focus has largely been on systems for unattended surveillance and technologies to better design stations and terminals to reduce the impact of security incidents. This approach is aimed at responding to threats and events instead of anticipating them.

Tip: In light of the growing threat and increasingly connected transport networks, public transport companies need to be more proactive approach in identifying future threats. The European Commission recommends taking a more universal and collaborative approach and to work with technology and security partners to integrate the right technologies and functionalities at all critical infrastructure levels.[8]

[8] European Commission: Research theme analysis report: Transport security

Part 2

Four key security challenges in public transportation

2. Crisis management

Transport systems have always been sensitive to the effects of natural and man-made crises, such as earthquakes, weather extremes, and armed conflicts. Not all critical events rise to the level of catastrophic emergencies, but a late or inadequate response to even a minor incident can put people, operations, and reputations at risk.

Having an effective response plan in place could reduce the most immediate, medium, and long-term impacts, saving lives, jobs, property, and millions of euro. Today's key challenge for smart cities in building an effective response plan is how to intelligently link information sources and stakeholders with related issues of interoperability of procedures and technologies.

Tip: A comprehensive crisis management strategy begins before the impact of an event is felt and continues after the immediate crisis has ended. This full life cycle strategy can be broken into four distinct phases: assess, locate, act, and analyze. We recommend taking this four-phase approach and working collaboratively with law enforcement and other city officials to gather and share intelligence on emerging situations.

Part 2

Four key security challenges in public transportation

3. Passenger security

Passengers across the transportation sector are vulnerable to different threats – that's why we take our shoes off at the airport, but we would not expect to do so in the metro station. One challenge in passenger security is how to deploy measures that meet increasing threats while meeting passenger expectations and comfort levels.

Another major challenge is implementing security measures while maintaining passenger flows through the network, particularly in large interchanges. Once again, in this area, policies and requirements are usually developed in response to specific incidents rather than proactively.

The two main security challenges identified for land transport are "avoiding interruptions to transport networks as a result of terrorist attacks and ensuring that transport does not become a means for an attack." [9]

Tip: Research shows that people experience journey disruptions differently depending on who they are and where they come from – and that passengers will feel more secure if the transport information systems and services are of high quality. Getting a deep understanding of who your passengers are, what they value, and what they need can help provide better service and a better feeling of security.

[9] EC (2017). Research theme analysis report: Transport security. European Union.

A review of international research evidence on harassment on public transport and its impacts on women's travel behavior revealed that:

- Sexual harassment on public transport appears to be a growing issue
- Harassment reinforces fear of crime, which reduces women's use of public transport
- Significant proportions of young women believe that it is unsafe to use public transport at night
- Public awareness campaigns and improved reporting mechanisms are highly valued by women[10]

[10] Gardner, N., Cui, J., & Coiacetto, E. (2017). Harassment on public transport and its impact on women's travel behaviour. Austrailian Planner

Part 2

Four key security challenges in public transportation

4. Cybersecurity and privacy
Transport security involves not only the protection of transport facilities and vehicles against destruction (such as bomb attacks) but also protection from abuse of the devices and software that control the traffic. This includes, of course, the personal data produced by the devices passengers use during transit. Given the quickly changing security and mobility landscape, the number, frequency, and severity of cyber-attacks in the transport domain are expected to grow.[11]

Public transport companies are typically challenged with infrastructure and network control equipment that's based on legacy software and hardware when securing critical infrastructure increasingly relies on the newest interconnected ICT technologies. And this raises integration challenges.

Tip: As you plan for the future security of the public transport system, consider using open-platform technologies with a proper cyber security policy or program. Look for solutions with robust APIs that allow for flexible integration with the latest software and hardware solutions. This can help ensure integration with pre-existing platforms and technologies, ensuring transparency, knowledge-exchange, and coordination in research and action across mobility sectors. Also, look for European privacy seals or compliance to other IT industry security standards like FIPS, ISO and GDPR.

[11] European Commission: Research theme analysis report: Transport security

In 2008

A 14-year-old Polish hacker used a television remote control to manipulate a Lodz tram network, derailing four tram cars and injuring 12 passengers.

