Technology Innovation in Security

Industry Insight 2023 / 2024

First Response Group
Total Security, Risk & Facilities Management

Contents

Introduction

Security technologies play a crucial role in protecting people and assets, as well as fighting crime and administering justice. And they are evolving rapidly, particularly in response to the digital revolution. The UK security industry is undergoing an unprecedented transformation. From enhancing surveillance and access controls and fortifying digital defences to biometric authentication, technology is revolutionising security practices across the board.

The surge from traditional to modern surveillance isn't simply about technological advancement. It's about harnessing information, both digital and visual, to generate actionable insights that can prevent crime and enhance public safety.

Alongside some of these advancements, questions arise about their ethical use, such as facial recognition and biometrics. The evolution of these technologies and their application in global security underpin a delicate balance between increasing surveillance effectiveness and preserving privacy rights. As these considerations are rationalised, and eventually woven into security policy and practice, a new landscape is opening up for the c-suite of organisations deploying these systems, both for security companies and the client community.

This paper takes a look at how technology is reshaping the industry, highlighting the crucial role being played by different technologies, but also underlining the importance of personnel and how technology is complementing rather than replacing tried and tested methodology.

As technology continues to evolve, the security industry is poised to embrace even more sophisticated solutions, ultimately creating a safer and more secure world for individuals and organisations.

Surveillance and Monitoring

Digital Revolution

Traditional surveillance systems are gradually being replaced by technology and automation, releasing human capital for other tasks whilst saving on costs.

Traditional	Technological
Physical patrolling	Digital video surveillance
Manual database checks	Biometrics / RFID
Identity document checks	Facial recognition / ANPR

CCTV (Closed-Circuit Television) is deployed widely throughout the UK and has had a profound impact on crime prevention and detection and is never out of the news for long.

A report published by the British Security Industry Association (BSIA) estimates that the total number of CCTV cameras in the UK stands at somewhere between 4 million and 6 million. That's around 7.5 cameras for every 100 people in the country – the third-highest total on the planet behind the US and China.

Advances in Technology

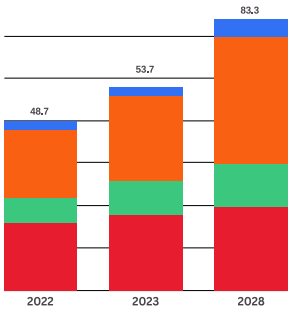
CCTV technology has undergone significant advancements in recent years, transforming the landscape of surveillance systems. From traditional analogue cameras to modern IP-based solutions, CCTV technology has become more sophisticated, intelligent, and versatile, and a number of trends have emerged which are reshaping how we conduct surveillance.

HD Video: A key development in CCTV technology has been the move towards high-definition (HD) and ultra-high-definition (UHD) video. HD cameras deliver considerably sharper and more intricate detail, enhancing the ability for precise identification and recognition. Ultra HD cameras, boasting resolutions of 4K and even 8K, provide unmatched levels of detail, making them particularly valuable for forensic investigations and critical operation.

IP Enabled Cameras and Network Video Recorders (NVRs): IP-based cameras and NVRs are gaining widespread popularity due to their scalable and flexible nature. These devices make use of existing network

Video Surveillance Trends

Global Forecast to 2028 (USD BN)



