



AI at the edge

transforming spaces into smart infrastructures



introduction

Smart spaces were once seen as a futuristic concept, blending cutting-edge technology with human interactions. Today we see them as an integral part of life, whether in office spaces, retail stores, factories, or increasingly entire cities – these interactive environments have entered the mainstream. Such spaces leverage Internet of Things (IoT) sensors, connectivity, and AI-powered analytics into intelligent solutions which adapt to the operational goals of the organisation, the needs of the institution, or the security and safety of occupants within an area.

Businesses are increasingly investing in smart building and smart space initiatives to boost efficiency and user experience. The evidence speaks for itself. For example, a [2023 survey](#) found 78% of facility leaders that deployed smart building technologies saw improved energy efficiency and cost savings as a result.

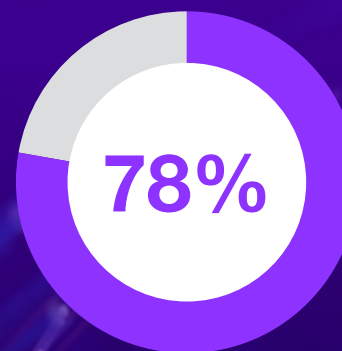
Such figures highlight that smart spaces deliver real ROI for those willing to invest, and it's becoming a corporate strategy that's hard to ignore. This is true to such an extent that the global smart space market was valued around \$13.45 billion in 2023 and is projected to reach [\\$37.23 billion by 2032](#).

The use of Edge AI and computer vision solutions which brings real-time intelligence outside of the data centre and into the field environment, is crucial to this success. It is estimated that there are [over one billion cameras deployed](#) worldwide, generating a massive amount of video data. Without analytics, much of this data's value is lost.

The ability to deploy machine learning models locally on edge devices rather than relying solely on cloud data centres dramatically cuts down latency and bandwidth use, as data can be processed on-site in milliseconds, enabling instantaneous responses. AI-powered computing can unlock insights from video in real time, allowing retailers, companies, and cities to improve efficiency and safety.

In this report, we look at how Edge AI is helping to augment smart spaces, responding to events as they happen, as well as the barriers organisations in the public and private sectors need to address to deliver real-world returns not only on investment but also on the way we go about our lives.

businesses are increasingly investing in smart building and smart space initiatives to boost efficiency and user experience



of facility leaders have seen **improved energy efficiency and cost savings** due to deploying smart building technologies.

operational efficiency within smart spaces

SMART SPACE TECHNOLOGY IS NOTHING NEW.

What is, however, is how seamlessly the technology can be integrated. Smart spaces can be created in their entirety from new, or they can leverage existing systems and rely on the same fundamental building blocks shared across many operational technologies.

They are an ecosystem of connected devices that sense and monitor the environment around them, communicate with each other, and act on data-driven insights. By continuously collecting data, whether in the form of retail foot traffic, video of traffic flow at a road junction, or even temperature fluctuations within an office space, information is sent to a local gateway or edge computer. Edge AI processes this data on-site using AI models and the smart space uses such insights to automate actions or inform decisions.

The benefits of Edge AI

Edge AI essentially makes sense of all the sensor inputs by executing responses in real time without the need for constant cloud connectivity. This local processing capability is especially important for environments that require real-time operation or are bandwidth constrained.

When rapid response times are essential, or network reliability is a concern, edge computing provides resilience and immediate operational feedback. For example, security applications can send alerts directly from the edge without routing through central systems.

By handling data at the edge, latency is minimised, and the system can respond in fractions of a second, while also significantly reducing the volume of data that needs to be sent to the cloud. This not only speeds up the automation of processes but also enhances privacy as raw video or personal data can be analysed and filtered locally, with only necessary insights sent upstream. This informed governance to determine what information can be collected and how it will be used, is key to the success of any smart space implementations.

The final critical component of any smart space infrastructure is business intelligence, or the extracting of meaningful insights that demonstrate ROI for retailers, governments, and other organisations choosing to deploy these systems. For retailers, this might involve advanced customer behaviour analytics that go far beyond traditional metrics. By integrating data from multiple sources, such as foot traffic sensors, purchase histories, dwell times, and interaction patterns, organisations can develop a highly nuanced understanding of customer journeys.

Equally, local governments can leverage similar insights for urban planning, public service optimisation, and resource allocation.

Overcoming barriers for change

Despite the clear advantages of Edge AI and computer vision for smart spaces, businesses and organisations face several significant challenges when implementing these solutions. For many, simply choosing the right edge device for an AI application presents a crucial challenge. Edge hardware must balance three competing requirements: powerful computation, low power consumption, and small form factor to fit next to cameras or in junction boxes. This creates a trade-off between model size, capability and hardware constraints, as larger models with more features and capabilities often cannot run on compact edge devices.

