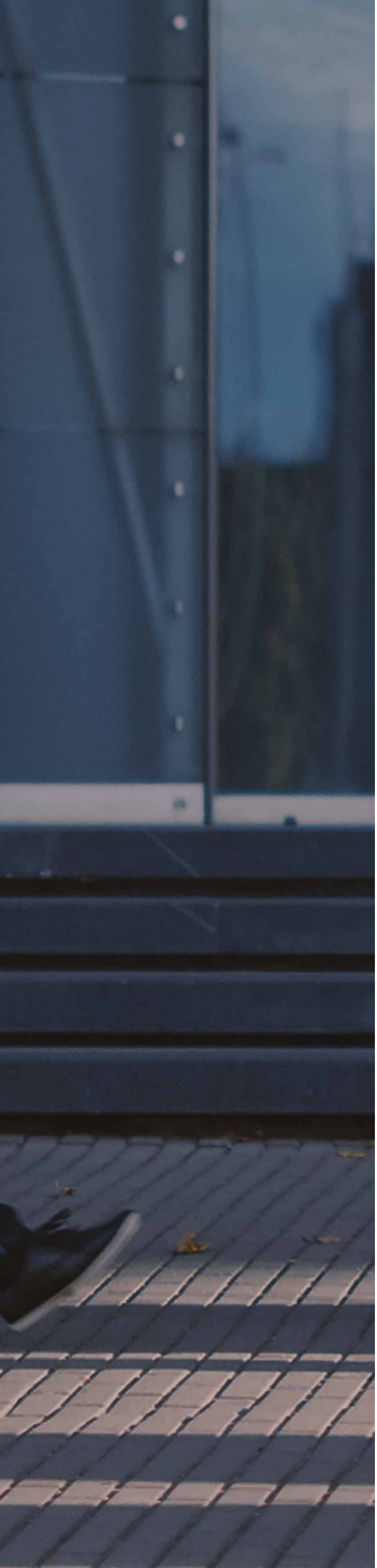
A Synectics Guide To

AI Surveillance Solutions for Public Spaces

Public Space Security and Surveillance

SYNECTICS


16103.70190 _ 14541.64281



Contents

This guide explores one distinct growth area, looking at how AI solutions can be used to better protect busy public space environments. Covering everything from the tech you'll need to real-world applications, it will help you understand how AI might become a valuable part of your surveillance team.

Introduction

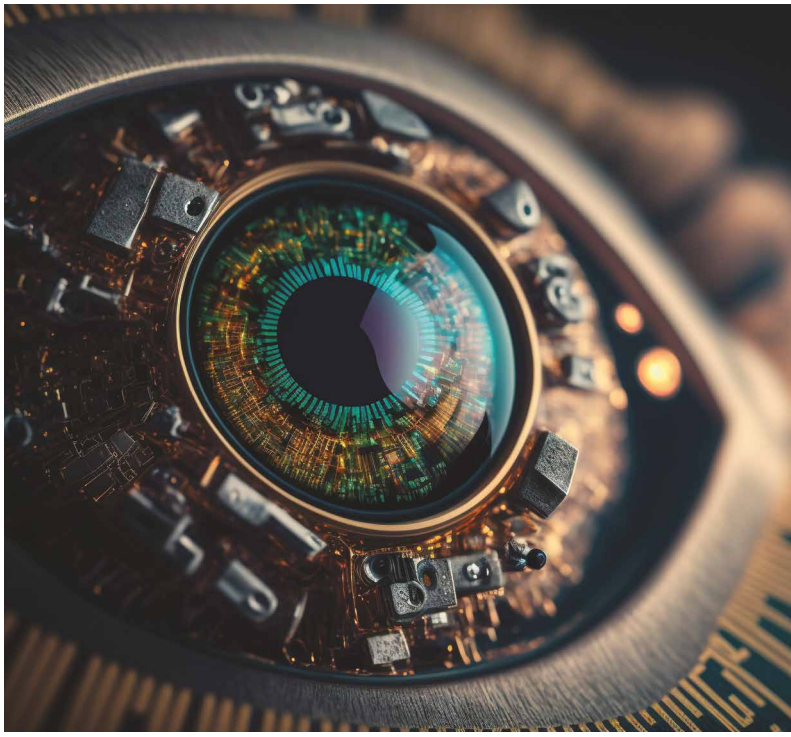
Wherever large groups of people gather – from towns and cities, hospitals, and transport hubs, to campuses and major event venues – surveillance solutions play a vital role in identifying risks, preventing harm, and investigating incidents.

Continuously monitoring them is a massive undertaking that requires significant manpower. It's also prone to error. Teams tasked with watching hundreds of video feeds can suffer from observational fatigue, easily resulting in things being missed and slow response times.

This guide looks at how AI can help solve this problem. Specifically, how AI-driven video surveillance analytics can be used – proactively and forensically – to protect members of the public.

The global Artificial Intelligence (AI) video analytics market is expected to be worth over $75.35 billion by 2028, with a diverse range of sectors increasingly leveraging the technology to advance their surveillance capabilities[1].

