

WHITE PAPER

Quick guide to Axis datasheets

Approvals, certifications, and protocols

October 2023

Table of Contents

1	Introduction	3
2	Approvals	3
	2.1 EMC (Electromagnetic compatibility)	3
	2.2 Safety	4
	2.3 Environment	5
	2.4 Other approvals	9
3	Certifications	9
4	Power	10
	4.1 Power over Ethernet (PoE) classes	10
5	Network	11
	5.1 Protection and security control	11
	5.2 Supported protocols	12

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 short descriptions of acronyms, approvals, certifications, and protocols found therein.

This document provides information about the datasheet sections that are highlighted and zoomed in below.

AXIS P5654-E PTZ Network Camera	
Model	AXIS P5654-E 60 Hz AXIS P5654-E 60 Hz
Image sensor	1/2.8" progressive scan RGB CMOS
Lens	Varifocal, 4.0-84.8 mm, F1.6 - 4.5 Horizontal field of view: 77.0° - 1.8° Vertical field of view: 43.1° - 2.0° Autofocus and auto-iris
Day and night	Automatically removable infrared-cut filter
Minimum illumination	Color: 0.1 lux at 30 IR1 F1.6 BW: 0.03 lux at 30 IR1 F1.6 BW: 0.01 lux at 30 IR1 F1.6
Shutter speed	1/60000 to 2 s
Pan/Tilt/Zoom	Pan: 180° endless, 0.1° - 360°/s Tilt: 180° - 0.1° - 360°/s Zoom: 21x optical, 12x digital, total 252x zoom 25x preset position, 4x-16x limited guard band control zones, on-screen directional indicators, set new pan 0°, focus window, focus reset
System on Chip (SoC)	
Model	ARMv7-C
Memory	1024 MB RAM, 512 MB Flash
Compute capabilities	Machine learning processing unit (MLPU)
Video	
Video compression	H.264 (MP@L Part 10/AVC) Baseline, Main and High Profiles H.265 (MP@L/H Part 10/AVC) Main Profile Motion JPEG
Resolution	1280x720 HDV, 720p to 320x180
Frame rate	Up to 60FPS for 1080p HD in all resolutions
Video streaming	Multiple, individually configurable streams in H.264, H.265 and Motion JPEG Controllable frame rate and bandwidth Axis Streamer technology in H.264 and H.265 VBR/ABR/MBR H.264/H.265
Image settings	Compression, saturation, brightness, sharpness, contrast, local contrast, white balance, exposure control, exposure zones, Forensic WDR: Up to 120 dB depending on scene, deblurring, day/night level, scene mapping, freezing of low-light behavior, rotation: 0°, 180°, lens and image overlay, image freeze on PTZ, electronic image stabilization, scene profiles, 20 individual polygon privacy masks
Network	
Security	Secure operations: IPsec, TLS, HTTPS, SSI/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTP, SRTP, TCP, UDP, ICMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, NTP, LLDP, CDP, MQTT v3.1.1, Syslog
Supported protocols	IPsec, TLS, HTTPS, SSI/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTP, SRTP, TCP, UDP, ICMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, NTP, LLDP, CDP, MQTT v3.1.1, Syslog
System integration	Open API for software integration, including VAPIP and AXIS Camera Application Platform, specifications at axis.com
Application Programming Interface	ONVIF Profile 1, ONVIF Profile S, and ONVIF Profile T, specifications at onvif.org
Event conditions	Device status: Above operating temperature, Above or below operating temperature, Below operating temperature, Fan failure, IP address removed, Network lost, New IP address, Shock detected, Storage failure, System ready, Within operating temperature, Edge storage, Streaming ongoing, Storage disjunction I/O: Manual trigger, Virtual Input PTZ: PTZ malfunctioning, PTZ movement: Camera 1, PTZ preset position reached, Camera 1, PTZ ready Scheduled and recurring: Scheduled event
Event actions	Day-night mode, go to preset position, guard tour, upload of images or video files via FTP, SFTP, HTTP, network share and email, notification to email, HTTP, HTTPS, TCP and SNMP trap, notify text, pushover text, record video to SD card and network share, WDR mode
Data streaming	Event data
Service installation aids	Fast connector
Identifiers	
AXIS Object Analytics	Object classes: humans, vehicles Trigger conditions: line crossing, object in area Up to 10 scenarios Markers visualized with color-coded bounding boxes Panorama include/exclude areas Perspective configuration ONVIF Motion Alarm event
Applications	Included AXIS Object Analytics AXIS Video Motion Detection, advanced antipeeper, auto tracker 2 Support for AXIS Camera Application Platform enabling installation of third-party applications, see axis.com/ocap
Casing	IP66, NEMA 4X and R10 Aluminum casting, polycarbonate (PC) dome Color: anodized PC: 3, 7000-B, repairable slide cover For mounting instructions of casing and impact on warranty, see your site partner
Sustainability	PVC free AXIS PoE+ midspan 1-port: 100-240 V AC, max 37 W IEE 802.3at, Type 2 Class 4 Camera consumption: typical 8 W, max 16 W (PoE+ midspan not included)
Connectors	RJ45 10BASE-T/100BASE-TX I/O RJ45 push-pull connector (PoE not included) Support for SD/SDHC/SDXC card Support for SD card encryption (AES-128/256bit) Recording to network-attached storage (NAS) For SD card and NAS recommendations see axis.com
Operating conditions	+20 °C to +50 °C (68 °F to 122 °F) Maximum ambient temperature +55 °C Humidity: 5-95% RH (non-condensing)
Storage conditions	-40 °C to 65 °C (-40 °F to 149 °F) Humidity: 5-95% RH (non-condensing)
Approvals	EMC EN 55022, EN 55024, EN 61010-1, EN 61010-2-1 EN 55022-3-2, EN 55022-3-3, EN 61010-2-2, EN 61010-2-3 FCC Part 15 Subpart B Class A, ICES-3A/INM-3A/IEC 62236-4, ICES-3B Class A, ICES-3B, ICES-3B/INM-3B/IEC 62236-4, VCCI Class A Safety IEC/EN 62368-1, IEC/EN/UL 60950-22, IS 13252 Environment IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP66, IEC/EN 62262 IK10, NEMA 250 Type 4X Network NIST SP500-267, IPv6 USGv6
Power	AXIS PoE+ midspan 1-port: 100-240 V AC, max 37 W IEEE 802.3at, Type 2 Class 4 Camera consumption: typical 8 W, max 16 W (PoE+ midspan not included)
Approvals	EMC EN 50121-4, EN 55024, EN 55032 Class A, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-3A/INM-3A/IEC 62236-4, KCC KN32 Class A, KC KN35, RCM AS/NZS CISPR 32 Class A, VCCI Class A Safety IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IS 13252 Environment IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP66, IEC/EN 62262 IK10, NEMA 250 Type 4X Network NIST SP500-267, IPv6 USGv6
Network Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware, secure boot
Supported protocols	IPv4, IPv6, USGv6, HTTP, HTTP/2, HTTPS, SSI/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTP, SRTP, TCP, UDP, ICMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, NTP, LLDP, CDP, MQTT v3.1.1, Syslog
Dimensions	Height: 217 mm (8 1/2 in) ø 188 mm (7 3/8 in)
Weight	2.8 kg (6.5 lb)
Included accessories	RJ45 Push-Pull Connector (RJ45), Hard ceiling mount, Spring pipe adapter, U-profile pipe adapter, Installation Guide, Windows® decoder 1-year license, AXIS Authentication key, anodized dome
Optional accessories	AXIS 1938 mount, AXIS 1942SD recessed mount, outdoor RJ45 cable with pre-terminated connectors, AXIS 19123 Midspan 30 W 1-port, repairable slide cover For more accessories, see axis.com

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

2 Approvals

The approvals section in Axis datasheets relates to compliance to various standards. The section is usually divided into subsections for EMC, Safety, Environment, Network, and Other, where "Other" may refer to explosion protection or security in access control. There can also be a subsection 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.

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 covers compliance globally, there can be different codes for different regions or applications.

2.1.1 Information Technology Equipment (ITE) standards

These standards apply to multimedia equipment (MME) that has 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, and entertainment lighting control equipment.

- EN 55032 Class A: emission standard (commercial, industrial, business), harmonized with international standards
- EN 55032 Class B: emission standard (residential), harmonized with international standards
- EN 55035: immunity standard, harmonized with international standards

2.1.2 Harmonized standards by country/region

- EN 61000-6-1 and EN 61000-6-2: generic standards for compliance (Europe)
- FCC Part 15 Subpart B Class A and B: FCC stipulates rules and regulations for telecommunication devices, referring to emission, not immunity (United States)
- ICES-3(A and B)/NMB-3(A and B) (Canada)
- VCCI Class A and B (Japan)
- KS C 9832 Class A and B, KS C 9835, KS C 9547, KS C 9815 (Korea)
- RCM AS/NZS CISPR 32 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 50121-3-2: Applies to the electromagnetic compatibility, i.e., immunity and emission requirements, of electrical and electronic apparatus used on railway applications.

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 62368-1: compliance of network cameras, encoders, power supplies to requirements intended to reduce risks of fire, electric shock or injury for anyone who might come into contact with the equipment. This safety requirement applies to both indoor and outdoor equipment.

- IEC/EN 62471-1: photobiological safety of lamps and lamp systems requirements for exposure limits, prevents hazard to eyes and skin
- IS 13252: India specific compliance of network cameras, encoders, power supplies to requirements intended to reduce risks of fire, electric shock or injury for anyone who might come into contact with the equipment
- UN ECE R118: ensures fire safety through specific standards requirements for equipments used and mounted in vehicles.
- EN 45545-2: This standard ensures that materials and components used on railway applications meet specific fire behavior requirements. It includes several test procedures that are determined by the type of train, application, and positioning (exterior or interior).
- NFPA 130.: fire safety standard for rolling stock in the United States, ensuring safety standard requirements for rail systems, including stations, vehicles, emergency procedures, communication systems, and trainways.
- NOM-001-SCFI-2018: safety requirements and test methods for electronic equipment that are manufactured, imported, sold, or distributed in Mexico.
- CSA/UL 62368-1:2019: safety standard for electrical and electronic audio, video, or information and communication technology equipment, that has a maximum voltage of 600 V.

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 2.1 IP ratings - the first digit after IP: 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 mm 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 2.2 IP ratings - the second digit after IP: liquids

Level	Protected against	Effective against
0	Not protected	No special protection
1	Dripping water	Dripping water (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	Protection against hot water with high pressure	Water directed at the housing from any angle with high temperature and under very high pressure has no harmful effect.

2.3.2 Other relevant standards

- IEC 60068-2: 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 60068-2-64: vibration (broadband random)
 - IEC 60068-2-78: damp heat (steady state)
- IEC 60825 Class I: A standard for ensuring that the kind of laser used in the laser focus module is safe under all conditions of normal use.
- IEC TR 60721-3-5: classifies the environmental conditions of products that are installed in a ground vehicle but not part of the vehicle. Products such as communication systems, radios, and fare meters.

- EN 50155: A standard for railway applications ensuring the safety, design, and operation of electronic equipment installed on rail vehicles, within scopes like temperature and humidity.
- EN 61373: A standard for shock and vibration testing of rolling stock equipment used on railway applications. It assesses the adequacy and capability of equipment to withstand vibrations and shock, due to the railway operating environment.
- MIL-STD-810H: A standard for products' assessment ensuring they can withstand environmental conditions such as vibration, shock, humidity, dust, and low and high temperatures. The methods below are recreated to imitate the various environmental conditions.
 - 501.7: High Temperature
 - 502.7: Low Temperature
 - 505.7: Solar Radiation
 - 506.6: Rain
 - 507.6: Humidity
 - 509.7: Salt Fog
 - 512.6: Immersion

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 2.3 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.

Table 2.3. NEMA ratings for enclosures in non-hazardous locations (Continued)

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 hosedirected water). Will be undamaged by the external formation of ice on the enclosure.
Type 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 hosedirected 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.

NEMA TS 2 is a design guide that applies to traffic signaling equipment.

- NEMA TS 2–2.2.7 Test Procedure: Transients, Temperature, Voltage, and Humidity
- NEMA TS 2–2.2.8 Vibration Test
- NEMA TS 2–2.2.9 Shock (Impact) Test

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.

Level	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK11*
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.

For a more complete list of standards and regulations for explosion protection, see certifications *here*

2.4.2 Approvals for midspans

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 the Class/Division ratings by NFPA70 (National Electric Code, NEC) and CSA C22.1 (Canadian Electric Code, CEC) over the Zone system described in ATEX and IECEx.