The global video surveillance market is expected to be worth by 2028

CAGR OF
9.2%

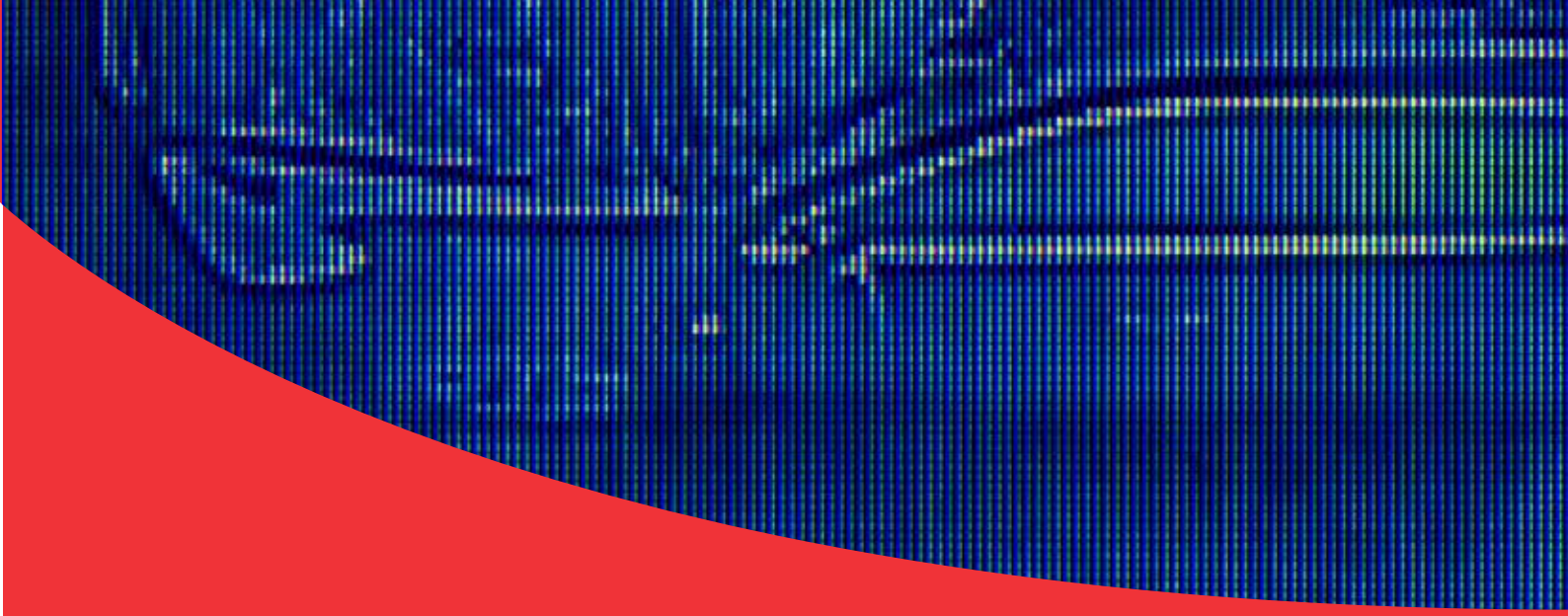
Infrastructure for video transmission and storage, allowing full integration with other systems. IP cameras also offer advanced benefits, such as remote access, intelligent analytics, and support for Power over Ethernet (PoE).

Cloud-Based Video Management: The landscape of video storage and management has undergone significant transformation with the advent of cloud-based solutions. Migrating from exclusive reliance on on-premises servers, CCTV systems can now harness the power of the cloud for secure storage, remote accessibility, and scalable architecture.

Cloud-based platforms further facilitate smooth integration with other applications, creating a comprehensive and interconnected surveillance ecosystem.

Artificial Intelligence (AI) & Video Analytics: AI-powered video analytics have revolutionised CCTV surveillance. Advanced algorithms can analyse video feeds in real-time, detecting specific objects, events, or behaviours. AI-driven analytics enable automatic alerts for suspicious activities, improved object tracking, and smart search capabilities, enhancing overall security and reducing manual monitoring efforts.

Deep Learning & Neural Networks: Image and video processing has been revolutionised through the application of deep learning techniques and neural networks. The training of models on extensive datasets enables CCTV systems to execute intricate tasks like object recognition, anomaly detection, and behaviour analysis. The iterative nature of machine learning is the continuous enrichment of knowledge, results and accuracy.