What is Meant by AI in a Surveillance Context?



AI has become a complex term but at a basic level it is 'a field which combines computer science and robust datasets to enable problem-solving[2]'.

In a public space surveillance context, the datasets in question typically relate to information from camera footage. Data from a wider range of integrated sensors and systems can also be included, but this guide will primarily focus on AI-based video analytics.

AI software or firmware loaded onto devices, uses complex algorithms to process and analyse images against these datasets to 'recognise' people, vehicles, shapes, specific event scenarios, and behaviours – applying intelligence to the footage captured. Modern AI algorithms are constantly evolving based on what they see and generating new data, which is why you will often hear this process referred to as 'video surveillance with generative AI'.

AI algorithms can be applied:

1. **At the edge, where cameras feature onboard AI capabilities**
2. **Natively within a video management system (on premises or cloud-based)**
3. **Using integrated AI engines (on premises or cloud-based)**
4. **Or involve a mixture of all three**

[1] https://www.secureredact.ai/articles/cctv-body-worn-cameras-video-analytics-retail-gdpr
[2] https://www.ibm.com/topics/artificial-intelligence

The Foundation of AI: Understanding Metadata

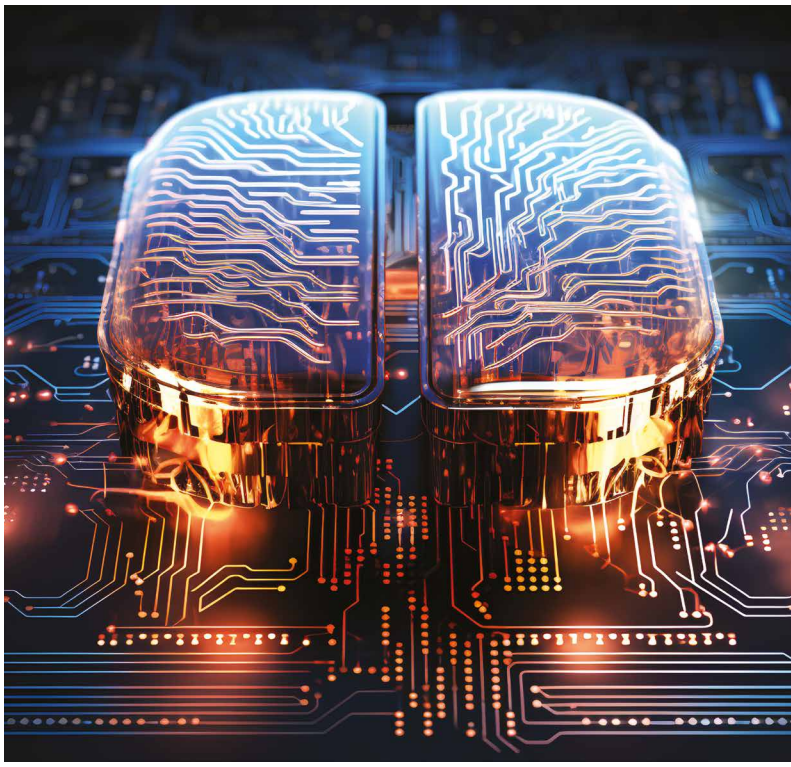
Wherever the analysis of content takes place, the key to successful AI implementation is always metadata.

Machines can't watch and understand video footage as a human would. But they can be taught to classify and describe the information captured by surveillance cameras. This information is known as metadata. It is essentially what turns unstructured video content into recognisable and actionable information.

Examples of metadata in video surveillance

- Location
- Time
- Colour
- Size
- Speed
- Direction of Travel
- Shape
- Volume
- Dwell Time

Going granular with deep learning



Deep learning is a term used to describe AI models that process data in a way that mimics the human brain. As the name suggests, these models can be used to add a layer of deeper learning to metadata descriptions, in order to make them more precise and granular in nature.

To illustrate the value of this for video surveillance, consider the following example.

Metadata Analysis	Colour	Vehicle	Movement
Deep learning AI model applied	Blue	Car	Current co-ordinates and direction of travel
AI model refined	Blue	Hyundai Santa Fe	Current co-ordinates, direction of travel
AI model further refined	Blue	Hyundai Santa Fe with licence plate EXAMP13	Current co-ordinates, direction of travel and speed

The Tech: What You Need (and What You Need to Know)

This section looks at the specific solutions that leverage AI, turning metadata into actionable intelligence, and what you need to know about using them.

AI-enabled cameras

This description typically refers to IP cameras where AI processing occurs within the camera as a stand-alone function. Previously, these types of cameras were relatively limited in their capabilities due to the processing levels required.

But this has changed. Camera vendors have adopted the latest generation AI-enabled chipsets from manufacturers such as Ambarella. These advanced chipsets have led to enhanced deep learning functionality 'at the edge', meaning many cameras can now apply accurate real-time analysis to the scenes they capture. Estimates suggest that 30% of cameras sold in 2024 can embed deep learning.