Table 3.1 Certifications

Regulation / Certification	Region / Country
ATEX	EU
CCC Ex	China
cMETus / cULus	Canada and USA
IA Certification	South Africa
IECEX	International certification of equipment used in hazardous areas
INMETRO	Brazil
JPEX	Japan
KCs	Korea
OSHA Taiwan	Taiwan
PESO	India

Table 3.2 Explosion protection ratings

Class / Division	Atmos- phere	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 I / Division 1	Gas	Area in which an explosive mixture is likely to occur in normal operation.	Zone 1
Class I / 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 4.1 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 3, 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 address 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.
- IEEE 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.
- Signed firmware: is implemented by the software vendor signing the firmware image with a private key, which is secret. When firmware has this signature attached to it, a device will validate the firmware before accepting and installing it. If the device detects that the firmware integrity is compromised, it will reject the firmware upgrade. Axis signed firmware is based on the industry-accepted RSA public-key encryption method.
- Secure boot: a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on signed firmware, secure boot ensures that a device can boot only with authorized firmware. Secure boot guarantees that the Axis device is completely clean from possible malware after resetting to factory default.

- **TPM:** A trusted platform module is a component that provides a set of cryptographic features suitable for protecting information from unauthorized access. The private key is stored in the TPM and never leaves the TPM. All cryptographic operations requiring the use of the private key are sent to the TPM to be processed. This ensures that the secret part of the certificate remains safe even in the event of a security breach.
- **Axis Edge Vault:** a secure cryptographic compute module (secure module or secure element) in which the Axis device ID is securely and permanently installed and stored.

For access to more cybersecurity resources, see 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.

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 layer of another system. Converts system-dependent data formats, such as ASCII, into an independent format, permitting syntactically correct data exchange between different systems.

Layer 5 – Session (Persistent connection between peer hosts)

Provides an application-oriented service and takes care 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.

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.

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.

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.

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 5.1 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 Application layer protocols

- **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.
- **DDNS** (Dynamic Domain Name System): is used to keep track of a domain name's link to changing IPv4 addresses.
- **DHCPv4/v6** (Dynamic Host Configuration Protocol): automatic assignment and management of IP addresses.
- **DNS/DNSv6** (Domain Name System): converts domain names into their associated IP address.
- **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.
- **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.
- **HTTP/2**: a major revision to the HTTP protocol defined in RFC 7540 and released in February 2015.

- **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).
- **MQTT (Message Queuing Telemetry Transport):** a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth.
- **NTP (Network Time Protocol):** used to synchronize the time of a computer client or server to another server.
- **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.
- **SFTP (Secure File Transfer Protocol):** provides file access, file transfer, and file management over any reliable data stream.
- **SIP (Session Initiation Protocol):** communication protocol for signaling and controlling multi-media communications sessions.
- **SIPS (Session Initiation Protocol Secure):** encrypted version of SIP.
- **SMTP (Simple Mail Transfer Protocol):** the standard for transferring email over the internet. Network cameras support SMTP to allow the sending of email alerts.
- **SNMPv1/v2/v3 (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.
- **SOCKS:** permits the transfer of network packets between clients and servers through a remote network proxy.
- **SRTP (Secure Real-Time Transport Protocol):** permits encrypted transfer of real-time data between system endpoints, and is therefore a secure variant of RTP.
- **SSH (Secure Shell):** permits management and debug access to network devices securely over an unsecured network.
- **TLSv1.2/v1.3 (Transport Layer Security):** negotiates a private, reliable connection between the client and the server.

5.2.3 Transport layer 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.

5.2.4 Network layer protocols

- **IGMPv1/v2/v3** (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.
- **IPv4/IPv6** (Internet Protocol): an individual public address necessary for internet-enabled devices to communicate. IPv4 is the original version, and it uses 32-bit addresses. IPv6 is the most recent version, and it uses 128-bit addresses that are divided into eight groups of four hexadecimal digits.
- **USGv6**: a technical standards profile for IPv6 defined by the US Government to ensure compatibility when procuring IPv6 enabled network devices.

5.2.5 Data Link layer protocols

- **ARP** (Address Resolution Protocol): is used to discover the MAC address of the destination host.
- **CDP** (Cisco Discovery Protocol): proprietary Cisco protocol used as an alternative to LLDP for discovering information about connected hardware devices.
- **IEEE 802.3 (i, u, ab)**: standards for Ethernet defining 10Mb/s (10Base-T), 100Mb/s (100Base-TX), and 1Gb/s (1000Base-T) data communication over twisted pair cabling.
- **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.

5.2.6 Discovery protocols

- **mDNS (Bonjour)**: can be used to discover network video products using Mac computers, or as a discovery protocol for new devices in any network.
- **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.

5.2.7 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.

5.2.8 Data transmission methods

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 packets 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.

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