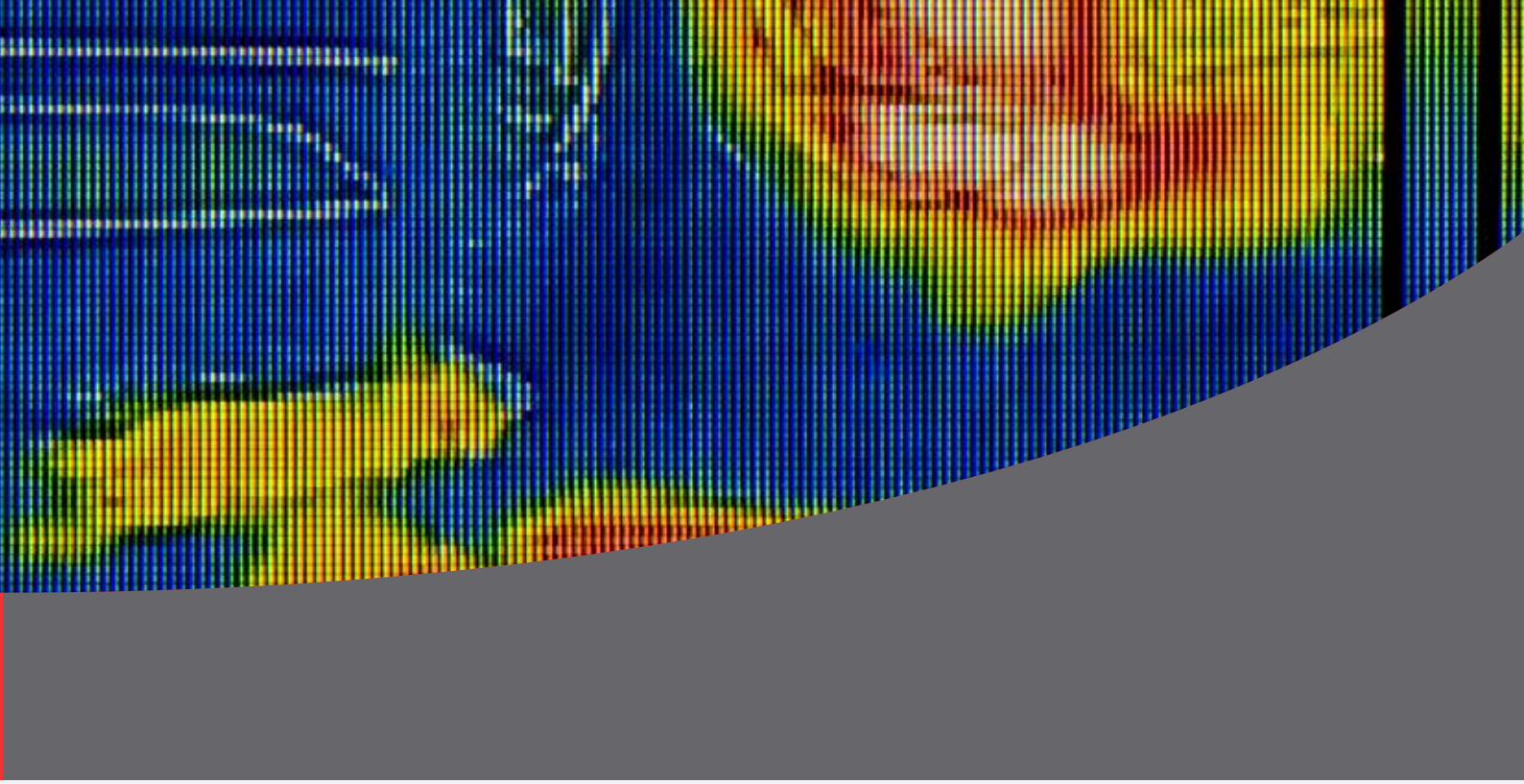
Thermal Imaging Cameras: By converting heat into visible images, thermal cameras provide an additional layer of security in various applications. These cameras excel in challenging lighting conditions and are effective in detecting intruders, even in pitch darkness.

360-Degree and Panoramic Cameras: 360-degree and panoramic surveillance cameras provide extensive coverage within a singular device. These advanced systems capture a broad field of vision, overcoming blind spots and minimising the need for multiple cameras. Many panoramic cameras are now equipped with de-warping software, enabling security officers to examine specific areas with much greater scrutiny.

Edge Computing & Edge Analytics: Edge computing brings processing power closer to the source of data, reducing latency and bandwidth requirements. In CCTV systems, edge analytics allow real-time analysis and decision-making at the camera level. This approach reduces the load on the network and central servers while enabling rapid response to security events.

