WHITE PAPER

The digitization and cybersecurity of physical access control

An exploration of the systems and protocols to enable businesses to unlock the full potential of access control and create a smarter, safer world

August 2021

AXIS COMMUNICATIONS

Table of Contents

1 Summary

The development of cloud connectivity is changing the face of the physical security industry and is forcing installers to adapt to stay in business. The control of access systems seems to be moving into the domain of the global technology firms, bringing an expectation of greater value from the systems themselves, as they become ever more intelligent, scaleable and edge-based.

This evolution, along with its potential for integration with other corporate systems, also means that cybersecurity needs to play an even greater role in system development and deployment, especially in those cases that build upon existing infrastructure. Overcoming technical barriers such as serial architecture, the absence of MAC addresses and so on, is a crucial step in the transition to digital access control systems able to meet today's and future requirements.

Implementing and securing a digital system for access control also means following the best practices to ensure the best possible security. We need to assess and test every component involved in the system, be it a device, a supplier or a protocol – these all need to be trustworthy and reliable. We also need to constantly be aware of the threat landscape and how to mitigate the dangers presented by newly discovered vulnerabilities and flaws.

Vendors especially should be given special consideration, as you are allowing their devices into your network. A serious vendor should provide and make known their own processes for securing their offerings by, for example, publishing a hardening guide, by providing dedicated management tools that make it simpler to manage and secure network devices, etc. Furthermore, a vendor should preferably be open and honest concerning their strategy for managing discovered vulnerabilities and flaws.

2 Introduction: The future of access control

Cloud connectivity has presented the physical security industry with a new vision of how systems should be deployed and utilized. End-users and buyers are demanding smarter, integrated and more business-focused solutions with surveillance and access control capabilities that reach well beyond those afforded by traditional legacy technologies.

Many suppliers have built up a strong business model around their expertise, service and knowledge of physical security. However, network connectivity and the IoT present a constantly shifting landscape, requiring a traditional vendor and installer of physical security to learn the language of IT; of open platforms, IP connectivity and software integration, in order to adapt to market changes and remain relevant.

It seems that control is rapidly shifting from the suppliers of electronic access systems to global technology firms, who now have the power to shape security in a direction that challenges its traditional operation. Smart buildings and cities present great opportunities, and many anticipate rapid growth of the modern access control market as ease-of-deployment and the sophistication of today's technologies bring many benefits to the smart environment.

It's no surprise that a drive towards embracing hosted access control comes about as the impact of tech giants have demonstrated the success of cloud technologies; so heavily relied upon during the global COVID-19 pandemic. Such companies have the scope, scale and imagination to bring about radical change, and physical security will also be transformed as businesses, realizing the value of the cloud, look to hosted solutions to take care of all of their security and business requirements.

Currently, however, many manufacturers are simply not ready for this changing market and still follow business models based upon rigid, proprietary designs. The shift toward smart physical security solutions exists in direct contrast to this traditional approach, which is likely to be strongly challenged. While change

will not happen overnight, and new cloud hosting solutions are yet to become mainstream, this bright new world is nevertheless the domain of the new engineers joining our industry right now.

The future of access control, and physical security as a whole, will therefore be based on expectations of greater value. Access control systems will become data collection points and door controllers will become intelligent I/O devices. QR codes for visitor management and biometric face recognition for frictionless access control will increasingly be managed at the edge as analytics in a camera or sensor. The future of access control presents an exciting and challenging time for those ready to accept it and help shape it; a true opportunity to innovate for a smarter, safer world.

In this paper we explore those aspects that are particularly relevant to access control, including many of the fundamental features of these systems. We will also look at considerations surrounding best practices for suppliers, with information and suggestions for endusers, intended to give them the confidence to challenge their providers and to make more enlightened purchasing decisions.

3 Challenges in an evolving access control market

When we focus on physical access control systems (PACS), we tend to address risk factors in terms of considerations concerning the granting or blocking of physical entry. Taking a balanced approach to the design of a physical access control system is an important consideration based on assessments of the potential threat.

Nowadays, as premises are increasingly protected by more and more sophisticated electronic access control solutions, these systems provide a quick and efficient way of managing access across the whole enterprise, leaving a digital footprint that can be examined and monitored if necessary, as well as being fully integrated with other systems such as HR and visitor management.