Video Management Systems

Many Video Management Systems (VMS) now offer built-in AI capabilities as standard. The key benefit of using AI here is that, in addition to analysing live video data, AI can be applied to recorded footage.

This is particularly important for using AI as a forensic tool for investigative purposes.

Integrated AI engines

As the name suggests, this term refers to a dedicated AI engine that is separate to but integrates with your surveillance solution to analyse live and recorded footage. Your VMS provider may offer this as a bolt-on to your core solution (meaning you don't have to replace your existing VMS to benefit), or provide integrations to a wide variety of third-party AI solutions, ensuring the customer has freedom of choice to select the best-of-breed AI for their specific application.

Rules, alerts and workflows

AI-based video analytics solutions may recognise what is happening in a particular video frame e.g. a car is moving from left to right. However, they don't know what you need to know unless you tell them. Make sure your VMS allows you to create and apply rules to specific types of events detected which you can then alarm and use to trigger workflows – manual, automated or a combination of both. This ensures the right responsive action is taken.

Frequently Asked Questions

Given that AI can be deployed in various different ways using different solutions, here are some common questions about best practice adoption from a technical perspective.

1 Should AI-enabled cameras be at least 4K?

It depends on the application – for instance if you simply need to detect movement, 4K may be unnecessary. However, the finer detail a camera can capture, the more intelligence AI algorithms can apply to the image, supporting a much wider range of use cases. For this reason, you will tend to find that cameras enabled with deep learning capabilities are higher resolution. It should be noted, however, that some high-resolution cameras use significant computational power to encode the video which may lead to a lower percentage of the camera's chipset being available for AI.

2 Do I always need to have AI-enabled cameras to benefit from AI?

No, you don't. Video Management Systems with onboard capabilities and AI engines are often compatible with standard IP cameras meaning analytics can be run in real-time and retrospectively centrally rather than at the edge. However, for sophisticated analysis you are likely to get the best results from pairing AI-enabled cameras with these other solutions.

3 Are there any benefits to using cloud-based surveillance to leverage AI?

A cloud-based VMS will give you easy access to a broader variety of AI solutions, which you can integrate as needed. However, the required processing level means that hosting this in the cloud can be expensive. It may also be problematic for real-time alerts as you could suffer delays. A cloud-based solution can work well if you only need AI to analyse video retrospectively.

4 Are there any particular standards I should be aware of?

The most important one when it comes to AI is to check that your solution is compliant with ONVIF Profile M. This "standardises the handling of analytics and metadata between cameras, VMS and software platform, reducing the complexity of pairing products from different manufacturers". It's important to note that Profile M also covers cloud and server-based analytics.

Applications: Using AI in the Real World

This section looks at specific use cases for AI-driven video surveillance, breaking these down into three clear categories.

1 Improving real-time risk and crime detection

High-risk object/weapon detection

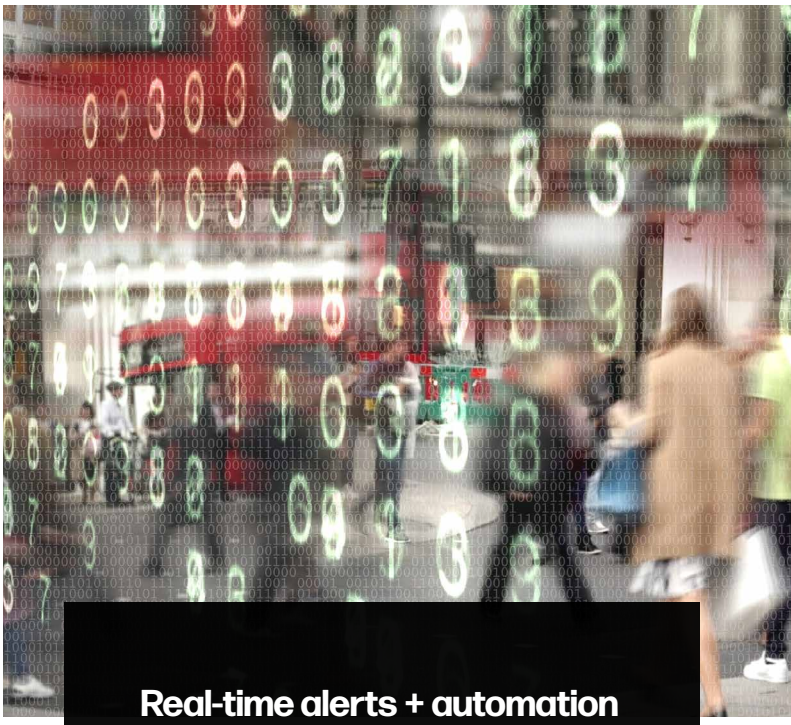
Just as deep learning can be used to train AI to spot and categorise different shapes, it can also be used to spot and categorise different combinations of shapes. For example, 'person carrying backpack' or 'arm holding knife'.