Mobile Surveillance: Mobile app-based surveillance solutions empower users to monitor CCTV systems on-the-go. With the ascendance of smartphones and tablets, security personnel can access live video feeds, control cameras, and receive alerts from anywhere, and on the move, adding convenience and flexibility whilst boosting situational awareness.

IoT Integration: CCTV systems can now be integrated with Internet of Things (IoT) devices for enriched functionality, communicating with sensors, access control systems, alarms, and other IoT devices, enabling intelligent automation and correlation of data. This effectively creates a unified security ecosystem with a comprehensive view of its environment.



Video Content Analysis (VCA): VCA is the automated analysis of video footage for extracting meaningful information. VCA algorithms can detect various events, such as abandoned objects, crowd management, traffic congestion, and more. These insights help operators make informed decisions and respond effectively to incidents.

Privacy-Enhancing Technologies: Privacy concerns have gained increasing attention with the increased deployment of surveillance technology.

To combat this, privacy-enhancing technologies are emerging, with techniques such as anonymisation, video-masking, and encryption without losing any of its surveillance functionality or detail.

Enhanced Cyber Security Measures: With the increasing integration of CCTV systems, the importance of cybersecurity cannot be overstated. It is imperative to implement resilient security protocols, encryption, two-factor authentication, and consistently update software to fortify surveillance systems against potential cyber threats.

Meanwhile, integration of Al-based cyber security solutions are further enhancing systems' resilience.

Integration with Other Security Systems: The fusion of CCTV systems with other security components like access control, intrusion detection, and alarm systems is on the rise.

Such integration allows for more efficient incident response, streamlined workflows, and improved overall security management.

Impact of Surveillance Technology

Security officers often encounter situations that require documentation and evidence gathering. Surveillance technology provides a valuable resource in this regard. High-definition cameras capture detailed footage, which can serve as crucial evidence in investigations, legal proceedings, or insurance claims. This not only aids in identifying perpetrators but also protects security officers from false accusations, enhancing their professional credibility.

Embracing surveillance and monitoring technology can lead to increased efficiency and cost savings for security operations. Automated systems can perform routine tasks, such as patrolling and monitoring, with consistency and accuracy, allowing security officers to focus on more critical aspects of their job.

In today's interconnected world, security officers can remotely access surveillance feeds and control security systems through smartphones, tablets, or computers.

This remote access capability allows officers to maintain vigilance even when off-site, providing a robust layer of security 24/7.

Additionally, remote access enables security companies to grant or restrict entry to specific areas, enhancing access control measures.

Facial recognition surveillance is growing at pace. As recently as October 2023, Essex Police, in their first trial of live facial recognition (LFR) technology, reported three arrests, including one for rape, hoping to use the technology to apprehend serious offenders. Despite the positive outcome, privacy advocates such as *Big Brother Watch* criticised LFR as 'dangerously authoritarian' and a threat to privacy and freedoms.

Likewise, in the same month, The Metropolitan Police used live facial recognition technology for the first time at a Premier League football match, resulting in three arrests, including one for a breach of a football banning order.

The allegedly 'controversial' technology, criticised as Orwellian by privacy campaigners, was defended by Minister of State for Crime,

Policing & Fire, Chris Philp, who endorsed its ability to help police to identify serious criminals, freeing up police resources.

Meanwhile, video surveillance, especially facial recognition technology, has faced criticism due to its potential impact on privacy and security.

Notwithstanding some concerns, the deployment of facial recognition technology is revolutionising how CCTV video surveillance can be used in security and policing. In Europe, the European Union (EU) is in the process of constructing an international facial recognition system.

The concerns surrounding surveillance primarily stem from how the technology is programmed and utilised, rather than inherent flaws in the technology itself.

These problems can potentially be addressed through increased transparency and industry-accepted protocols in its implementation.

Notwithstanding, it remains crucial to acknowledge that facial recognition is not the exclusive solution for surveillance technology implementation. It has to be part of a symphony of other technologies and procedures to improve security and protect lives on the one hand, and preserve individual rights and privacy on the other.

