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

September 2020

Authors:
John Allen, Business Development Manager, Access Control, Axis Communications
Steven Kenny, Industry Liaison Manager, Architecture & Engineering, Axis Communications

AXIS COMMUNICATIONS

Table of contents

1. 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 utilised. End users and buyers are demanding smarter, integrated and more business focussed solutions with surveillance and access control capabilities that reach well beyond those afforded by traditional legacy technologies.

Suppliers have built up a strong business model around their expertise, service and knowledge of physical security. Yet, network connectivity and the IoT present a constantly shifting landscape, requiring the traditional physical security vendor and installer 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 away from the suppliers of electronic door access systems to become the domain of the global technology firms who have the power to shape security in a direction which 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, realising the value of cloud, look to hosted solutions to take care of all of their security and business requirements.

Yet, at the present time, many manufacturers are simply not ready for this changing market and still follow business models set around 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 of physical security as a whole, will therefore be based on an expectation 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 to help shape it; a true opportunity to innovate for a smarter, safer world.

In this paper we explore those aspects which are particularly relevant to access control, including many of the fundamental features of these systems; we also look at considerations around best practice for suppliers, with information and suggestions for end users, intended to give them the confidence to challenge their providers and make more enlightened purchasing decisions.

2. 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 around granting or blocking 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.

Now, 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 enterprise, leaving a digital footprint that can be interrogated and monitored if necessary and fully integrated into other systems such as HR and visitor management.

With such unification of systems producing powerful insights to aid both business and security decision making as well as controlling access, it's crucial that the cyber maturity of the system is thoroughly

evaluated. As criminals become more sophisticated and the threat landscape continues to evolve, the challenge lies in preventing 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 aged infrastructure. With converging security technologies commonly utilising this existing infrastructure, the challenge for vendors is not only to be able to adapt their hardware offering to connect to corporate networks, but also to realise the importance of IT security and a changing security landscape in driving 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 recognised cybersecurity principles, incident reporting and best practises. It is important to acknowledge that the cyber integrity of a system is only as strong as its weakest link. A system which is not prepared to accept it is a potential source of cyber exposure, and which cannot demonstrate the readiness to accept, inform and put in place publicly acknowledged recovery actions will ultimately impact negatively on its ability to provide the necessary high levels of physical security for which it has been deployed.

2.1 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 which 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 potential attack discussed are equally relevant.

2.2 The future of security systems' architecture

Modern access control devices are connected via network cables and by RJ45 connectors. Networks provide the device power for access controllers, as well as the communications medium between devices and a central management system. 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 never could have been attained by solely relying on legacy technology.

Examples of such innovation include QR code readers for the facilitating of frictionless access control, facial recognition through integration with network cameras, and license plate reading, all interacting with PACS databases for edge based decision making around the granting or refusal 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.

2.3 IP versus traditional access control

The advantages of IP will be realised in new, modern access control designs, certainly in frictionless or contact free systems which end users expect will become the norm. Users also want to see access control adapt to the use of smartphones and tablets, and not just with a mobile credential. How will this 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 for the supply side of the industry.

Up to now, these opportunities have not been exploited, perhaps because legacy access control systems are dependent on having door controllers in a serial architecture, with RS-485 cable into one central unit or central server. Most systems are also proprietary, which means the door controller is 'locked' to allow management through a certain piece of software, installed by the provider. This limits the end user to one single provider of hardware and software, and the complexity of such systems requires expert personnel to handle installation and configuration.

When expanding traditional access systems the process is complicated by the need to consider that a typical central controller is built to accommodate a certain number of doors, with any requirement to deviate from a standard configuration bringing high costs due to a lack of flexibility in the system. For example, adding just one additional door can equate to much higher marginal costs, which can make the addition unjustifiably expensive.

IP networks have allowed the introduction of much simpler, easy to install PACS architectures, with far greater flexibility and customisation. IT professionals have a stronger preference towards true IP devices and their inclusion in future designs where network connection is key. Such devices are also key to lower cost system expansion and will be a requirement for future access control designs.

2.4 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. The resistance to this is clear and obvious as many access system developers seem to favour a process that will tie-in end users to their own solutions, guaranteeing a future revenue stream. Yet this approach does not hold any 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 do not have the resources or IT know-how to offer all of the solutions that users are asking for as part of a comprehensive physical security system. Many seem genuinely unaware that their offerings are rapidly being eclipsed by innovative new solutions which threaten both their business model and their standing in the access control marketplace. In fact, such are the capabilities of new systems, and the speed of modern innovation, that we are now only a step away from not needing an access controller at all; with intelligent I/O units becoming the obvious replacement.

Openness allows vendors to build devices which are suited to small 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 by an end user today will still be relevant in the future, as the end user's estate grows and business 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.

3. 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 avoid existing technology, and the processes associated with it, becoming a barrier to upgrading and embracing new solutions.

3.1 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, carry 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 raise reliability issues or is detrimental to 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 visualise 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 – 'completely accessible' does not mean any device should be a cyber weak device: quite the opposite.

Open Supervised Device Protocol (OSDP)
A new communications method, which has been accepted by the IEC and offers 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 of note is that using OSDP means card reader, door strike, alarm contact, and request to exit functions are supported using 2 wires, not the multiple connections that used to be 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.'

3.2 The value of devices with a MAC address

The MAC address is the worldwide 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 like TCP/IP to function. MAC addresses are hard coded into each device and although it is possible to spoof the address via the operating system it is, of course, not to be advised and should be protected within the cyber hygiene of your security solution.

TCP/IP and other mainstream network architectures generally adopt an Open Systems Interconnection (OSI) model. In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model). 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 matches one on the router's list, access is granted. Access is otherwise denied and blocked.

3.3. Power over Ethernet (PoE)
PoE offers two benefits that are consistent across applications; cost savings and flexibility of device placement. PoE runs data and power together in the same cable, meaning device architecture can be simplified compared to traditional designs. It is worth acknowledging that many access control systems are promoted as IP connected.

4. The hallmarks of best practice

Access control management is an important component of effectively handling the flow of people and restricting access where there is a need. Much more than just locking a door or putting up a barrier, businesses require better control options to deliver 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 exhibit the right attitudes and behaviours.

4.1 Stakeholder management and the converged security approach

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

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

4.2 What to expect from partners, vendors and suppliers

It is important to carry out due diligence, making sure that third parties understand the importance of keeping security best practice at the forefront of everything they do and are operating in such a way that meets 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 on regulations and legislation for 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.

4.3 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 products chosen and the partners engaged with to the requirements set.

4.3.1 Standards and directives

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

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

4.3.2 Cyber Essentials Plus

Cyber Essentials is a government-backed, industry-supported scheme to help organisations protect themselves against common online threats. Cyber Essentials is an effective indicator for businesses that understand the challenges posed by cybersecurity. Cyber Essentials 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. From 1 October 2014, the government required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

4.3.3 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 demonstrates 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 right 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)

5. Guides and tools (vendor processes)

When it comes to securing a network, organisations will often deploy several technical controls to create a 'layered defence' approach. This approach 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 which exist in all systems.

5.1 Manufacturing Hardening Guide

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

All vendors should strive to apply cybersecurity best practice 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 organisation. A secure environment depends on its users, processes, and technology.

Examples of good hardening guides should follow baseline uses such as the CIS Controls - Version 6.1 . These controls were previously known as SANS Top 20 Critical Security Controls. This document refers to these CSC (Critical Security Control) by marking CSC#.

5.2 Device management

A device manager is an on-premise tool that delivers an easy, cost-effective and secure way to manage 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

5.3 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 which is specified and eventually branded by another firm for sale. Such companies allow the brand firm to produce, without having to engage in the organisation or running of a factory.

There are many pros for a manufacturer looking to OEM or ODM a product from another supplier. The first being that it removes any manufacturing risks and costs, and it allows an organisation to focus on the sales and marketing process. This is one of the key reasons that many camera manufacturers across the security industry OEM or ODM their branded products. It has been reported that as many as 96 vendors OEM or ODM cameras from another supplier.

This brings several challenges, one of the most obvious being cybersecurity. If one of the manufacturers has a vulnerability it can impact all 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 the due diligence process and refused technologies from a certain manufacturer could unwittingly end up using those technologies in a re-badged form, yet be totally unaware of that fact.

5.4 CPU microprocessor chip

It has become apparent that off the shelf CPU processing chips that are 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 , which are 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.

5.5 Firmware strategy

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

5.6 Vulnerability management

The continued growth of cyber-crime and its associated risks are forcing most organisations to focus more attention on information security. A vulnerability management process should be part of an organisation's efforts to control information security risks. This process will allow an organisation to obtain 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 an organisation prevent attackers from penetrating its networks and stealing information .

It is essential that suppliers ensure the management of vulnerabilities are covered within their operations, including processes to detect and remediate 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 an 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 have measures to protect the vulnerable system. All changes must be undertaken in accordance with the supplier's change management process.

5.7 Security Advisory Notifications

Security advisories help reduce risks of known vulnerabilities. The security advisory may refer to official CVE (Common Vulnerability and Exposure) or other vulnerability reports. The security advisories include a vulnerability description, risk assessment, recommendations and information relating to 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 aren't registered within any of the partner programs that a manufacturer has in place, 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 may not have a contract with the company that originally carried out the installation.

5.8 Building Security in Maturity Model (BSIMM)

BSIMM is a software security measurement framework established to help organisations compare their software security to other organisations' initiatives and find out where they stand. BSIMM helps to assess processes, activities, roles and responsibilities. These include:

> Design and architectural reviews
> Code Review
> Testing for known vulnerabilities
> Run a standard vulnerability scanning tool that is used to find CVE vulnerabilities in open source packages

5.9 Long Term Support (LTS)

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

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

5.10 Learning and collaboration

One of the key areas for consideration when selecting any technology vendor is the education and support that it has in place. As the challenges facing the channel and industry evolve, in particular around cybersecurity, manufacturers should look to proactively address the subject and provide collateral and content for the market. Potential examples include:

> Free to attend, classroom-based academy courses on cybersecurity
> Online cybersecurity training academy
> Online cybersecurity quick test
> Hardening guide
> Vulnerability policies
> Cybersecurity best practice
> Cybersecurity concepts and terminology

6. Creating a cyber hygiene profile: next steps and considerations

Good cyber hygiene involves identifying, prioritising, and responding to risks to the organisation's key services and products. Implementing cyber hygiene security best practice will help prevent data breaches and system misconfigurations, as well as minimising the associated risks to the business. It's also important to gain stakeholder agreement on the key areas of threat, to focus on prime objectives around risk management.

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

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?

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 that are networked 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.

EN/R1/2009

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,500 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.