Rapid crowd formation/unusual foot traffic

AI can detect when the number of people in a specific area grows 'beyond the norm' in a given time frame. It can also detect when the direction of foot traffic is 'not the norm' e.g. people running out of an entrance. This could indicate that a security or safety incident is occurring, or that there is a problem preventing the normal flow or people in a given area.

Suspicious/threatening behaviour detection

A cyclist riding in the bike lane is not suspicious. A cyclist weaving in and out of people on a pavement in a random pattern could indicate bag snatching intent. AI can be taught to recognise patterns like this, including signs of aggression linked to body movements.



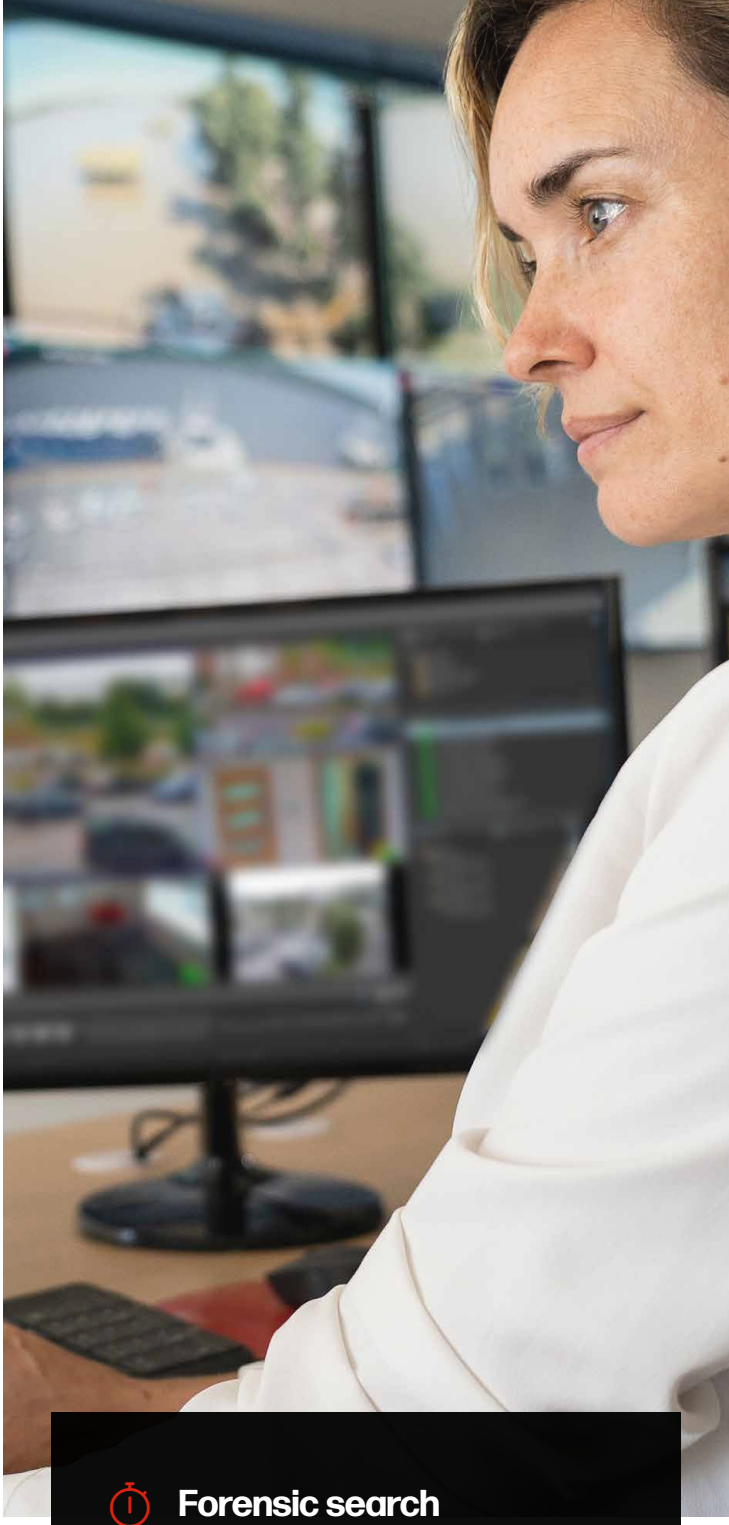
Real-time alerts + automation

In each of these use cases, the threat detected can be used to trigger a specific workflow for the risk detected. This guides operators to verify threat, notify police and dispatch specific personnel. It will also automate certain actions, such as object/person tracking, launch pre-recorded evacuation messages, lockdowns, and switch to emergency lighting.

This capability has distinct implications for areas such as terrorist threat risk mitigation. With the imminent arrival of legislation like the UK's Protect Duty, using AI in this way could become more commonplace.

2 Your new forensic scientist

AI isn't just good for instant alerts. Applying detailed metadata to video content makes it highly sortable and searchable. This offers a powerful forensic tool for rapid incident investigation. Here are some examples:



Missing person tracking

A child goes missing in a busy shopping centre wearing a red jumper and a blue hat. With AI, operators can ask the system to rapidly scan all footage using height, clothing type and clothing colour filters to show all matches as interactive thumbnails.

Person of interest search

Following a suspected theft, operators could rapidly search footage for a man, last seen on 'Example Street', wearing a green jacket and carrying a bag. Person of interest searches may also involve use of facial detection/recognition – see section on 'Safeguarding Privacy' for more on this.

Law/rule enforcement

Litter being thrown from a car. Items left in a known fly-tipping area. Cars driving in bus lanes or jumping red lights. AI can learn what metadata combinations signify these events so footage can be quickly searched for occurrences.

The same principle can be applied to ensuring monitoring operational rules are followed – for example, to identify PPE violations.

Forensic search + automation

In these cases, the primary value of automation is speed. AI takes seconds to complete a review process that might take operators minutes/hours/days to complete.

Workflows and automation can also be used here in the same way as with real-time alerts – to ensure next steps are efficient and protocol compliant. There is also potential administrative resource value, for example in automating the issuing of fines based on law breaches.

3 AI-driven planning

Because AI enables insights to be gleaned from footage and categorises incident types, it is a valuable tool for reporting and planning. Here are some examples:

Incident cause analysis

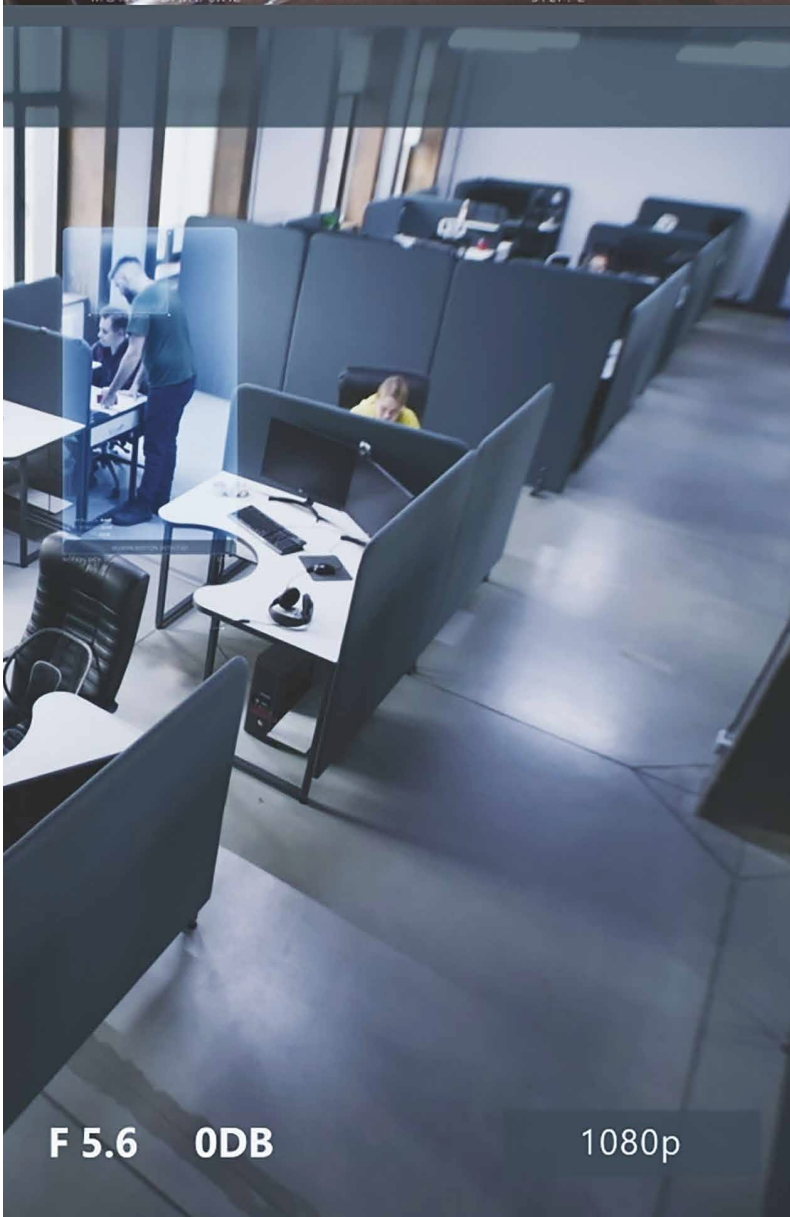
AI is used to analyse footage from numerous incidents to identify root cause commonalities – such as specific event combinations that typically result in x. This can help facilities better understand, for example, the causes of slips and trips or specific types of workplace accidents.

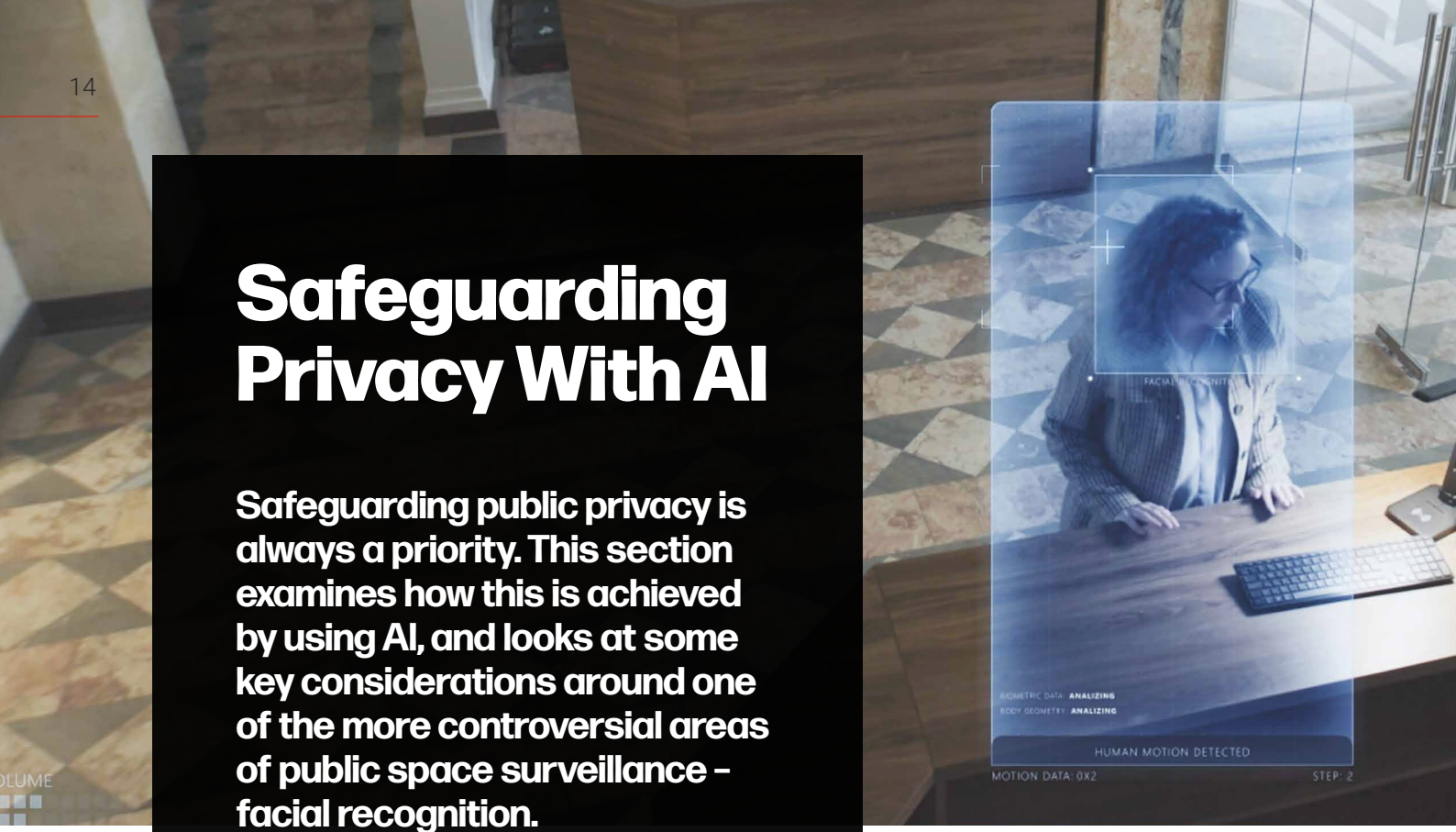
Traffic improvements

AI-driven video analytics can used to identify traffic patterns over a specific time e.g. congestion hot spots by time of day or roads that have an unusually high number of incidents. This information can then be used to inform new layouts, signage, speed limits etc. for safer, smoother traffic flow.

Crime prevention

Where might additional lighting prevent more assaults? Which areas would benefit from increased security guard or police presence? Questions like these are increasingly answered by generating reports from AI-driven surveillance analysis.





Safeguarding Privacy With AI

Safeguarding public privacy is always a priority. This section examines how this is achieved by using AI, and looks at some key considerations around one of the more controversial areas of public space surveillance – facial recognition.

AI used for anonymisation

AI can be a very useful solution for protecting public privacy thanks to its ability to differentiate between and categorise different shapes.

This capability means AI can be trained to spot and redact (blurring or completely covering) specific details from video footage such as faces, bodies, vehicles, license plates etc. depending on the requirement. It can automatically anonymise footage. This can be done in real-time or applied to video retrospectively.

Real-time facial blurring is a key trend, becoming increasingly commonplace for securing sensitive environments such as hospitals.

Three key benefits of video redaction/anonymisation

Data compliance	Especially useful for rapid, data-compliant responses to Data Subject Access Requests (DSARs) and Freedom of Information Act enquiries (FOIAs).
Responsible evidence sharing	Organisations can easily share evidence with third parties such as the police or insurers while also protecting privacy.
Public trust	Using AI in this way can be used as a way to build trust with members of the public around the use of surveillance.

Face detection vs facial recognition

AI-based face detection solutions use algorithms to analyse a shape within a video image to detect that a human face is present. They can also be used to distinguish between typically male/female feature characteristics etc. They do not identify that a specific person is present and do not match what they 'see' with a source image.

AI-based facial recognition (FR) is where the metadata is more granular, allowing very detailed facial characteristics to be identified and matched against source image metadata in order to identify a specific person.

Used responsibly in public environments, facial recognition has many potential advantages – for instance searching for high-risk watch list individuals and supporting police investigations. In fact, the Defence and Security Accelerator (DASA) in the UK is currently undertaking an exploration of solutions that will support the use of facial recognition technologies within policing and other security stakeholders.

But for those organisations concerned over adopting FR, the distinction between the two concepts is important. For example, both facial detection and facial recognition "could" be used to support a request to share video of a crime with innocent parties masked out.

Facial Detection requires more manual intervention to allow an operator to selectively retain or redact individuals from the scene, whereas Facial Recognition simply requires the operator to have a matching image of the perpetrator for the FR engine to automatically match and redact all other faces.

Do you know?

Most AI engines for video surveillance applications feature some form of facial detection and recognition capability but allow this to be configured on/off as required or even restrict its use based on the region of sale.

Conclusion

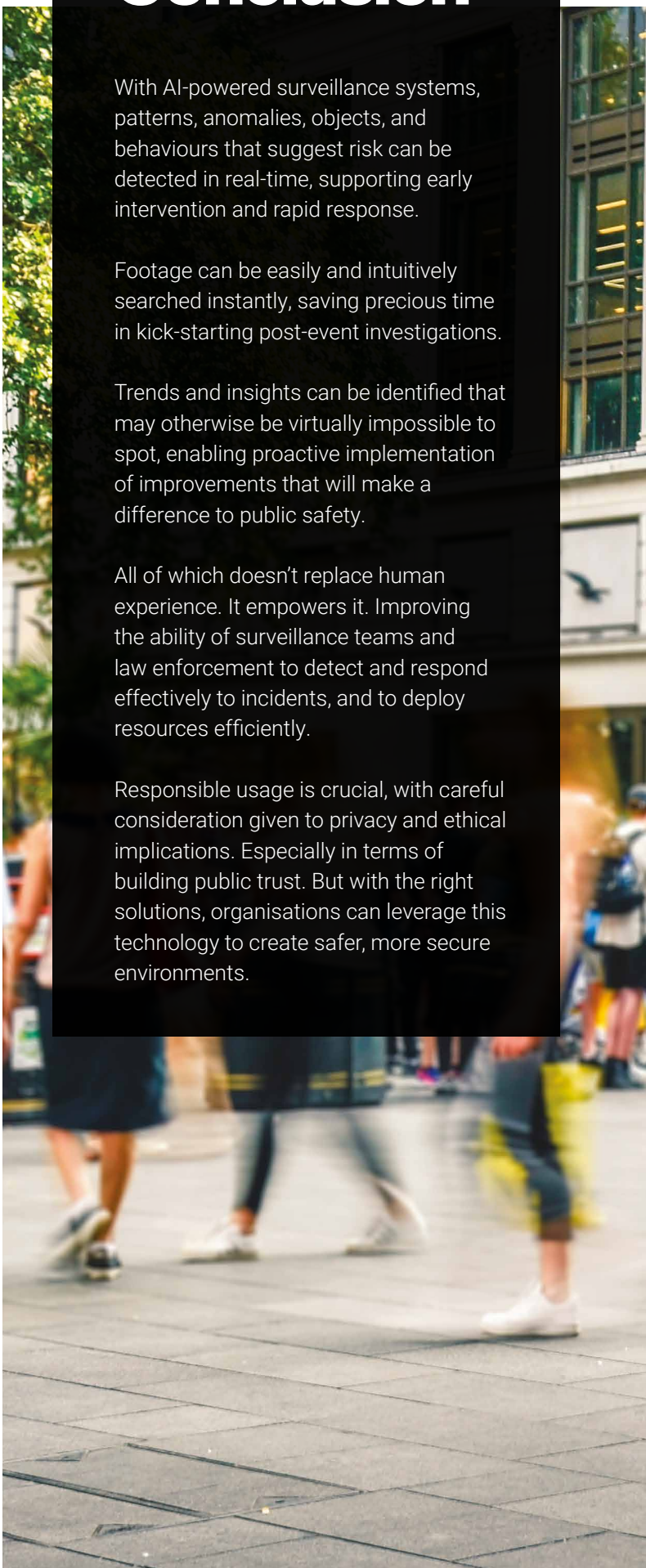
With AI-powered surveillance systems, patterns, anomalies, objects, and behaviours that suggest risk can be detected in real-time, supporting early intervention and rapid response.