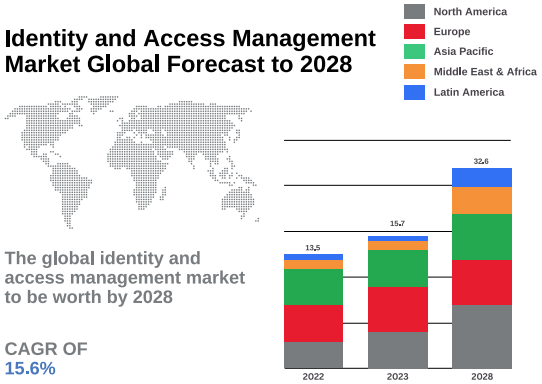
Access Control and Identity Verification

Evolution of Access Control Technology

Access control technologies have come a long way, progressing from simple physical methods to sophisticated digital systems. Increasingly, we talk about ‘intelligent buildings’, although these still require physical and human intervention and oversight. In essence, there are five main types of access control system:

1. Discretionary Access Control: Here, a system administrator decides who has the authority to enter, a technology commonly found in domestic systems.

2. Rule-based Access Control: In this system, administrators establish rules to determine access rights, such as out of hours access or pattern-based conditions.



3. Mandatory Access Control (MAC): Most commonly applied in government and high-security settings, a MAC system grants access to authorised individuals based on vetting criteria.

4. Role-based Access Control: Entry is granted based on a user’s roles within an organisation, such as board directors or finance. This system is frequently employed in business settings.

5. Attribute-based Access Control: This operating system combines rules and roles to determine entry, blending aspects of both role-based and rule-based access control.

Communication & Control

RFID. Radio Frequency Identification (RFID) is a type of passive wireless technology that allows for tracking or matching of an item or individual. As well as in security first and foremost, it is also used in several commercial and industrial applications, from tracking items along a supply chain to keeping track of hotel property.

Near-field Communication (NFC). NFC mirrors RFID technology but is applied at close ranges, less than 4cm. As a token is brought close to the receptor, both devices communicate electromagnetically.

Most NFC systems use smartphones instead of key cards or fobs.

Bluetooth. Bluetooth Low Energy (BLE) is the latest iteration of Bluetooth with a range of up to 800 feet, comprising a reader and pre-paired device, often again a smartphone.

Biometrics. Biometric access control determines access based on an individual's unique physical attributes, matching the person's characteristics - such as face, fingerprint, iris, palm, and hand geometry - to a database of authorised personnel.

Identity Verification Technology

Access control technology enables security officers to manage entry and exit points effectively. By employing keycards, biometric scanners, or PIN codes, security companies can regulate who enters a secured area. This meticulous control minimises the risk of unauthorised personnel infiltrating sensitive zones. Modern access control systems offer real-time monitoring capabilities, providing security officers with instant visibility into who is entering and leaving a facility or restricted area.

Innovations in identity verification are proving a robust means of automating authentication and

saving time whilst reducing the risk of human error. Monitoring movement through areas with these systems in place enables the maintenance of comprehensive logs, which security officers can review to track and analyse patterns, irregularities, and investigate security incidents. These logs serve as invaluable tools for forensic analysis and accountability, helping security companies to ensure compliance and also to improve security protocols.

Meanwhile, alarm systems can be seamlessly integrated, alerting security officers in the event of unauthorised access or suspicious activity. By automating access control and identity verification processes, security officers can focus their attention on other critical security tasks. The accountability and transparency offered by these technologies boosts trust and confidence, both for owner-occupiers, its users and its security companies.

Biometrics

Categorisation of Biometrics

Although, we touched on biometrics in our earlier section on access control, such is its importance to future security measures that it deserves particular attention and analysis.

Biometric controls are classified based on physiological characteristics, including the following main applications:

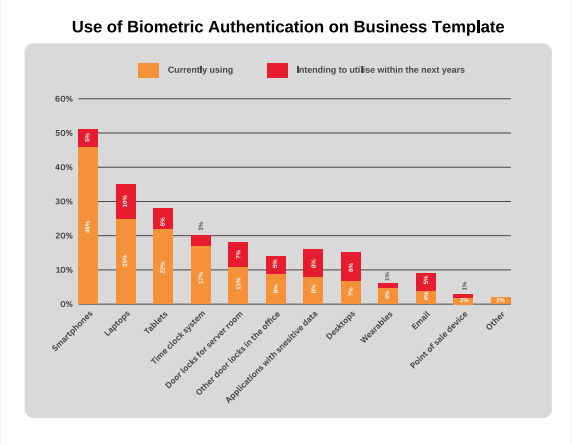
- **Facial Recognition Terminal** (camera)
- **Fingerprint Recognition Terminal** (scanner)
- **Iris Recognition** (scanner)
- **Palm Vein Recognition** (with infrared)
- **Hand Geometry Recognition** (geometry scanner)
- **Multi-Factor Authentication Terminal** (with multi-sensor types, such as RFID, barcode scanner, or multi-biometrics scanners.)

The two types of biometric access control, contact and contactless (or touch and touchless), suit different environments, with contactless systems in the main reducing a degree of congestion where large bodies of people need to be processed.

Contact biometric access controls require users to physically touch something to gain access to a secured area, and this might include a fingerprint sensor, for example. Conversely, contactless biometric access control systems allow the user to enter a building by simply scanning their faces, or carrying a contactless RFID card, or NFC mobile device.

During the COVID pandemic, contactless systems gained significant popularity for obvious reasons, and are widely deployed now in public places such as banks, and in some parts of the world, even grocery stores and general businesses.

Some of these systems have body temperature sensors and mask detection technology built in to circumvent other personal protection measures and increase user convenience.



Industry Boon

For the security industry in particular, biometric technology holds immense promise and has gained widespread popularity due to its ease of use, enhanced security features, and far-reaching benefits. First and foremost, they outperform traditional access control authentication methods such as PIN codes and passwords in terms of accuracy and security.

The convenience factor is clearly a boon, whilst speed and cost-savings feature highly for the building's owners or occupiers. Adopting biometric access control system can also reduce the number of false alarms, requiring less human intervention or monitoring, enabling the deployment of security officers to higher risk locations or for more decision-based security work.

Equally, for multi-entry complexes, a biometric access control system allows the deployment of a single guard to monitor all doors through an integrated central platform.

These technologies are not only highly accurate but fast and non-intrusive. Voice recognition technology analyses an individual›s vocal patterns and characteristics for identity verification. Security officers can use voice recognition systems for telephone-based access control or to confirm identities during verbal interactions, adding an extra layer of security.

Increasingly, the fusion of multiple biometric modalities provides an even more robust security framework, minimising the chances of false positives and negatives. Meanwhile, scans can be cross-referenced with criminal databases, aiding in the prevention of access to thieves and even terrorists, particularly in public spaces with large crowds, such as sports and entertainment venues. Biometrics is here to stay and is only getting to get better.

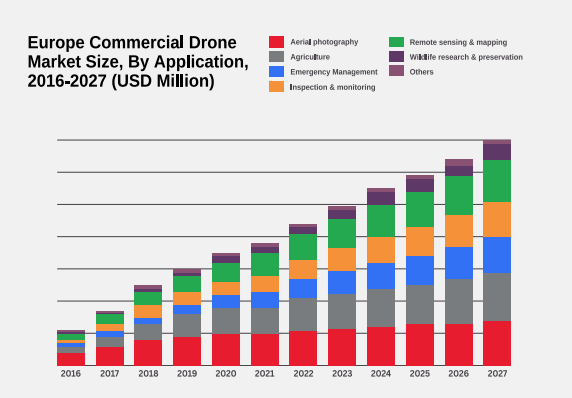
UAVs & Drones

Open and Complex Real Estate

Unmanned Aerial Vehicles (UAVs), most commonly known as drones, have emerged as powerful tools in enhancing security measures, especially for large, open or complex real estate.

With their ability to navigate diverse terrains, collect real-time data, and operate in challenging environments, drones offer a unique and effective solution to bolster security efforts, increasingly employed by first responders as well as by the commercial security industry.

The potential economic impact of drones in the United Kingdom is substantial, with PWC estimating a value of £45 billion to the economy by 2030, and a significant portion of this value, £7 billion, being attributed to the security sector.



Equipped with high-resolution cameras and advanced sensors, drones can provide a birds-eye view of large areas, making them invaluable for monitoring critical infrastructure and public events.

This capability enhances situational awareness, enabling security personnel to detect and respond to potential threats promptly.

One of the pioneering applications of security drones lies in their deployment as a drone in a box. These autonomous units are strategically positioned at sites, following pre-programmed flight paths set by security companies. Equipped with sensor technology, including thermal imaging, these drones identify movement even in the most challenging light conditions.

A New Era in Surveillance

The deployment of security drones presents a paradigm shift in risk management. Drones offer enhanced risk analysis capabilities, enabling security personnel to address potential threats before they escalate and to provide crucial early warning and enhanced reaction time.

In the realm of intelligence gathering, drones prove invaluable, particularly in areas like criminal damage and aggravated trespass. Drones can navigate challenging terrains, gather evidence, and transmit data to control rooms for analysis. This capability significantly aids the police and security personnel in their efforts to combat crime, ensuring a more comprehensive and technologically advanced approach to surveillance and evidence collection.

Another notable aspect of security drone systems is the transparency they provide to clients who can have full access to the data collected. This transparency not only enhances the effectiveness of security measures but also promotes accountability and trust, ensuring moreover that clients are well-informed about potential risks and vulnerabilities.

As technology, regulations, and public perception continue to evolve, the widespread adoption of commercial drone capabilities in the UK is not only imminent but increasingly integral to the future of security.

While drones offer immense potential for improving security, their deployment raises concerns related to privacy, data security, and potential misuse. Striking a balance between harnessing the benefits of drone technology and addressing these ethical considerations is crucial. Establishing clear regulations, guidelines, and ethical frameworks is essential to ensure responsible and lawful use of drones in security applications.

The Future of Technology in Security

It is beyond doubt that scientific research and the advancement of technology will continue to transform the way we live our lives and the threats we face, as well as provide new opportunities to address these threats and those of the future.

Underpinning this are some important trends, including:

- The increasing pace of innovation
- Exponential growth in data and communications technologies
- More complexity as different technologies converge or enable each other
- Increasing automation – including AI Biometric technology and tracking systems.

Biometric ID Processes: A Leap Beyond Traditional Identification

One of the most promising developments in security technology is the use of biometric identification processes. Cameras and sensors are now capable of capturing intricate details of an individual›s face, palm, and even weight.

This advancement could possibly usher in a new era of seamless travel without the need for physical identification documents, marking a significant departure from traditional security measures. This new way of verifying identity and allowing access to areas is also going to revolutionise the security industry. By utilising biometric data, security systems can verify the identity of individuals with a high degree of accuracy, enhancing both convenience and security.

The integration of non-invasive automation in identification processes is another pivotal aspect of the future of security technology. Beyond traditional biometrics, such as fingerprints and facial recognition, advancements in technology now allow for the analysis of body biometrics. The way individuals walk, their weight, clothing choices, and even unique features like moles and tattoos can be automatically processed for identification purposes. This holistic approach to biometrics enhances the precision and reliability of identification systems.

Doubtless this will be outcry from some corners around civil rights, and what personal identification data might be used for, but in a controlled environment, such as passport control for instance and places of ultra high security, this can be managed and maintained for improved access, speed and safety.

Identity Super Search Engine for Law Enforcement

A significant stride in forensic identification is the possible future development of an identity super search engine, connecting various databases and law enforcement agencies. This centralised system may allow for the rapid and efficient capture of images and faces, transcending jurisdictional boundaries. The EU is currently working on a cross border database of images. Unlike traditional databases where police images are merely stored, this super search engine would collate data for comprehensive search purposes. The introduction of image search capabilities represents a quantum leap in the speed and effectiveness of law enforcement efforts.

The architecture of biometric databases is evolving to accommodate the growing volume and complexity of data. Unlike conventional databases, where information is stored in a linear fashion, new biometric databases are designed to facilitate efficient searches. These databases not only store data but also employ advanced algorithms to categorise and link biometric information. This structural enhancement ensures that identification processes are not only accurate but also swift, crucial in time-sensitive security scenarios. These areas are all in development and have the potential to be game changers for security.

