White paper

Quick guide to Axis datasheets

Approvals, certifications, and protocols

February 2019

AXIS COMMUNICATIONS

Table of contents

1. Introduction

Axis Communications adheres to the applicable industry standards and compliance standards for all products that are brought to market. This document supplements Axis datasheets with definitions and simplified descriptions of acronyms, approvals, certifications and protocols found therein.

In the current version, this document provides information that regards those datasheet sections that are highlighted and zoomed in the datasheet image below.

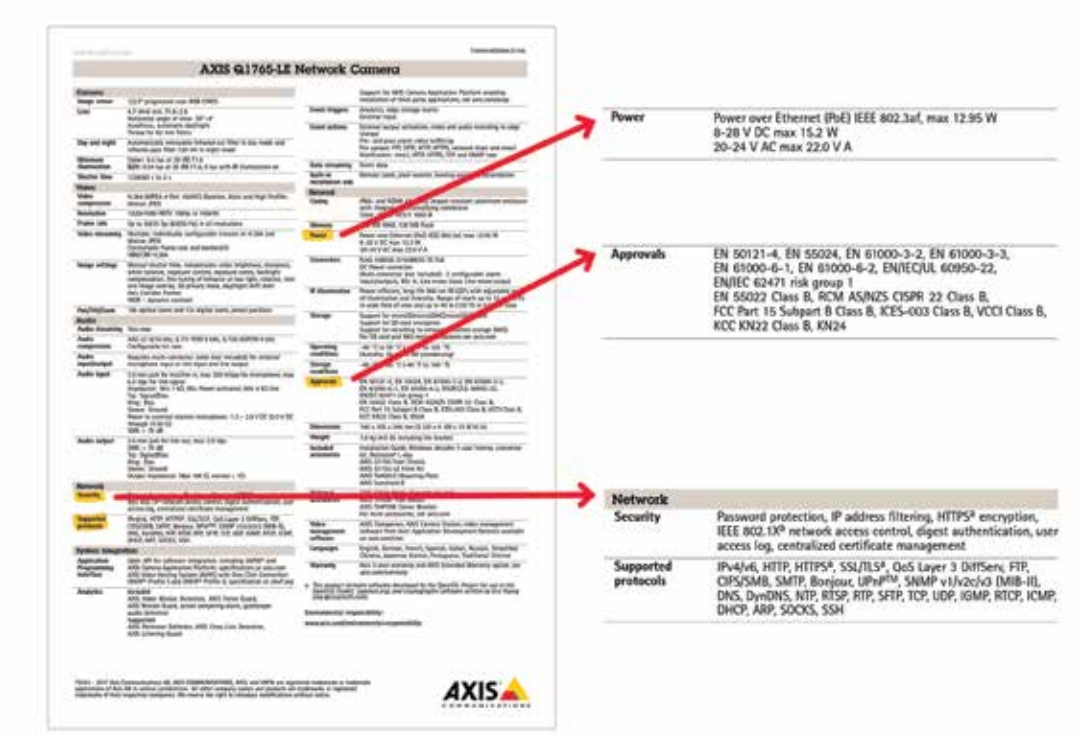

Figure 1. Highlighting the Axis datasheet sections that are in focus of the current document.

2. Approvals

The approvals section in Axis datasheets relates to compliance to various standards. The section is often subdivided into sections for EMC, Safety, Environment, and Other, where "Other" may refer to explosion protection or security in access control. There may also be a subdivision for approvals that concern the midspan, in cases where a midspan is sold with the product.

2.1 EMC (Electromagnetic compatibility)

All network video manufacturers must declare the EMC of their network video products. Under some circumstances manufacturers can self-certify, but most manufacturers use accredited test laboratories that provide a report to verify compliance. EMC approvals are based on two parts, emission and immunity, as below.

Emission refers to the ability of equipment to function satisfactorily without emitting too much electromagnetic energy that can disturb other equipment in that environment.

Immunity is a measure of the ability of electronic products to tolerate the influence of electromagnetic phenomena and electrical energy (radiated or conducted) from other electronic products. In Europe, EMC is included in the CE mark, which in turn is included in the EU's harmonization legislation.

The standards listed below define limits and test methods for electromagnetic emissions and immunity tests. As there is not one test that globally covers compliance, each region/application may have a different code.

2.1.1 Information Technology Equipment (ITE) standards

> EN 55022 Class A: emission standard (commercial, industrial, business), harmonized with international standards

> EN 55022 Class B: emission standard (residential), harmonized with international standards

> EN 55024 Class A: immunity standard (commercial, industrial), harmonized with international standards

> EN 55024 Class B: immunity standard (residential), harmonized with international standards

2.1.2 Harmonized standards by country/region

> EN 61000-6: Generic standards for compliance (Europe)

> FCC Part 15 Subpart B Class A and B: FCC stipulates rules and regulations for telecommunication devices, refer to emission not immunity (United States)

> ICES-003 Class A and B (Canada)

> VCCI (Japan)

> KN22, KN24, KN32, KN35 (Korea)

> CISPR 22 Class A and B (Australia/New Zealand)

2.1.3 Additional standards by application/product

> EN 50121-4, IEC 62236-4: provides performance criteria for signaling and telecommunications apparatus which may interfere with other apparatus in the railway environment.

> EN 50130-4: applies to the components of alarm systems, including: access control systems, CCTV systems, fire detection and fire alarm systems, hold-up alarm systems, intruder alarm systems, social alarm systems.

> EN 55032 (emission) – EN 55035 (immunity): applies to multimedia equipment (MME) having an AC or DC supply voltage not exceeding 600 V. Multimedia equipment (MME) is defined as Information technology equipment (ITE), audio equipment, video equipment, broadcast receiver equipment, entertainment lighting control equipment.

2.2 Safety

> The Low Voltage Directive (2014/35/EU): provides broad objectives for the safety of electrical equipment. Ensures products are safe to use without risk of personal injury or property damage.

> IEC/EN/UL 60950-1: compliance of network cameras, encoders, power supplies to requirements intended to reduce risks of fire, electric shock or injury for the anyone who may come into contact with the equipment.

> IEC/EN/UL 60950-22: specific safety requirements for outdoor products and outdoor enclosures.

> IEC/EN 62471: requirements for exposure limits, prevents hazard to eyes and skin.

> EN 62368-1: replaces EN 60950 standard, but both will co-exist until 2019. IEC and UL developing sister standards with same number.

> EN/UL/CSA 60065: applies to electronic apparatus designed to be fed from the mains, from a supply apparatus, from batteries or from remote power feeding and intended for reception, generation, recording or reproduction respectively of audio, video and associated signals.

2.3 Environment

2.3.1 IP rating

The IEC (International Electrotechnical Commission) standard IEC 60529 defines IP (ingress protection or international protection) ratings as a two-digit code. The code defines the level of protection of electrical appliances against the intrusion of solid objects or dust, accidental contact, and water.

Table 1. IP ratings, first digit (IP**x**x) – foreign solid objects

Level	Protected against	Effective against
0	Not protected	No protection
1	Objects larger than 50 mm	Large surface of the body such as back of the hand, but no protection against deliberate contact with a body part
2	Objects larger than 12.5 mm	Fingers or other objects can penetrate as far as 80 mm assuming it is safe from hazardous parts. Objects with a diameter of 12.5 diameters cannot penetrate fully
3	Objects larger than 2.5 mm	Objects, such as tools and thick wires, cannot penetrate at all
4	Objects larger than 1 mm	Objects, such as wires and screws, cannot penetrate at all
5	Dust protected	Ingress of dust is not completely prevented, but dust does not enter in sufficient quantity to interfere with satisfactory operation of the equipment
6	Dust tight	No ingress of dust

Table 2. IP ratings, second digit (IPx**x**) – liquids

Level	Protected against	Effective against
0	Not protected	No special protection
1	Dripping water	Dripping waters (vertically falling drops) has no harmful effect)
2	Dripping water when tilted up to 15°	Vertically dropping water has no harmful effect when the enclosure is tilted at any angle up to 15° from its normal position
3	Spraying water	Water falling as spray at an angle up to 60° from the vertical has no harmful effect
4	Splashing water	Water splashed against the enclosure from any direction has no harmful effect
5	Water jets	Water projected from a nozzle against the enclosure from any direction has no harmful effect
6	Powerful water jets	Water from heavy seas or water projected in powerful jets cannot enter the enclosure in harmful quantities
7	Brief immersion in water	Ingress of water in a harmful quantity cannot be possible when the enclosure is immersed in water under defined conditions of pressure and time
8	Continuous submersion in water	The equipment is suitable for continuous submersion in water under conditions that shall be specified by the manufacturer. The conditions must be harsher than for IPX7 (see previous)
9	Water from high pressure and steam jet cleaning	Water directed at the housing from any angle under very high pressure has no harmful effect

2.3.2 Other relevant IEC standards

> IEC 60068-2 is a standard for environmental testing of electronic equipment and products to assess their ability to perform under environmental conditions including extreme cold and dry heat. The procedures below in this standard are typically intended for objects that achieve temperature stability during the test procedure.

- IEC 60068-2-1: cold
- IEC 60068-2-2: dry heat
- IEC 60068-2-6: vibration (continuous)
- IEC 60068-2-14: change of temperature
- IEC 60068-2-27: shock
- IEC 60068-2-30: damp heat (cyclic)
- IEC 60068-2-64: vibration (broadband random)
- IEC 60068-2-78: damp heat (steady state)

> IEC 60825 Class I is a standard for ensuring that the kind of laser used in the laser focus module is safe under all conditions of normal use.

2.3.3 NEMA rating

NEMA (National Electrical Manufacturers Association) is a U.S. based association that provides standards for electrical equipment enclosures. NEMA has launched their own standard NEMA 250 worldwide. NEMA has also adopted and published a harmonizing IP standard, ANSI/IEC 60529, through the American National Standards Institute (ANSI).

NEMA 250 addresses ingress protection, but also considers other factors such as corrosion resistance, performance, and construction details. Because of this, NEMA type is comparable to IP, but IP is not comparable to NEMA.

UL standards UL 50 and UL 50E are based on the NEMA 250 standards. NEMA allows self-certification, while UL enforces compliance by demanding that products pass third-party testing and inspection.

Table 3. NEMA ratings for enclosures in non-hazardous locations

NEMA	Equivalent IP rating	Indoor	Outdoor	Protected against
Type 1	IP10	X		Access to hazardous parts and ingress of solid foreign objects (falling dirt). No protection against liquids.
Type 3	IP54	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow). Will be undamaged by the external formation of ice on the enclosure.
Type 3R	IP14	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt). Ingress of water (rain, sleet, snow). Will be undamaged by the external formation of ice on the enclosure.
Type 3S	IP54	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow). The external mechanisms remain operable when ice laden.
Type 4	IP56	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow, splashing water, and hose-directed water). Will be undamaged by the external formation of ice on the enclosure.
NEMA 4X	IP56	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow, splashing water, and hose-directed water). Provides an additional level of protection against corrosion. Will be undamaged by the external formation of ice on the enclosure.
Type 6	IP67	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt). Ingress of water (hose-directed water and the entry of water during occasional temporary submersion at a limited depth). Will be undamaged by the external formation of ice on the enclosure.
Type 6P	IP67	X	X	Access to hazardous parts and ingress of solid foreign objects (falling dirt). Ingress of water (hose-directed water and the entry of water during prolonged submersion at a limited depth). Provides an additional level of protection against corrosion. Will be undamaged by the external formation of ice on the enclosure.
Type 12	IP52	X		Without knockouts. Access to hazardous parts and ingress of solid foreign objects (falling dirt and circulating dust, lint, fibers, and flings). Ingress of water (dripping and light splashing).
Type 12K	IP52	X		With knockouts. Access to hazardous parts and ingress of solid foreign objects (falling dirt and circulating dust, lint, fibers, and flings). Ingress of water (dripping and light splashing).
Type 13	IP54	X		Access to hazardous parts and ingress of sold foreign objects (falling dirt and circulating dust, lint, fibers, and flings.) Ingress of water (dripping and light splashing). Spraying, splashing, and seepage of oil and noncorrosive coolants.