With this system unification producing powerful insights to aid both business and security decision making, as well as controlling access, it becomes crucial to thoroughly evaluate the cyber-maturity of the system. As criminals become ever more sophisticated and the threat landscape continues to evolve, the challenge lies in mitigating the risk of cloned access credentials, insider threats or remotely launched cyber-attacks.

However, the architecture itself presents a problem. Many traditional access control systems are built upon outdated infrastructure. With converging security technologies commonly utilizing this infrastructure, the challenge for vendors is partly to adapt their hardware to connect to these corporate networks, and partly to realize the importance of IT security and the changing security landscape that drive the need to thoroughly evaluate and guard against the many risks posed to an enterprise.

Cybersecurity considerations should be a key factor in the development of new security systems. Access control technologies play an integral part in any physical security solution and should therefore be manufactured according to recognized cybersecurity principles, incident reporting and best practises. It is important to acknowledge that the integrity of a system is only as strong as its weakest link. **A system that is not prepared to accept it** constitutes a potential risk of exposure. If it cannot demonstrate the readiness to accept, inform and put in place publicly acknowledged recovery actions, this will ultimately impact negatively on its ability to provide the necessary levels of physical security for which it has been deployed.

3.1 Cybersecurity credentials (cyber-maturity)

The growing involvement of the IT industry is beginning to change the way technologies are evaluated, deployed and maintained. A key consideration for IT stakeholders is the evaluation of a business's cybersecurity credentials with a key focus on vendor cybersecurity knowledge. This knowledge is also referred to as cyber-maturity. Being cyber-mature suggests a good understanding of the threat

landscape and the mitigation of risk. The extensive cybersecurity documentation and guidance that has already been developed for network cameras can also be applied to physical access control, as the challenges, assessments and explanations of cyber risk and the potential for attack are equally relevant for these products.

3.2 The future of security systems architecture

Modern access control devices are connected via network cables and RJ45 connectors. Networks provide power for access controllers, as well as the communication between devices and central management systems. The driving force in access control is the transition to TCP/IP-based systems. Since the introduction of the first truly IP-enabled door controller (AXIS A1001) in 2013, PACS has continued to evolve, now delivering a wide range of advanced features that would never have been possible by relying solely on legacy technology.

Examples of such innovation include QR code readers for the facilitation of touch-free access control, facial recognition through integration with network cameras, and license plate reading, all interacting with PACS databases for edge-based decisions on the granting or refusing of admission. Key benefits of IP systems include low installation costs with simple configuration and device management. Easy integration with other devices means a future-proof solution that enables simple plug-and-play connectivity of new security technologies and enhancements as they become available.

3.3 IP versus traditional access control

The advantages of IP will be realized in new and modern access control designs, especially in contact-free systems, which end-users expect as standard. Users will also want to see access control adapt to the use of smartphones and tablets, and not just with a mobile credential. How will the industry deliver better, more useful and time/cost saving access control systems, and can it keep pace with the innovation cycles being driven by big tech companies? These are the challenges on the supplier side of the industry.

Up until now, these opportunities have not been exploited, possibly because legacy access control systems depend on door controllers installed in serial architecture and connected by RS-485 cabling to a central unit or server. Most systems are also proprietary, which means the door controller is 'locked' to only allow management via software designated by the supplier. This limits the end-user to a single hardware and software supplier, and the complexity of such systems often requires expert personnel for installation and configuration.

When expanding traditional access systems, the process is complicated by the fact that a typical central controller is designed to accommodate a certain number of doors, with non-standard configurations incurring high costs due to limited system flexibility. For example, adding just a single additional door may result in much higher costs, making the addition unjustifiably expensive.

IP networks have allowed the introduction of much simpler, easy to install PACS architecture, with far greater flexibility and customization. IT professionals have a strong preference for true IP devices and their use in network-based access control systems. Including these persons in the future design process is key, as they will ensure the use of these IP devices, which are also key in reducing the cost of expansion and will be a requirement for future access control designs.

3.4 Open protocols

The future of access control is tied to the willingness of manufacturers to share their skills and abilities in an open protocol forum. Resistance to this openness is obvious, as many access system developers seem to

favor a process that ties end-users to their own solutions, guaranteeing future revenue. However, this approach contains no long-term value. Users are demanding more from their solutions and are happy to share their data in order to do so.