Securing Biometric Visual Data

With the increasing reliance on biometric data, ensuring its security is paramount. Robust database security measures are being implemented to safeguard biometric visual data from unauthorised access and potential misuse.

Encryption protocols, multi-factor authentication, and secure transmission channels are becoming standard practices in the management of biometric information. These measures not only protect privacy rights but fortify the overall integrity of the security systems.

Trends Towards Automation and Non-Invasive Monitoring

The overarching trend in the future of security technology is moving towards greater automation and non-invasive monitoring. As technology becomes more sophisticated, the need for physical identification documents diminishes, and security systems become more intuitive and streamlined. Non-invasive biometric monitoring allows for enhanced security without compromising individual privacy, creating a delicate balance between effective surveillance and civil liberties.

Conclusion

The realms of surveillance and monitoring, access control and identity verification, cybersecurity, biometrics, and predictive analysis have all significantly evolved and converged to redefine the role of security officers in safeguarding our modern world.

These technological advancements have ushered in a new era of security, one that is proactive, efficient, and highly effective.

In this ever-changing security landscape, security officers are at the forefront of integrating and harnessing the power of these advanced technologies.

Their role has evolved into one that not only responds to security incidents but also actively prevents them.

As technology continues to advance, the partnership between security officers and cutting-edge security technologies will undoubtedly lead to safer and more secure environments.

Deploying Technology in the Field: FRG's Experience

In the rapidly evolving landscape of security challenges, technological innovation has become a driver for more effective and comprehensive solutions.

First Response Group (FRG), accredited with NSI NACOSS Gold, the mark of the security elite who meet the industry's highest technical standards and maintain a commitment to continual improvement, stands out for its strategic use of cutting-edge technology to address security requirements across various sectors. These include:

Advanced Surveillance Systems

At the core of FRG's technological arsenal lies advanced surveillance systems. High-resolution Closed-Circuit Television (CCTV) cameras, equipped with sophisticated analytics, provide real-time monitoring and threat detection capabilities. These systems go beyond traditional surveillance, offering intelligent features such as facial recognition, license plate recognition, and behaviour analytics. FRG's CCTV solutions play a crucial role in deterring criminal activities and facilitating rapid response to security incidents.

Intrusion Detection & Access Control

FRG employs state-of-the-art intrusion detection systems that utilise a combination of sensors, motion detectors, and advanced algorithms. These systems are designed to detect unauthorised access or suspicious activities promptly. Coupled with robust access control solutions, FRG ensures that only authorised individuals have entry to secured areas. Biometric access, smart card systems, and advanced authentication protocols contribute to a layered and secure access management strategy.

Wireless Technology and IoT Integration

The advent of wireless technology and the Internet of Things (IoT) has transformed the security landscape. FRG utilises wireless communication protocols to create flexible and scalable security infrastructures. This facilitates rapid deployment of security solutions without the need for extensive cabling.

Additionally, IoT integration enables seamless communication between various

security components, enhancing the overall effectiveness of the security ecosystem.

Remote Monitoring and Management

FRG understands the importance of real-time situational awareness. Remote monitoring and management tools empower security personnel to monitor and manage security systems from centralised locations. This not only improves response times but also allows for proactive decision-making based on live data feeds. Whether it›s a retail store, an industrial facility, or a critical infrastructure site, FRG's remote management capabilities provide a comprehensive view of the security landscape.

Integration of Artificial Intelligence (AI)

Artificial Intelligence has become a game-changer in the security domain, and FRG is quick to harness its potential. AI algorithms analyse vast amounts of data from various sources, enabling predictive analysis and anomaly detection. FRG's security systems equipped with AI can learn and adapt, identifying patterns indicative of potential threats and minimising false alarms. This proactive approach significantly enhances the efficiency of security operations.

Cybersecurity Measures

Recognising the increasing sophistication of cyber threats, FRG incorporates robust cybersecurity measures into it's security solutions. From secure network architectures to encryption protocols, FRG ensures the integrity and confidentiality of sensitive security data. This comprehensive approach safeguards against cyber-attacks that could compromise the effectiveness of security systems.

First Response Group

Total Security, Risk & Facilities Management