2.3.4 IK rating

IK ratings can be found in IEC/EN 62262, an international standard that specifies degrees of protection against external mechanical impact. Originally approved in 1994 as European standard EN 50102, it was adopted as an international standard in 2002.

Many manufacturers choose to test the weakest part of a product to ensure robustness through the product lifespan.

Table 4. IK ratings

Level	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
Impact energy (Joule)	0.14	0.2	0.35	0.5	0.7	1	2	5	10	20	50*
Mass (kg)	<0.2	<0.2	0.2	0.2	0.2	0.5	0.5	1.7	5	5	
Drop height (mm)	56	80	140	200	280	400	400	300	200	400	

*Impact up to 50 J. Manufacturer must indicate energy, mass, and drop height of striking element.

2.4 Other approvals

2.4.1 Explosion protection

> IEC/EN/UL/SANS/CSA 60079-0: general requirements for construction, testing and marking of Ex equipment and Ex components intended for use in explosive atmospheres.

> IEC/EN/UL/SANS/CSA 60079-1: specific requirements for the construction and testing of electrical equipment with the type of protection flameproof enclosure “d”, intended for use in explosive gas atmospheres.

2.4.2 Approvals for midspan

For the cases where a midspan is included with the product, approvals specifically relating to the midspan are listed in this section of the datasheet. Explanations can be found in the previous sections of the current document.

2.4.3 Security in access control

> UL 294: defines requirements regarding construction, performance, and operation of access control systems.

3. Certifications

When a camera is installed in a potentially explosive environment, the housing must meet very specific safety standards. They should protect the environment from potential igniters from the camera and other equipment.

European products must comply with the ATEX directive, and the corresponding international standard is IECEx. North America mainly uses NEMA's Class/Division ratings over the Zone system described in ATEX and IECEx.

Table 5. Explosion protection ratings

Class / Division	Atmosphere	Definition	Zone (IECEx and ATEX)
Class I / Division 1	Gas	Area in which explosive mixture is continuously present or present for long periods.	Zone 0
Class 1 / Division 1	Gas	Area in which an explosive mixture is likely to occur in normal operation.	Zone 1
Class 1 / Division 2	Gas	Area in which an explosive mixture is not likely to occur in normal operation and if it occurs, will exist only for a short time.	Zone 2
Class II / Division 1	Dust	Area in which explosive mixture is continuously present or present for long periods.	Zone 20
Class II / Division 1	Dust	Area in which an explosive mixture is likely to occur in normal operation.	Zone 21
Class II / Division 2	Dust	Area in which an explosive mixture is not likely to occur in normal operation and if it occurs, it will exist only for a short time.	Zone 22

4. Power

4.1 Power over Ethernet (PoE) classes

PoE classes ensure efficient power distribution by specifying the amount of power that a powered device (PD) will require.

Table 6. PoE classes

Class	Type	Guaranteed power level at Power Sourcing Equipment (PSE)	Maximum power level used by Powered Device (PD)
0	Type 1, 802.3af	15.4 W	0.44 W - 12.95 W
1	Type 1, 802.3af	40.0 W	0.44 W - 3.84 W
2	Type 1, 802.3af	7.0 W	3.84 W - 6.49 W
3	Type 1, 802.3af	15.4 W	6.49 W - 12.95 W
4	Type 2, 802.3at*	30 W	12.95 W - 25.5 W
6	Type 3, 802.3bt	60 W	51 W
8	Type 4, 802.3bt	100 W	71.3 W

*This type is also referred to as PoE+.

5. Network

5.1 Protection and security control

There are several ways to counter threats to system assets. Some threats pose risks to devices while others pose risks to networks or data in transit/storage. A few selected security controls that can be applied to devices and networks:

> Credentials (user/password) protect unauthorized access to video and prevent unauthorized access to device configuration. Having different account privilege levels provides control of who has access to what.

> IP filtering (firewall) reduces the local network exposure of a device and thereby protects it from being accessible to unauthorized clients. This reduces risks in case a device password is compromised and it also mitigates risks in case a new critical vulnerability is discovered.

> 802.1X – protects the network from unauthorized clients. 802.1X is a network infrastructure protection, using managed switches and RADIUS server. The 802.1X client in the device provides authentication to the device on the network.

> HTTPS – (Hypertext transfer protocol secure) – protects data (video) from network eavesdropping. The use of signed certificates in HTTPS provides a way for a video client to detect whether it is accessing a legitimate camera or a malicious computer impersonating a camera.

For access to more cybersecurity resources, see www.axis.com/cybersecurity

5.2 Supported protocols

Many protocols come into play when data is transferred securely from one networked device to another.

5.2.1 Protocol reference models

The best way to understand how the different protocols interact is to examine the Open Systems Interconnection (OSI) communication model. There is also the TCP/IP reference model.

5.2.1.1 OSI reference model

A model that describes data communication between open systems.
To provide a service, each layer utilizes the services of the layer immediately below it.
Each layer must follow certain rules, or protocols, to perform services.

Layer 7 – Application
Makes functions such as web, file, and email transfer available to applications.

Examples
> File Transfer Protocol (FTP)
> Simple Mail Transfer Protocol (SMTP)
> Hypertext Transfer Protocol (HTTP)

Actual applications, such as web browsers or email programs, exist above this layer and are not covered by the OSI model.

Layer 6 – Presentation (Data)
Ensures that data sent by the application layer of a system can be read by the application later of another system. Converts system-dependent data formats, such as ASCII, into an independent format, permitting syntactically correct data exchange between different systems.

Examples
> Telnet
> Apple Filing Protocol

Layer 5 – Session (Persistent connection between peer hosts)
Provides an application-oriented service and takes acre of the process communication between two systems. Process communication begins with the establishment of a session, which provides the basis for a virtual connection between two systems.

Examples
> Remote Procedure Call
> Network File System

Layer 4 – Transport (End-to-end transport (connection-oriented protocol))
Provides reliable data transfer service (through flow control and error control) to Layer 5 and above.

Examples:
> Transmission Control Protocol (TCP)
> User Datagram Protocol (UDP)

Layer 3 – Network (Packet (addressing / fragmentation))
Performs the actual data transfer, by routing and forwarding data packets between systems. Creates and administrates routing tables and provides options for communicating beyond network boundaries. Data in this layer are assigned destination and source addresses, which are used as the basis for targeted routing.

Examples
> IP (Internet Protocol) – an individual public address necessary for Internet-enabled devices to communicate
> IPv4 – original version of the IP, uses 32-bit addresses
> IPv6 – most recent version of the IP, uses 128-bit addresses that are divided into eight groups of four hexadecimal digits
> Routing Information Protocol
> Internet Protocol Security (IPSec)

Layer 2 – Data Link (Frames)
Provides data transmission and controls access to the transmission medium, by combining data into units known as frames. Layer 2 is divided into two sublayers, upper range corresponding to Logical Link Control (LLC) and the lower part corresponding to the media access control (MAC). LLC simplifies data exchange, while MAC controls access to the transmission medium.

Examples
> IEEE 802.2 (LLC)
> IEEE 802.3 (Ethernet MAC)
> 802.11 (WLAN MAC)

Layer 1 – Physical (Bits)
Provides services that support the transmission of data as a bitstream over a medium, such as a wired or wireless transmission link.

5.2.1.2 Transmission Control Protocol/Internet Protocol Reference Model

TCP/IP reference model is another model used to understand protocols and how communication takes place. The TCP/IP reference model falls into four different layers which correspond to the OSI reference model as below.