System designers and access hardware suppliers seldom have the resources or IT know-how to offer all the solutions that users request as part of a comprehensive physical security system. Many seem genuinely unaware that their offerings are rapidly being eclipsed by innovative new solutions that threaten both their business model and their standing in the access control marketplace. Such are the capabilities of the latest systems, and the speed of modern innovation, that we are now very close to not needing an access controller at all; with intelligent I/O units becoming the obvious replacement.

Openness allows vendors to build devices suitable for small-scale access systems, where simplicity is key and where purchase and installation costs need to be competitive. These same devices can then be adapted for larger and more technically complex operations as required. This flexibility is the hallmark of modern security and ensures that the systems purchased today will still be relevant in the future, as the user's business grows and requirements change.

More information on openness and open technology can be found on the ONVIF website *www.onvif.org*, an industry body created to drive development toward open standards.

4 Technical barriers to adoption

There is much to consider in terms of the technical connections, interfaces and devices that make digital access control possible. There may be ramifications as a result of the move from traditional to cloud-enabled systems. The following sections detail those points that must be considered to help existing technology, and the processes associated with it, avoid becoming a barrier to upgrading and embracing new solutions.

4.1 RS-485 controllers

One consideration is the deployment of the RS-485 controller and the potential risk of installing semi-intelligent devices that rarely, if ever, possess a media access control (MAC) address, making them difficult to identify. RS-485, also known as TIA-485(-A) or EIA-485, is a standard defining the electrical characteristics of drivers and receivers for use in serial communications systems. Electrical signalling is balanced, and multipoint systems are supported. But RS-485 only specifies the physical layer; the generator and the receiver. It does not govern the vital communications layer.

Note that the absence of a MAC address or the adoption of a serial architecture does not itself mean reliability issues or detrimental effects on the operation of an access control system: such designs have been the mainstay of access control for more than 30 years. However, advances in security expectations are difficult to visualize unless each and every control device in an access control system is intelligent and can be individually addressed. We postulate that only fully intelligent systems and completely accessible devices can deliver the future value expected. Note that 'completely accessible' does not mean devices with poor cyber security: quite the opposite.

4.1.1 Open Supervised Device Protocol (OSDP)

A new communications method, having been accepted by the IEC and offering the potential to increase security in access communications, is the Open Supervised Device Protocol (OSDP); an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP uses 128-bit encryption, supports multidrop installations and supervises connections to report reader issues. A further point to note is that OSDP supports card readers, door strikes, alarm contacts, and request to exit functions using just 2 wires and not the multiple

connections previously required per door. The SIA website reports: 'OSDP was approved as an international standard by the International Electrotechnical Commission in May 2020 and will be published as IEC 60839-11-5 in July 2020. SIA OSDP is in constant refinement to retain its industry-leading position.'

4.2 The value of devices with a MAC address

The MAC address is the globally unique hardware address of a single network adapter or device. In relation to IT networking, the MAC address is every bit as important as an IP address. MAC addresses uniquely identify a computer on the LAN, and are required for network protocols such as TCP/IP to function. The MAC address is hard-coded into the device, and although possible to spoof via the operating system, this is, of course, not advisable and the address should be protected by your security solution.

TCP/IP and other mainstream network architectures generally adopt an Open Systems Interconnection (OSI) model, in which network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model), and they allow computers to uniquely identify themselves on a network. MAC address filtering adds an extra layer of security. Before allowing any device to join the network, the router checks the device's MAC address against a list of approved addresses. If the client's address is on the router's list, access is granted, if not access is denied.

4.2.1 Power over Ethernet (PoE)

PoE offers two benefits that are consistent across applications; cost savings and flexibility of device placement. PoE carries both data and power in the same cable, meaning device architecture can be simplified as compared to traditional designs. It is worth noting that many access control systems are promoted as IP-connected

5 The hallmarks of best practice

Access control management is an important component of effectively handling the flow of people and controlling access. Much more than just locking a door or putting up a barrier, businesses require better control options for delivering an improved customer service relationship and high levels of security and safety at all times. Adopting a best practice approach to comprehensive access control goes beyond selecting the right tools. It's about having the right architecture in place; incorporating high-quality technologies; following the right procedures and protocols; and encouraging staff and stakeholders to adopt the correct attitudes and behavior.

5.1 Stakeholder management and the converged security approach

As we see the technology landscape converge across the same infrastructure to deliver the operational technologies required for these sites to function seamlessly, we also need a converged decision-making process. We've already seen successful examples where a converged security approach has broken down walls and allowed different business teams to work together. This convergence has never been so important as it is today, when traditional electronic and physical security offerings exist side-by-side on corporate networks.