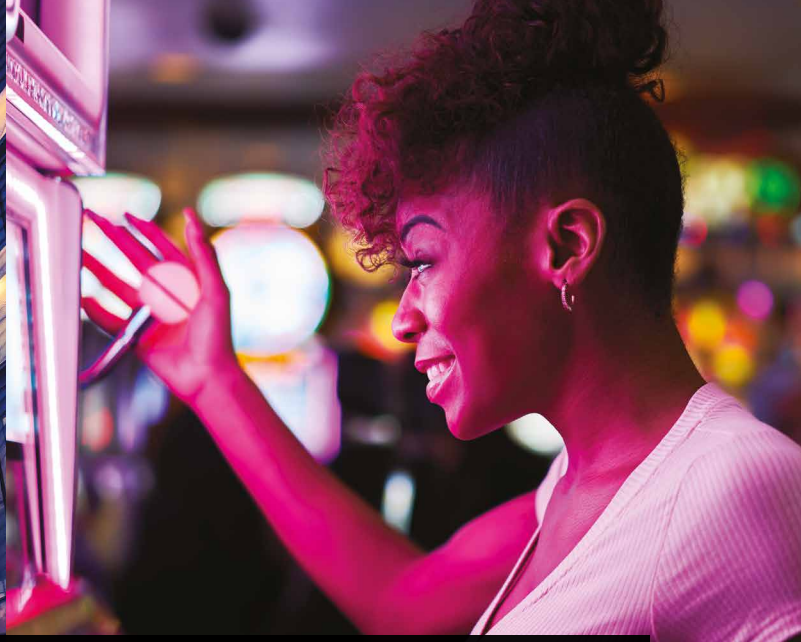
Footage can be easily and intuitively searched instantly, saving precious time in kick-starting post-event investigations.

Trends and insights can be identified that may otherwise be virtually impossible to spot, enabling proactive implementation of improvements that will make a difference to public safety.

All of which doesn't replace human experience. It empowers it. Improving the ability of surveillance teams and law enforcement to detect and respond effectively to incidents, and to deploy resources efficiently.

Responsible usage is crucial, with careful consideration given to privacy and ethical implications. Especially in terms of building public trust. But with the right solutions, organisations can leverage this technology to create safer, more secure environments.



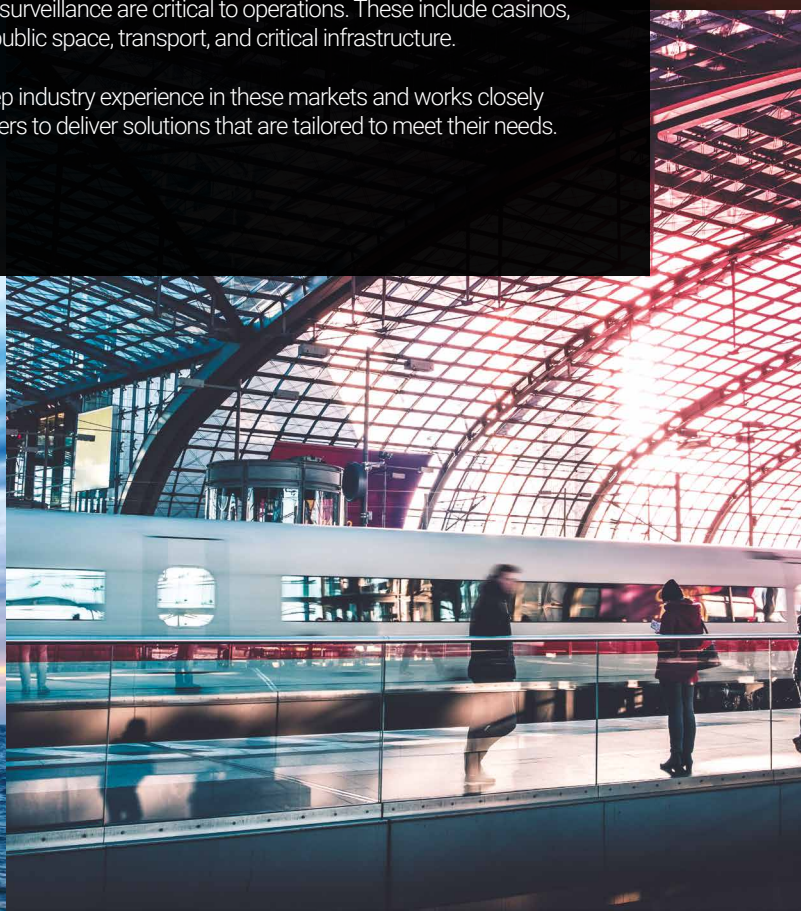


Protecting what matters, where it matters most

Synectics is a leader in advanced security and surveillance systems that help protect people, property, communities, and assets around the world.

Our expertise is in providing solutions for specific markets where security and surveillance are critical to operations. These include casinos, oil and gas, public space, transport, and critical infrastructure.

We have deep industry experience in these markets and works closely with customers to deliver solutions that are tailored to meet their needs.



Specifications subject to change. E & OE.

Literature Reference: AI-PS/0124 Iss1

SYNECTICS

synecticsglobal.com