Due to the complexity and variety of options, creating smart spaces typically involves multiple vendors and technologies, from CCTV cameras and networking infrastructure to servers. Building this complete pipeline requires coordination across various systems, making integration challenging. Finding the right system integrators and partners who can effectively combine these components becomes essential.

Smart space implementations, particularly for large public or private infrastructure, require significant upfront investment. Projects typically demand hundreds, if not thousands, of Edge devices running multiple AI algorithms, creating substantial hardware costs and research and development expenses. This initial outlay can deter adoption despite long-term benefits.

Equally, many organisations, particularly public institutions, lack the internal expertise to evaluate and manage these technologies with confidence. This creates uncertainty about total cost of ownership and return on investment. The technical teams may not fully grasp the business case, while those who understand the business advantages may not comprehend the technical requirements.

Despite these barriers, the operational advantages of Edge AI solutions are compelling. For retail, implementing AI-powered loss prevention can significantly reduce theft while respecting privacy by processing data locally. For cities, smart traffic management can improve sustainability through real-time adjustments, reducing pollution and citizen complaints.

Once organisations overcome these initial hurdles, they often find that the Edge AI solutions deliver clear benefits with relatively modest infrastructure requirements compared to traditional approaches.

In essence, Edge AI gives smart space infrastructures the ability to sense, see, hear, think, and act locally, making them far more responsive and efficient than traditional connected systems.

► in summary:



EDGE AI LEVERAGES EXISTING CAMERA INFRASTRUCTURE BY SIMPLY ADDING INTELLIGENCE



IT PROCESSES DATA LOCALLY, REDUCING BANDWIDTH DEMANDS



IT ENABLES IMMEDIATE RESPONSE WHEN NEEDED, NO LATENCY



IT FUNCTIONS EVEN DURING NETWORK DISRUPTIONS, INCREASED RESILIENCE



IT ALLOWS FOR DATA ANONYMISATION BEFORE TRANSMISSION, RESPECTING PRIVACY

02

data security and privacy within smart spaces

In the world of edge computing, data security is far more complex than most people realise. While Edge AI offers incredible advantages such as processing sensitive information locally and eliminating the need to transmit raw information over the internet, it simultaneously introduces unprecedented security challenges that traditional data centres have never faced.

Unlike secure data centres with robust protection, these edge devices are not just digital endpoints, but physical objects potentially susceptible to unauthorised access and sophisticated cyber-attacks. As such, data protection goes beyond preventing external hacking. It involves safeguarding against physical threats like rain damage, moisture infiltration, or someone physically tampering with the device.

Smart space infrastructures rely on a network of connected devices often deployed in public or accessible areas, such as on a street corner, inside a trade show, or mounted on a smart pole. By the very nature of the devices, they are designed to be small and serve a specific purpose, therefore have limited computational resources compared to centralised systems. Traditional security measures, such as perimeter security to control physical access are not applicable to in field deployments. As a result, companies must develop entirely new strategies for protecting distributed technological infrastructures.

Edge AI devices continuously stream data, making secure transmission

critical. This requires advanced certification exchanges, encryption protocols, and secure device enrolment methods.

One recommended approach replaces traditional passwords with hardware-embedded digital certificates. Instead of manually changing passwords, devices now have unique, unforgeable identities built directly into their hardware. This approach prevents “man-in-the-middle” attacks and provides a more robust security mechanism.

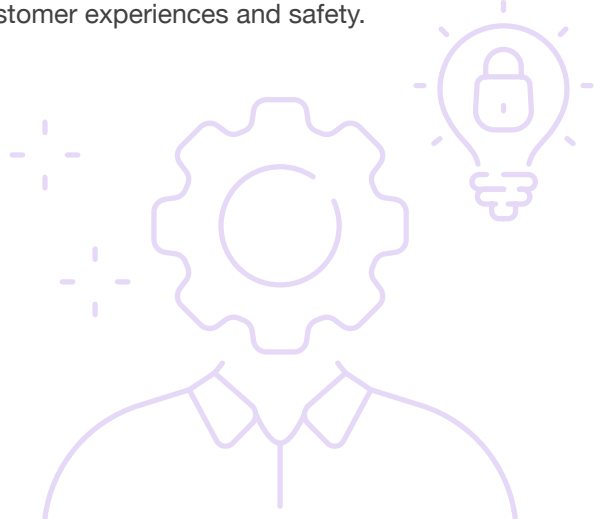


Edge AI and people counting

One of the key tools organisations and businesses can use smart technologies for is people counting and flow analysis, the use of which has transformed simple headcounts into powerful strategic insights. Using overhead cameras and sophisticated AI algorithms, sometimes with the aid of precise people counting appliances at the entry/exit gates, these systems provide real-time, accurate tracking of individuals entering, moving through, and occupying spaces. The technology captures nuanced data about foot traffic, occupancy patterns, Point of Interests and human movement.

This is perhaps no more evident than in retail spaces, where people counting can enable tracking of visitor numbers and conversion rates so that stores can optimise staffing to match peak trading hours, better understand customer behaviour to maximise store layout performance and essentially improve overall sales strategies. Facility managers can leverage people counting to dynamically adjust building systems based on real-time occupancy, optimise space utilisation, or simply to implement energy-efficient climate controls for better efficiencies.

Whether for corporations or organisations, people counting delivers the ability to convert physical presence into informed strategic decision-making and actionable data to improve conversion rates, optimise labour costs, and enhance customer experiences and safety.



Privacy within smart spaces

Security of Edge AI devices goes beyond protecting the data it contains from outside attacks. Ensuring that devices are aligned with privacy regulations such as GDPR (General Data Protection Regulation) in Europe and similar regulations around the world is vital. Such regulations are designed to protect the privacy and personal data of individuals and apply to any organisation that processes data related to citizens, regardless of where the business is based.

Under the terms of the regulations to help comply with regulations, Edge AI devices must automatically anonymise sensitive information before transmission. This means transforming personal data, whether that is facial recognition, measurements or outlines, into unrecognisable formats. In this way, even if a bad actor gains unauthorised access to the data, they cannot reconstruct personal information.

Edge AI can help organisations comply with GDPR as processing happens locally, which means sensitive personal data may not need to leave the device, reducing the risk of exposure. This local processing aligns with GDPR's goal of minimising unnecessary data sharing.

Overall, organisations need to ensure that personal data is processed securely, user consent when necessary is managed, and that privacy by design is integrated into AI systems at the edge. Despite the complexities, the combination of Edge AI and GDPR can provide opportunities to enhance data privacy while enabling innovative AI-driven solutions.

As smart space infrastructures continue to evolve, the boundary between physical and digital security will become increasingly blurred. Organisations that understand and embrace this complexity will have a competitive edge over their rivals, transforming how we think about data protection in an interconnected world.

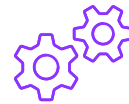
► In summary:



IMPLEMENT SSL CERTIFICATION EXCHANGES



ENCRYPT DATA BEFORE TRANSMISSION



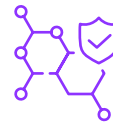
IMPLEMENT A PROPER DEVICE ENROLMENT AND PROVISIONING



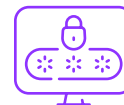
MAKE SURE TO HAVE DEVICE MANAGEMENT STRATEGY OVER THE LIFE CYCLE OF THE DEVICE



USE SECURE COMMUNICATION PROTOCOLS



ALLOW DEVICES TO INITIATE CONNECTIONS RATHER THAN ACCEPTING EXTERNAL CONNECTIONS



ENSURE NO PERSONALLY IDENTIFIABLE INFORMATION IS TRANSMITTED

addressing cybersecurity risks with ISA/IEC 62443-certified solutions

Developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), the ISA/IEC 62443 standard provides a framework for securing industrial automation and control systems (IACS) to help organisations secure their industrial environments from cyberattacks.

Attacks come in a variety of forms, whether from unauthorised access to industrial control systems, vulnerabilities in the system, such as in the communication channels between components, to ensuring that the safety and reliability of industrial operations are not compromised due to insufficient security updates and patch management.

The standard takes a comprehensive approach by addressing risks at multiple levels:



COMPONENT LEVEL
(INDIVIDUAL DEVICES)



SYSTEM LEVEL
(INTERCONNECTED EQUIPMENT)



ORGANISATIONAL LEVEL
(POLICIES AND PROCESSES)

Eurotech actively adheres to the ISA/IEC 62443 standards, ensuring all products meet the highest level of industrial cybersecurity. Products are designed and built using a 'security by design' approach that integrates robust cybersecurity features into products to meet the stringent requirements for IACS, providing a secure foundation for edge computing regardless of environment.

Certified and compliant products implement security controls like secure-by-design development practices, robust authentication, encrypted communications, and secure update mechanisms.



#8

integration and future proofing of smart spaces

Smart space infrastructures are complex by their nature. A typical solution involves CCTV cameras capturing raw video, attached to Edge AI devices processing and analysing the feed. It then needs to connect to a central server to share and manage information. For organisations looking to implement smart space infrastructures in large public or private infrastructures, this means deploying hundreds, if not thousands, of edge devices running multiple AI algorithms.

The barriers to entry are significant. Companies must invest substantial resources in finding the right partners, understanding complex networking requirements, and creating a cohesive technological ecosystem. It's not just about purchasing devices, it is also about building an intelligent, interconnected infrastructure that can scale and adapt to evolving technological needs.

System integrators are crucial in bridging the gaps between different technologies, ensuring that devices from various manufacturers can communicate seamlessly and effectively with each other. No single company can realistically provide every component of such a sophisticated system, but each plays a critical role in the overall infrastructure. To implement smart spaces, therefore, it's necessary to address the complex challenge of integrating technologies from multiple vendors.

Using 'open standards and protocols' is key, as it ensures interoperability and easier integration between devices and software while maintaining security. This collaborative approach benefits the entire industry ecosystem. By establishing common frameworks, developers and companies can build upon existing technologies without being locked into proprietary systems.

This approach accelerates smart space implementation by reducing the barriers to entry for new public or private organisations by creating a more collaborative, innovative, and interconnected system that benefits developers, businesses, and end-users alike.

Solutions to smart space complexities

When working with multiple vendors a centralised management platform is essential, as it can bring together multiple vendor software solutions in one place. This is not only beneficial for streamlining operations, but it also implements consistent security and compliance protocols across different vendor solutions.

Eurotech is a steering committee member of the Eclipse Foundation Edge and IoT Working Groups. It founded and mentors several of its IoT open source projects. Eurotech then offers enterprise-ready editions of such projects through its Everyware Software Framework (ESF) and Everyware Cloud (EC). ESF is a platform that enables developers to create and deploy applications across diverse embedded and IoT devices with simplified connectivity and management, while EC is a dedicated cloud-based service platform designed to collect, store, process, and manage data from connected devices.



Together they enable organisations to provision, monitor health, status, and configuration of deployed edge devices in the field from a single dashboard.

From a device integration perspective, it is vital that devices have zero-trust architecture embedded within them that enables effortless third-party software integration. The goal is to create a 'single-click, high trust' deployment process that simplifies onboarding for partner companies and reduces friction in software implementation.

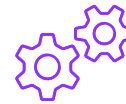
It's equally important to embrace modularity. It's possible to create a more flexible architecture by breaking complex problems into smaller, more manageable microservices. Modular design enables easier customisation, faster innovation, and smoother integration with complementary technologies. This approach not only simplifies internal development but also makes products more compatible with solutions from different vendors.

This balanced approach of leveraging open standards, comprehensive management platforms, and appropriate technological advancement is essential when creating solutions to meet the needs of smart space infrastructures.

► In summary:



OPEN STANDARDS AND PROTOCOLS ARE CRITICAL TO PROJECT SUCCESS



SYSTEM INTEGRATORS ARE CRITICAL TO BRIDGING GAPS BETWEEN DIFFERENT MANUFACTURERS' DEVICES



A CENTRALISED MANAGEMENT PLATFORM SIMPLIFIES OVERALL SYSTEM MANAGEMENT



DEVICE INTEGRATION REQUIRES ZERO-TRUST ARCHITECTURE



MODULARITY IS CRUCIAL FOR CREATING FLEXIBLE ARCHITECTURES



04 conclusion

Smart space infrastructures are complex by their nature. A typical solution involves CCTV cameras capturing raw video, attached to Edge AI devices processing and analysing the feed. It then needs to connect to a central server to share and manage information. For organisations looking to implement smart space infrastructures in large public or private infrastructures, this means deploying hundreds, if not thousands, of edge devices running multiple AI algorithms.

The barriers to entry are significant. Companies must invest substantial resources in finding the right partners, understanding complex networking requirements, and creating a cohesive technological ecosystem. It's not just about purchasing devices, it is also about building an intelligent, interconnected infrastructure that can scale and adapt to evolving technological needs.

System integrators are crucial in bridging the gaps between different technologies, ensuring that devices from various manufacturers can communicate seamlessly and effectively with each other. No single company can realistically provide every component of such a sophisticated system, but each plays a critical role in the overall infrastructure. To implement smart spaces, therefore, it's necessary to address the complex challenge of integrating technologies from multiple vendors.

Using 'open standards and protocols' is key, as it ensures interoperability and easier integration between devices and software while maintaining security. This collaborative approach benefits the entire industry ecosystem. By establishing common frameworks, developers and companies can build upon existing technologies without being locked into proprietary systems.

This approach accelerates smart space implementation by reducing the barriers to entry for new public or private organisations by creating a more collaborative, innovative, and interconnected system that benefits developers, businesses, and end-users alike.

**Find out more about
Eurotech Edge AI solutions**

Get in touch