It is vital that physical security teams can rely on technologies that support their operational requirements and that address the associated risks, while at the same time, supporting IT security policies and ensuring that physical devices do not become a back door into the corporate network. With all stakeholders working together it is possible to create a secure cyber and physical environment.

5.2 What to expect from partners, vendors and suppliers

It is important to ensure that third parties understand the importance of keeping security best practices at the forefront of everything they do, and that they operate to meet specific needs. Relationships with third parties are key to establishing a healthy supply chain and forging a strong and trusted bond.

Key considerations when evaluating third parties and their impact on the supply chain:

- They understand and acknowledge the associated risks around cybersecurity
- They can demonstrate a mature cybersecurity approach with processes and tools available
- They understand the impact of regulations and legislation on their offering
- They can demonstrate how they will support a user's compliance requirements
- Cybersecurity is a process and not just a technology - they can demonstrate cybersecurity life cycle management to protect a user's enterprise.

5.3 Security Management: Governance and vendor processes

Like all effective security, cybersecurity is about the depth of the defence. It's about appropriately protecting the IP camera network at every level; from the selected products and partners to the requirements set.

5.3.1 Standards and directives

ISO 27001 – Information Security Management ISO/IEC 27001 is a Security Management System that requires:

- The systematic examination of an organization's information security risks, taking account of threats, vulnerabilities, and impacts
- The design and implementation of a coherent and comprehensive suite of information security controls and/or other forms of risk management (such as risk avoidance or transfer) to address those risks deemed unacceptable
- The adoption of an overall management process to ensure that information security controls continue to meet the organization's information security needs on an ongoing basis.

5.3.2 Cyber Essentials Plus

Cyber Essentials is a government-backed, industry-supported scheme to help organizations protect themselves against common online threats. Cyber Essentials is an effective indicator for businesses that understand the challenges posed by cybersecurity, and is an evaluation of a company's policies and processes. It looks specifically at:

- Secure configurations
- Access control and administration
- Malware protection
- Patch management
- Firewall and internet gateways

For technology manufacturers, the first line of defence should be the mitigation of risk associated with their own systems. As of 1st October 2014, the government required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified according to the Cyber Essentials scheme.

5.3.3 Secure by Design, Secure by Default

Launched by the Surveillance Camera Commissioner in 2019, **Secure by Design, Secure by Default** sets a minimum requirement for manufacturers of surveillance camera systems and components. The scheme requires that manufacturers take a holistic approach to solving security problems at the root cause, rather than treating the symptoms; acting at scale to reduce the overall harm to a system or type of component.

Secure by Design, Secure by Default covers the long-term technical effort to ensure that the correct security primitives are built into software and hardware. It also covers the equally demanding task of ensuring that those primitives are available and usable in such a way that the market can readily adopt them.

To support our technologies, Axis has aligned Secure by Design, Secure by Default to the National Cybersecurity Strategy code of conduct:

- Password Prompt
- Password Strength Indicator
- HTTPS Encryption
- 802.1x
- Remote Access DISABLED (NAT traversal)

6 Guides and tools (vendor processes)

When it comes to securing a network, organizations will often deploy several technical controls to create a 'layered defence' approach, which helps to limit the single points of failure and exposure. However, one important process that is often overlooked is 'system hardening', which includes making configuration changes to default system settings so that the system is more secure against information security threats. In addition, this process helps to reduce the amount of inherent vulnerabilities that exist in all systems.

6.1 Manufacturing Hardening Guide

A system hardening process should be in place for all devices attached to a network. This includes workstations, servers and other network devices. As each manufacturer knows their own system setup and configuration better than most, it should be their own responsibility to provide partners and users with the necessary information to protect the integrity of their devices and the end-user's installation. A hardening guide should provide technical advice for anyone involved in deploying video surveillance solutions. It should establish a baseline configuration, as well as provide comprehensive information on dealing with the evolving threat landscape.

All vendors should strive to apply cybersecurity best practices in the design, development and testing of devices, to minimize the risk of flaws that could be exploited in an attack. However, securing a network, its devices, and the services it supports requires active participation from the entire vendor supply chain, as well as the end-user organization. A secure environment depends on its users, processes, and technology. A good hardening guide should follow baseline uses such as the CIS Controls - Version 6.1 . These controls were previously known as SANS Top 20 Critical Security Controls.