Table 7. Reference models comparison

OSI model	TCP/IP model
Layer 7 - Application	Layer 4 - Application
Layer 6 - Presentation	
Layer 5 - Session	
Layer 4 - Transport	Layer 3 - Transport
Layer 3 - Network	Layer 2 - Internetwork
Layer 2 - Data Link	Layer 1 - Network Interface
Layer 1 - Physical	

5.2.2 Protocols for managing IP addresses

DHCP (Dynamic Host Configuration Protocol) – automatic assignment and management of IP addresses

DNS (Domain Name System) – converts domain names into their associated IP address, operates on the transport layer

DynDNS (Dynamic Domain Name System) – is used to keep track of a domain name's link to changing IPv4 addresses

UPnP (Universal Plug and Play) – Microsoft operating systems can automatically detect resources (Axis device) on a network.

Zeroconf – automatically allocates a network device to an unused IP address from the range of 169.254.1.0 to 169.254.254.255

Bonjour – can be used to discover network video products using Mac computers, or as a discovery protocol for new devices in any network.

ARP (Address Resolution Protocol) – is used to discover the MAC address of the destination host.

5.2.3 Application level protocols

HTTP (Hypertext Transfer Protocol) – primarily used to load text and images from a website to web browser. Network video systems provide an HTTP server service that permits access to the systems through web browsers, for downloading configurations or live images.

HTTPS (HTTP Secure) – an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network and is widely used on the Internet. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS).

FTP (File Transfer Protocol) – primarily used to transmit files from a server to a client (download) or from a client to a server (upload). Can also be used to create and select directories and rename or delete directories and files.

RTP (Real-Time Transport Protocol) – permits the transfer of real-time data between system endpoints.

RTCP (Real-Time Control Protocol) – provides out-of-band statistics and control information for an RTP session. It partners with RTP in the delivery and packaging of multimedia data but does not transport any media data itself.

RTSP (Real-Time Streaming Protocol) – extended control over the transmission of real-time media.

SMTP (Simple Mail Transfer Protocol) – the standard for transferring email over the internet. Network cameras support SMTP to allow the sending of email alerts.

SNMP (Simple Network Management Protocol) – used to remotely monitor and manage networked equipment such as switches, routers, and network cameras. SNMP support allows network cameras to be managed by open source tools.

SIP (Session Initiation Protocol) – communication protocol for signaling and controlling multi-media communications sessions.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) – negotiates a private, reliable connection between the client and the server. SSL was the predecessor to TLS, which is the common standard.

LLDP (Link Layer Discovery Protocol) – used in to advertise a device's identity and abilities, as well as other devices connected within the same network.

CIFS/SMB (Common Internet File System/Server Message Block) – mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.

NTP (Network Time Protocol) – used to synchronize the time of a computer client or server to another server.

SFTP (Secure File Transfer Protocol) – provides file access, file transfer, and file management over any reliable data stream.

IGMP (Internet Group Management Protocol) – used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships, allows more efficient use of resources when supporting these types of applications.

5.2.4 Data transport protocols

TCP (Transmission control protocol) – connection-oriented, reliable, and in-order delivery of data streams. Most common protocol for data transport.

UDP (User Datagram Protocol) – connectionless transmission service, favors timely delivery of data over reliability.

ICMP (Internet Control Message Protocol) – send error messages and operational information indicating that a requested service is not available or that a host or router could not be reached.

5.2.5 Unicast, broadcast, and multicast

There are three different methods for transmitting data on a computer network.

Unicast – most common, sender and recipient communicate on a point-to-point basis. Data packers are sent only to one recipient, and no other clients will receive that information.

Multicast – communication between a single sender and multiple receivers on a network. Reduces network traffic by delivering a single stream of information to many recipients.

Broadcast – sender sends the same information to all other servers on a network, all hosts on the network receive the message and will process it to some extent.

5.2.6 Quality of Service

In an IP Network it is necessary to control how network resources are shared to fulfill the requirements of each service.

QoS (Quality of Service) – ability to prioritize network traffic so that critical flows can be served before flows with less priority. Greater reliability in a network by controlling the amount of bandwidth an application can use and providing the ability to control bandwidth competition between applications.

DiffServ – network tries to deliver a specific service based on the QoS specified by each packet.

72900/EN/R1/1902

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 3,000 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.

AXIS COMMUNICATIONS