In 2016

The British transport system experienced four cyber-attacks in just one year, with cybercriminals hacking into computer networks, message boards, and individual trains.

In 2019

IT security professionals discovered hackers selling access to a Chinese rail system on the dark web that would have enabled the buyer to virtually manipulate the train control system.[12]

In 2019

A major airline faces a record $230 million fine after a website failure compromised the personal details of roughly 500,000 customers.[13]

[12] Cylus Blog: The reason why cybersecurity is so essential to the future of transportation
[13] The Guardian: BA faces £183m fine over passenger data breach

Part 3

How to heighten proactive security with an open video surveillance platform

An open-platform video surveillance system delivers an entire network of open security solutions. It offers a breadth of components from a community of technology partners that work together to create a comprehensive solution to meet each customers' evolving needs. At any time, solutions can be upgraded or added as partners develop new technologies and functionality while maintaining existing investments.

An agile, secure video management system

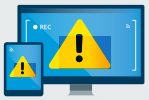
Milestone's XProtect® is an open, agile video management system that enables you to add custom, best-in-class security solutions to your surveillance, such as access control, cameras, and video analytics – all of which empower security teams to take a more proactive approach to mitigating threats and disruptive events.

Seamless integration with law enforcement and central monitoring stations

Milestone offers an open ONVIF interface for standardized and secure private-to-public video integration. It ensures full video interoperability in multivendor installations, enabling law enforcement, monitoring stations, and similar private or government organizations to easily integrate video from Milestone platforms into their central monitoring solution. This enables true interoperability and freedom of choice for large-scale, multi-vendor security deployments and seamless private-to-public video integration.

The power of video

Quicker response time
Video surveillance lets you react faster and make better informed decisions.



Efficient reporting
With software analyzing your video material, you can achieve reporting, which can save costs and help identify new security opportunities.

Reduced costs
You can also operate more efficiently to ensure both safety and cost-effectiveness.

Part 3

Proactive threat detection and prevention

Intelligent video surveillance technologies seek out threats before they can strike

Security operators used to be burdened by countless false alarms and the manual process of reviewing hours of video footage. At that time, cameras had no built-in intelligence, so surveillance recordings were only effective for analyzing past crimes and not preventing future ones.

Today video surveillance is a proactive security operation. There are three main elements to an intelligent approach to video surveillance:

1. An intelligent video surveillance platform

An intelligent video surveillance platform is equipped with monitoring software that analyses, assesses, and responds to data, events, and images it sees via intelligent cameras.

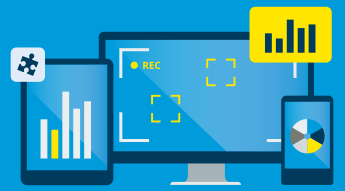
2. Intelligent cameras

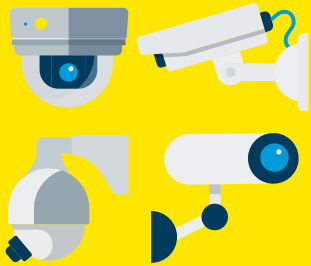
Focus on intelligent cameras that can integrate with video management systems. They actively detect individual risks and interpret and highlight security issues.

3. Sensor technology

Sensor technology can be added to your video management system to, for instance, independently recognize visual security breaches such as abandoned packages or suspicious behavior.

Milestone's XProtect® video surveillance platform with integrating intelligent cameras, AI, video analytics, and innovative sensor technologies offers the sophistication that can tell the difference between moving people and safe background conditions, such as blowing trees or splashing fountains. No longer do these areas form a security blind spot and most time-consuming false alarm scenarios can be eradicated. This means security personnel can apply their judgment and experience based on clear, actionable information.





Part 3

Quick-response crisis management

Enacting the four-phase approach to crisis management: assess, locate, act and analyze

Assessing threatening events and their potential impact used to be hampered by limited intelligence to accurately respond. Today, video surveillance technology can visualize massive amounts of real-time data within the context of an incident. This makes it possible to adequately respond in a timely manner and even preempt and reduce the scale of the crisis.

1. Assess

Technologies capable of monitoring behavior, social media feeds, weather conditions, etc., ensure that security teams can quickly see if there are actual threats and don't lose any time trying to make sense of intelligence reports. The more they can see on a 'single pane of glass,' the faster they can initiate the appropriate response.

2. Locate

Radar, thermal, AI, and video analytics technologies enable security professionals to locate threats. The information is visualized on the threat map to help determine who is actually in danger and who can respond the fastest. The emergency response then becomes targeted and more effective.

3. Act

The next step is to act and automate a response. Organizations can build and execute their standard operating procedures (SOPs) fully within our Xprotect® platform; sirens, alarms, digital signs, and messages can all be automatically activated based on event type, severity, and location.

4. Analyze

When the crisis has been responded to and the emergency handled, analysis of what occurred is needed. That's where audit and log reports can assist. Finding ways to better prepare for and respond to critical events will improve performance and effectiveness next time a similar incident occurs.

Part 3

Systematic passenger security

Increasing security methods without compromising passenger comfort

To manage increasing passenger threats facing the transportation industry, security management is looking to leverage new surveillance technologies to help streamline operations and to build stronger security programs. They also need to increase operational efficiencies as budgets are always tight

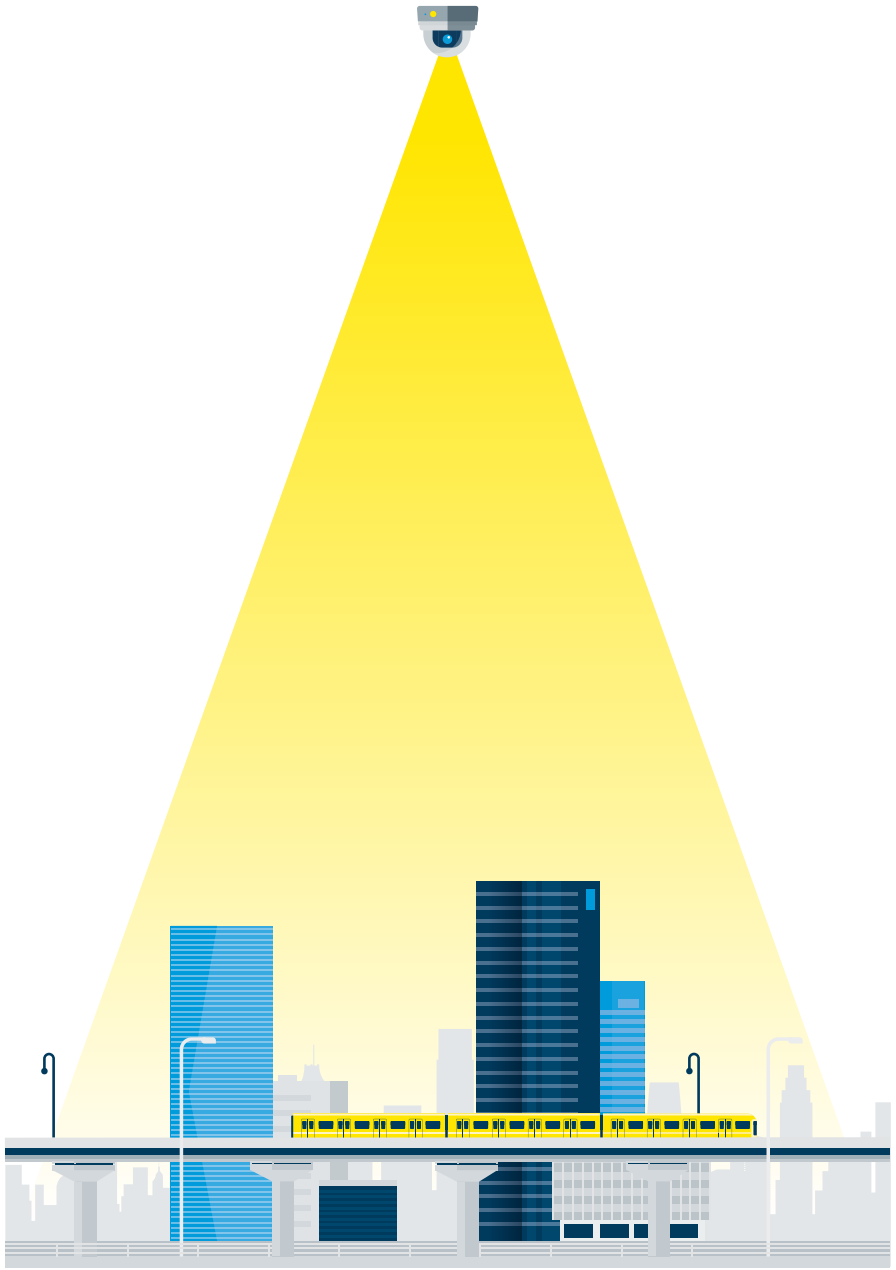
A range of partner technologies to complete passenger security

Imagine an alert is detected. Data from a partner sensor solution can be accessed via Milestone XProtect® to monitor and track the activity while security personnel get into position to investigate further. This ensures that passengers are safe, incidences of theft reduced and prevented, crowds are monitored and counted, foot traffic managed and ANPR (automatic number-plate recognition) is captured, all to reduce risk and improve security.

Solutions from our technology partners can recognize gender and age. For example, you can see how many women use public transportation and when, indicating when they feel safe and when they don't.

Solutions using facial recognition can quickly and efficiently locate a person of interest, such as a lost child, and search for shirt color, estimated height to facial features, and more. With the ability to track via recorded and live video, security personnel can start their search from the moment the child was last seen and track their movement throughout the premises.

These passenger security capabilities are why our open platform Video Management System together with intelligent cameras and highly specialized sensors, AI, and video analytics are at the heart of today's advanced surveillance solutions for transportation facilities.



Part 3

Effective cybersecurity and privacy

A comprehensive proactive strategy can dissolve threats

As transport operators digitalize their operational technology, the risk of a cyber-attack is elevated, and the focus needs to be on controlling and protecting this architecture. No enterprise is completely immune to cyber-attacks, but a comprehensive proactive strategy can eliminate many threats.

With Milestone XProtect®, it's possible to reduce the likelihood of disruption resulting from cyber-attacks.
It enables:

- Implementation of security best practice
- Establishing an effective risk governance structure in line with other risk types and maintaining board engagement
- Establishing a process to better understand the threats and risks to the organization and setting of risk appetite for cyber exposures
- Establishing incident-response capability with tested incident-response plans, minimizing the impact of any cyber-attack

GDPR and data protection

The GDPR and the Data Protection Act 2018 are in place to regulate the processing of personal data to protect privacy and prevent data breaches. Milestone XProtect® was the first major video management system to obtain the EuroPriSe (European Privacy Seal) GDPR-ready certification. This ensures users that they have the right foundation to build GDPR-compliant video surveillance installations, including a holistic set of data privacy tools, ready-to-use templates, and privacy awareness training for end users.

Milestone XProtect® cybersecurity includes Milestone cybersecurity development policy, Milestone Secure by Design philosophy, and the Milestone hardening guide. It also includes the Milestone Cybersecurity Training Track which can provide you with the knowledge and skills you need to optimally design and securely deploy your XProtect® System.

MAKE THE
WORLD SEE

milestone

Masthead
Milestone Systems A/S Headquarters
Banemarksvej 50 C
DK-2605 Brøndby
Denmark
Telephone: +45 88 300 300

Any questions?
Please reach out to us **here** if you have any questions or inquiries.

For more information visit:
milestonesys.com

Sources:
European Parliament: How many smart cities are there in Europe?
European Commission: Research Theme Analysis Report: Transport Security.
European Commission: Smart Mobility and services, Expert group report.
Goldstein Research (2020) Europe IoT Market: Size, Share, Trends, Growth Factors, Key Players, Opportunity Assessment And Demand Analysis.
European Commission: Making European cities greener, Towards clean and smart mobility, Horizon 2020.
Inform: Platforms are increasingly key to cybersecurity.
Verdict: How data is powering smart city micromobility and public transport.
Cylus Blog: The reason why cybersecurity is so essential to the future of transportation.
Australian Planner: Harassment on public transport and its impact on women's travel behaviour.
United Nations: UN World Urbanization Prospects, The 2014 Revision.