6.2 Device management

A device manager is an on-premises tool that provides a simple, cost-effective and secure way of managing connected devices. It offers installers and system administrators a highly effective tool to manage all major installation, security and maintenance tasks.

Device inventory / Asset management system:

- Account and Password Policy
- Efficient installation of firmware upgrades and applications
- Apply cybersecurity controls — manage HTTPS and upload IEEE 802.1x certificates, manage accounts and passwords
- Certificate lifecycle management - Manage all major installation, security & operational tasks
- Fast, easy configuration of new devices — backup and restore settings
- Suitable for sites of all sizes — single or multiple site installations

6.3 Challenges associated with OEM / ODM

Original equipment manufacturers (OEMs) are manufacturers who resell another company's product under their own name and branding. An original design manufacturer (ODM) is a company that designs and manufactures a product that is specified and eventually branded by another firm for sale. Such companies allow the brand firm to engage in production without having to start or run a factory.

There are many pros for a manufacturer looking to OEM or ODM a product from another supplier. The first is that it removes any manufacturing risks and costs, and it allows an organization to focus on its sales and marketing processes. This is one of the key reasons that many camera manufacturers across the security industry OEM or ODM their branded products.

This presents several challenges, one of the most obvious being cybersecurity. If one manufacturer has a vulnerability in its products, this can impact all the other resellers and partners throughout the supply chain. It can also make full visibility of the supply chain very difficult. With the sheer number of OEMs and ODMs in operation, an end-user who has followed due diligence and refused technologies from a certain manufacturer could unwittingly end up using those technologies in a re-branded form, yet be totally unaware of the fact.

6.4 CPU microprocessor chip

It has become apparent that generic CPU processing chips installed into devices are being targeted by hackers, with many vulnerabilities being identified. One of the main reasons for this is the scalability that they generate from a single identified vulnerability. Recent examples include the 'Meltdown' and 'Spectre' flaws , two related, side-channel attacks against modern CPU microprocessors that have the ability to unlawfully access data using unprivileged code.

Most devices, from smartphones to hardware in data centres, may be vulnerable to some extent. The major operating system vendors have produced patches which mitigate the issues, though some parts of the patches need to be installed via the equipment manufacturer (OEM) as they contain platform-specific elements. The National Cybersecurity Centre (NCSC) advises to patch devices as soon as possible.

6.5 Firmware strategy

Signed firmware is important for end-users and mitigates some of the potential risks of devices being tampered with through the logistics and/or distribution process. The signature, sometimes called a hash, is appended to the firmware when distributed. A processor calculates its own hash and will only load a firmware image that has a hash matching one signed by a certificate that it trusts.

6.6 Vulnerability management

The continued growth of cyber-crime and its associated risks are forcing many organizations to focus more on information security. A vulnerability management process should be part of an organization's efforts to control information security risks. This process will give an organization a continuous overview of vulnerabilities in its IT environment and the risks associated with them. Only by identifying and mitigating vulnerabilities in the IT environment can attackers be prevented from penetrating its networks and stealing information.

It is essential that suppliers ensure that the management of vulnerabilities is covered in their operations, including processes to detect and remedy vulnerabilities in all systems and to prevent new vulnerabilities being introduced during change processes and new system deployments. All issues related to risk that the supplier accepts must be communicated and agreed with the end-user. If this principle is not implemented, attackers could exploit vulnerabilities within systems to carry out cyber-attacks against an enterprise and its suppliers.

IT security patches and security vulnerability updates must be installed through an approved process in a timely manner to prevent any security breaches. Supplier systems that for any reason cannot be updated must implement measures to protect the vulnerable system. All changes must be undertaken in accordance with the supplier's change management process.

6.7 Security Advisory Notifications

Security advisories help reduce the risks due to known vulnerabilities. The security advisory may refer to official CVE (Common Vulnerability and Exposure) or other vulnerability reports, and they include a vulnerability description, risk assessment, recommendations and information on when a service release will be available. Most vendors deploy an indirect sales model and have a partner program in place.

Security Advisory Notifications allow customers that are not registered in a manufacturer's partner program to obtain relevant cybersecurity notifications at the earliest opportunity, and when they are communicated to the channel. This is a critical tool for end-users that have equipment installed, but who do not have a contract with the company that originally carried out the installation.

6.8 Building Security in Maturity Model (BSIMM)

BSIMM is a software security measurement framework established to help organizations compare their software security with other initiatives, and to find out where they stand. BSIMM helps to assess processes, activities, roles and responsibilities in the following:

- Design and architectural reviews
- Code reviews
- Testing for known vulnerabilities

- Running a standard vulnerability scanning tool that can find CVE vulnerabilities in open source packages

6.9 Long Term Support (LTS)

Long-term support (LTS) is a product lifecycle management policy in which a stable software release is maintained for a longer period of time than the standard edition. Long Term Support firmware should include only patches for stability, performance and security. Vendors provide LTS firmware for up to 10 years from when a device is introduced to the market.

It is expected that LTS will exist in parallel with, but independently of existing active software support. One of the key benefits of LTS support is that it will retain integration with third parties related to the original firmware version.

6.10 Learning and collaboration

One of the key areas for consideration when selecting any technology vendor is the training and support it provides. As the challenges facing the channel and industry evolve, particularly for cybersecurity, manufacturers should seek to pro-actively address the subject and provide collateral and content for the market. Potential examples include:

- Free of charge, classroom-based courses on cybersecurity
- Online cybersecurity training
- Online cybersecurity quick test
- Hardening guide
- Vulnerability policies
- Cybersecurity best practices
- Cybersecurity concepts and terminology

7 Creating a cyber hygiene profile: next steps and considerations

Good cyber hygiene involves identifying, prioritizing, and responding to risks to the organization's key services and products. Implementing cyber hygiene security best practice will help prevent data breaches and incorrect system configurations, as well as miniming the associated risks to the business. It's also important to get stakeholder agreement on the key threat areas, to focus on the prime objectives for risk management.

While not an exhaustive list, the following considerations will help to improve efficiency in dealing with cyber threats.

7.1 Suppliers

Check registrations and certifications

Review appropriate registrations and certifications: e.g. ask for evidence of ISO9000 registration and other quality certifications. Determine if the supplier's products have been designed for use on a corporate network.

Look for evidence of best practice

Ensure that a chosen provider can demonstrate cybersecurity best practice. They should offer a cyber hardening guide which will describe cyber and physical security measures, and best practices to help secure the network.

Audit your provider

Conduct a thorough audit before making any commitment to purchase. Check their terms of business to make sure they are clear and transparent. From a financial perspective, it's important to ask what would happen to the product and support should the business run into trouble.

Determine resources for ongoing support

Ascertain whether your provider has the resources to continue to create the solutions that you anticipate you will need in future. Verify that your provider is of a size, reach and capability to support your business requirements moving forward.

Define future business needs

Focus on your needs for the future. Intelligent devices and solutions have the capabilities to enhance and future-proof a business, so you should feel confident that your supplier will meet or exceed your expectations, with maintenance agreements and ongoing support.

Seek verification of ethical business practices

Check for evidence of ethical and sustainable practices. A partnership built on trust and common goals is a powerful foundation for longevity. Does the provider have environmental management systems in place, a corporate social responsibility (CSR) program or an ethical sourcing policy?

7.2 Products and systems

Exercise due diligence

Carry out technical due diligence on the system and its core elements to make sure that it delivers value and that there are no underlying factors that might affect ongoing operation. Ensure that information on risk assessment and risk mitigation is clear and available.

Check the maintenance contract

Verify what is included as part of a contract, such as whether the service and maintenance contract includes manufacturer software updates and firmware upgrades.

Secure connected devices

Be confident that your network connected physical security system is secure. Security systems should be deployed with cybersecurity in mind; changing default username and password; installing the latest firmware; utilising encryption (ideally HTTPS); disabling remote access.

Request a statement of design security

Your supplier should be able to provide a statement of design security as proof of the cyber secure status for any network connected devices.

Assess the intelligence of the system

Connected devices that are fully intelligent are those that are networked with a MAC address and form an intrinsic part of the system architecture. Devices without a MAC address are not intelligent and cannot be individually identified, managed or protected.

Evaluate GDPR / Data Protection Act compliance

The GDPR came into effect in 2018, along with the updated Data Protection Act of 1998. Ensure that products and systems support the ability to comply with the Data Protection Act 2018 and the GDPR.

T10168631/EN/M4.2/2108

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden