

백서

# Axis 데이터시트 퀵 가이드

승인, 인증, 프로토콜

10월 2023

# 목차

<b>1</b>	<b>서론</b>	<b>3</b>
<b>2</b>	<b>승인</b>	<b>3</b>
	2.1 EMC (전자기 적합성)	3
	2.2 안전	4
	2.3 환경	5
	2.4 기타 승인	9
<b>3</b>	<b>인증</b>	<b>9</b>
<b>4</b>	<b>전원</b>	<b>11</b>
	4.1 PoE(Power over Ethernet) class	11
<b>5</b>	<b>네트워크</b>	<b>11</b>
	5.1 보호 및 보안 컨트롤	11
	5.2 지원되는 프로토콜	12

# 1 서론

Axis Communications는 시장에 출시된 모든 제품에 대해 해당 업계 표준 및 준수 표준을 충실히 지키고 있습니다. 이 문서는 Axis 데이터 시트에 있는 약어, 승인, 인증 및 프로토콜에 대한 정의와 간략한 설명을 보완합니다.

이 문서는 아래에서 강조 표시되고 확대된 데이터시트 섹션에 대한 정보를 제공합니다.

AXIS P5654-E PTZ Network Camera	
<b>Models</b> AXIS P5654-E 50 Hz AXIS P5654-E 60 Hz	<b>Video</b> Day-night mode. Live stream open Day-night mode: go to preset position, guard line without of images or video clips via FTP, SFTP, HTTP, HTTPS, network share and email. Indicators on email, HTTP, HTTPS, TCP and SFTP trace, overlay text, prioritized text, record video to SD card and network share, WDR mode
<b>Camera</b> 1/2.8" progressive scan CMOS	<b>Event actions</b> Event data Built-in Installation aids
<b>Lens</b> Variable: 4.5-84 mm F1.6 - 4.5 Horizontal field of view: 77.0° - 3.8° Vertical field of view: 43.1° - 2.6° Autofocus and auto-iris	<b>Analytics</b> Object classes: humans, vehicles Trigger conditions: line crossing, object in area Up to 10 scenarios Metadata visualized with color-coded bounding boxes Polygon include/exclude areas Persistent configuration ONVIF Motion Alarm event
<b>Day and night</b> Automatically removable infrared-cut filter <b>Illumination</b> Color: 0.1 lux at 30 IR F1.6 BW: 0.01 lux at 30 IR F1.6 BW: 0.01 lux at 30 IR F1.6	<b>Applications</b> Industrial AXIS Object Analytics AXIS Video Motion Detection, advanced gatekeeper, autostracker 2 Support for AXIS Camera Application Platform enabling installation of third-party applications, see axis.com/comp
<b>Shutter speed</b> 1/6000.0 to 1"	<b>General</b> Case: IP66, NEMA 4X and X10 Aluminum grade polycarbonate (PC) dome Color: white, NCS S 1003-B, repairable skin cover For additional instructions of casing and impact on warranty, visit your Axis partner.
<b>Pan/tilt/zoom</b> Pan: 360° endless, 0.1° - 360°/s Tilt: 180°, 0.1° - 360°/s Zoom: 24x optical, 24x digital, Total 252x zoom 256 preset positions, e-tilt, limited guard tour control queue, on-screen directional indicators, set new pan/tilt/zoom window, focus recall	<b>Power</b> 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)
<b>Systems on Chip (SoC)</b> Model Memory 1024 MB RAM, 512 MB Flash Machine learning processing unit (MLPU)	<b>Connects</b> SAS: SAS/SAS2/SAS3/SAS4/SAS5 RJ45 push-pull connector (RJ45) included Support for SD/MSD/CF/SDXC card Support for SD card encryption (AES-XTS, P256/A4 256bit) Recording to network-attached storage (NAS) For SD card and NAS recommendations, see axis.com
<b>Video compression</b> H.264 (H.264 Part 10/AVC) Baseline, Main and High Profiles H.265 (H.265 Part 2/HEVC) Main Profile Motion JPEG	<b>Operating conditions</b> Maximum permitted temperature: +55°C Humidity: 0 - 100% RH (condensing) -20°C to 60°C (4°F to 140°F) Salt-crystallization: 5-50% RH (non-condensing)
<b>Resolution</b> 1280x720 HDV 750p to 320x180	<b>Storage conditions</b> EMC EN 50121-4, EN 55024, EN 55032 Class A, EN 61000-3-3, EN 61000-3-1, EN 61000-6-1, EN 61000-6-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-003/NMB-3(A), IEC 62236-4, IEC KN32 Class A, KC KN35, RCM AS/NZS CISPR 32 Class A, VCCI Class A <b>Safety</b> IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IS 13252 <b>Environment</b> IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, EC 60068-2-78, IEC/EN 60529 IP66, IEC/EN 62262 IK10, NEMA 250 Type 4X <b>Network</b> NIST SP800-267, IPv6 USv6
<b>Frame rate</b> Up to 60 FPS (60 FPS Hz) in all resolutions	<b>Dimensions</b> Height: 217 mm (8 1/2 in.) ø 118 mm (4 1/2 in.)
<b>Video streaming</b> Multiple, individually configurable streams in H.264, H.265 and Motion JPEG Compatible frame size and bandwidth Axis Zoomstream technology in H.264 and H.265 VFR/AFR/MFR 1/2/3/4/5/6	<b>Weight</b> 2.5 kg (5.5 lb)
<b>Image settings</b> Compression, saturation, brightness, sharpness, contrast, local contrast, white balance, exposure control, exposure zones, Forensic WDR, Up to 120 dB (depending on scene, debugging, day/night shift level, tone mapping, the tuning of low-light behavior, rotation 0°, 180°, flip and image overlay, image freeze on PTZ, electronic image stabilization, scene profiles, 20 individual on/off primary modes	<b>Optional accessories</b> AXIS T818 mounts, AXIS T84022, network mount, outdoor RJ45 cable with pre-mounted connector, AXIS T8122 Midspan 20 W 1-port, repairable skin cover For more accessories, see axis.com
<b>Network</b> <b>Security</b> Hardware processor-based encryption (AES-256) IEEE 802.1X network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware, secure boot	<b>Supported protocols</b> IPV4, IPV6 USv6, HTTP, HTTPS, HTTPS SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMPv1/v2/v3, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, NTCP, LLDP, CDP, MQTT v3.1.1, Syslog
<b>Supported protocols</b> IPV4, IPV6 USv6, HTTP, HTTPS, HTTPS SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, NTCP, LLDP, CDP, MQTT v3.1.1, Syslog	<b>Event conditions</b> Device status: Allow operating temperature. Allow or below operating temperature. Allow or below operating temperature. Low operating temperature. Low failure, IP address renewal, Network loss, New IP address, Check detected, Storage failure, System ready, Window operating temperature, Edge storage, Recording ongoing, Storage dislocation I/O: Manual trigger, Visual input PTZ: PTZ malfunctioning, PTZ movement: Camera 1, PTZ preset position reached: Camera 1, PTZ ready Scheduled and recurring: Scheduled event

Figure 1. 이 문서에서 중점을 두고 있는 Axis 데이터 시트 섹션 강조 표시.

# 2 승인

Axis 데이터 시트의 승인 섹션은 다양한 표준의 준수에 관한 것입니다. 이 섹션은 일반적으로 EMC, 안전, 환경, 네트워크 및 기타의 하위 섹션으로 나뉘며, "기타"는 방폭 또는 접근 제어의 보안을 의미하는 것일 수 있습니다. 또한 미드스팬이 제품과 함께 판매되는 경우, 미드스팬 승인과 관련된 하위 섹션이 있을 수 있습니다.

## 2.1 EMC (전자기 적합성)

모든 네트워크 비디오 제조업체는 네트워크 비디오 제품의 EMC를 명시해야 합니다. 경우에 따라 제조업체는 자체 인증을 할 수 있지만 대부분의 제조업체는 규정 준수를 확인하기 위해 보고서를 제공하는 공인 시험 검사소를 사용합니다. EMC 승인은 방사량과 내성이라는 두 부분을 기반으로 합니다.

방사량은 주변의 다른 장비를 방해할 수 있는 전자기 에너지를 너무 많이 방출하지 않고도 만족스럽게 작동하는 장비의 성능을 나타냅니다.

내성은 전자 제품이 다른 전자 제품의 전자기 현상 및 전기 에너지(방사 또는 전도) 영향을 견딜 수 있는 능력을 측정한 것입니다. 유럽에서는 EMC가 CE 마크에 포함되어 있습니다. 즉, EU의 조화 법령에 포함됩니다.

아래에 있는 표준은 전자기 방사량과 내성 시험에 대한 한계와 시험 방법을 정의합니다. 전 세계적으로 규정 준수를 다루는 단일한 시험이 없기 때문에 지역이나 응용 분야에 따라 규정이 다를 수 있습니다.

### 2.1.1 정보 기술 장비(ITE) 표준

이 표준은 AC 또는 DC 공급 전압이 600V를 초과하지 않는 멀티미디어 장비(MME)에 적용됩니다. 멀티미디어 장비(MME)는 정보 기술 장비(ITE), 오디오 장비, 비디오 장비, 방송 수신기 장비 및 엔터테인먼트 조명 제어 장비로 정의됩니다.

- EN 55032 Class A: 방사량 표준(상업, 산업, 업무), 국제 표준과 조화를 이룸
- EN 55032 Class B: 방사량 표준(거주), 국제 표준과 조화를 이룸
- EN 55035: 국제 표준과 조화를 이루는 내성 표준

### 2.1.2 국가/지역별 표준

- EN 61000-6-1 및 EN 61000-6-2: 적합성에 대한 일반 표준(유럽)
- FCC Part 15 Subpart B Class A 및 B: FCC에는 전기 통신 기기의 내성이 아닌 방사량에 대한 규칙 및 규정이 명시되어 있습니다(미국).
- ICES-3(A 및 B)/NMB-3(A 및 B)(캐나다)
- VCCI Class A 및 B(일본)
- KS C 9832 A종 및 B종, KS C 9835, KS C 9547, KS C 9815(한국)
- RCM AS/NZS CISPR 32 Class A 및 B(호주/뉴질랜드)

### 2.1.3 애플리케이션/제품별 추가 표준

- EN 50121-4, IEC 62236-4: 철도 환경에서 다른 장치를 방해할 수 있는 신호 및 통신 기기에 대한 성능 기준을 제공합니다.
- EN 50130-4: 접근 제어 시스템, CCTV 시스템, 화재 감지 및 화재 알람 시스템, 홀드 업 알람 시스템, 침입자 알람 시스템, 사회 알람 시스템 등의 알람 시스템 구성 요소에 적용됩니다.
- EN 50121-3-2: 철도 애플리케이션에 사용되는 전기 및 전자 장치의 전자파 적합성, 즉 전자파 내성 및 방출 요구 사항에 적용됩니다.

## 2.2 안전

- The Low Voltage Directive(2014/35/EU): 전기 장비의 안전을 위해 광범위한 목표를 제공합니다. 개인 상해 또는 재산 피해 없이 제품을 안전하게 사용할 수 있는지 확인합니다.

- IEC/EN/UL 62368-1: 네트워크 카메라, 엔코더, 전원 공급 장치의 화재 위험, 감전 위험 또는 장비와 접촉할 수 있는 사람의 부상 위험을 줄이기 위한 요구 사항의 준수. 이 안전 요구 사항은 실내 및 실외 장비 모두에 적용됩니다.
- IEC/EN 62471-1: 램프의 광생물학적 안전 및 노출 제한에 대한 램프 시스템 요구 사항, 눈과 피부에 대한 위험 방지
- IS 13252: 네트워크 카메라, 엔코더, 전원 공급 장치의 화재, 감전 또는 장비와 접촉할 수 있는 사람의 부상 위험을 줄이기 위한 요구 사항의 준수(인도).
- UN ECE R118: 차량에 사용 및 장착되는 장비에 대한 특정 표준 요구 사항을 통해 화재 안전을 보장합니다.
- EN 45545-2: 이 표준은 철도 애플리케이션에 사용되는 소재 및 부품이 특정 화재 행동 요구 사항을 충족하도록 보장합니다. 여기에는 열차 유형, 애플리케이션 및 위치(외부 또는 내부)에 따라 결정되는 몇 가지 시험 절차가 포함되어 있습니다.
- NFPA 130.: 미국의 철도 차량에 대한 화재 안전 표준으로, 역, 차량, 비상 절차, 통신 시스템, 선로 등의 철도 시스템에 대한 안전 표준 요구 사항을 보장합니다.
- NOM-001-SCFI-2018: 멕시코에서 제조, 수입, 판매 또는 유통되는 전자 장비에 대한 안전 요구 사항 및 시험 방법.
- CSA/UL 62368-1:2019: 최대 전압이 600V인 전기 및 전자 오디오, 비디오 또는 정보 통신 기술 장비에 대한 안전 표준입니다.

## 2.3 환경

### 2.3.1 IP 등급

국제 전기 기술 위원회(International Electrotechnical Commission: IEC) 표준 IEC 60529에는 IP(방진/방수 또는 국제 보호) 등급이 두 자리 코드로 정의되어 있습니다. 이 코드는 고체 물질이나 먼지 침투, 우발적 접촉, 물에 대한 전기 기기의 보호 수준을 정의합니다.

표 2.1 IP 등급 - IP 다음 첫 번째 숫자: 이물질 고체

레벨	보호 대상	효과
0	보호되지 않음	보호 없음
1	50mm 이상의 물체	손등과 같은 신체의 넓은 표면. 단, 의도적인 신체 부위 접촉은 보호되지 않음.
2	12.5mm 이상의 물체	위험한 부분에서 안전하다는 가정 하에 손가락이나 다른 물체가 80mm까지 들어갈 수 있음. 지름이 12.5mm인 물체는 완전히 들어갈 수 없음
3	2.5mm 이상의 물체	공구 및 굵은 전선 같은 물체가 전혀 들어갈 수 없음.
4	1mm 이상의 물체	전선 및 나사 같은 물체가 전혀 들어갈 수 없음.

표 2.1. IP 등급 - IP 다음 첫 번째 숫자: 이물질 고체 (계속)

5	먼지로부터 보호	먼지의 침투가 완전히 방지되지는 않지만 장비의 양호한 작동에 방해가 될 정도로 많은 먼지가 침투하지 않음.
6	방진	먼지가 침투하지 못 함.

표 2.2 IP 등급 - IP 다음 두 번째 숫자: 액체

레벨	보호 대상	효과
0	보호되지 않음	특별한 보호 기능 없음
1	낙수	낙수(수직으로 떨어지는 물방울)로 인한 부정적인 영향이 없음
2	최대 15° 기울어졌을 때 낙수	인클로저가 정상 위치에서 어느 각도로든 최대 15° 기울어졌을 때, 수직으로 떨어지는 물방울로 인한 부정적인 영향이 없음.
3	분무되는 물	수직 위치에서 최대 60° 각도로 분무되어 떨어지는 물로 인한 부정적인 영향이 없음.
4	튀는 물	어느 방향에서든 인클로저에 물이 튀어도 부정적인 영향 없음.
5	물 분사	어느 방향에서든 노즐에서 인클로저에 물이 분사되어도 부정적인 영향 없음.
6	강력한 물 분사	거친 파도나 강력하게 분사된 물이 부정적인 영향을 줄 만큼 인클로저 안으로 침투하지 않음.
7	잠깐의 침수	정의된 조건의 압력과 시간에 따라 인클로저를 물에 담갔을 때 부정적인 영향을 줄 정도로 물이 침투하지 않음.
8	지속적인 침수	제조자가 명시한 조건에서 장비를 물에 지속적으로 담글 수 있음. 이 조건은 IPX7(위 레벨 참조)보다 가혹해야 함.
9	고압 온수로부터 보호	고온 및 고압 상태에서 어떤 각도에서든 하우징을 향하는 물은 유해한 영향을 미치지 않습니다.

### 2.3.2 기타 관련 표준

- IEC 60068-2: 극한의 추위와 건조 열을 포함한 환경 조건에서 기능 수행 능력을 평가하기 위한 전자 장비 및 제품의 환경 시험 표준. 이 표준의 아래 절차는 일반적으로 시험 절차 중의 온도 안정성을 달성하는 대상을 위한 것입니다.
  - IEC 60068-2-1: 추위
  - IEC 60068-2-2: 건조한 열
  - IEC 60068-2-6: 진동 (지속)
  - IEC 60068-2-14: 온도 변화
  - IEC 60068-2-27: 충격
  - IEC 60068-2-64: 진동 (광범위한 무작위)

- IEC 60068-2-78: 습한 열 (일정한 상태)
- IEC 60825 Class I: 레이저 포커스 모듈에 사용되는 레이저 종류가 정상적으로 사용되는 모든 조건에서 안전함을 보장하기 위한 표준.
- IEC TR 60721-3-5: 지상 차량에 설치되어 있지만 차량의 일부가 아닌 제품의 환경 조건을 분류합니다. 통신 시스템, 무전기, 요금 미터기 등의 제품.
- EN 50155: 온도 및 습도와 같은 범위 내에서 철도 차량에 설치된 전자 장비의 안전, 설계 및 작동을 보장하는 철도 애플리케이션용 표준.
- EN 61373: 철도 분야에서 사용되는 철도 차량 장비의 충격 및 진동 시험을 위한 표준. 철도 운영 환경으로 인한 진동과 충격을 견딜 수 있는 장비의 적절성과 성능을 평가합니다.
- MIL-STD-810H: 진동, 충격, 습도, 먼지, 저온 및 고온과 같은 환경 조건을 견딜 수 있는지 확인하기 위한 제품 평가 표준. 아래 방법은 다양한 환경 조건을 모방하기 위해 재현된 것입니다.
  - 501.7: 고온
  - 502.7: 저온
  - 505.7: 태양 복사
  - 506.6: 비
  - 507.6: 습도
  - 509.7: 염무
  - 512.6: 침수

### 2.3.3 NEMA 등급

미국전기공업협회(National Electrical Manufacturers Association: NEMA)는 전기 장비 인클로저에 대한 표준을 제공하는 미국 협회입니다. NEMA는 전 세계적으로 자체 표준 NEMA 250을 발표했습니다. NEMA는 또한 미국국가표준협회(American National Standards Institute: ANSI)를 통해 조화 IP 표준인 ANSI/IEC 60529를 채택하고 발표했습니다.

NEMA 250은 침투 방지를 다루면서, 내식성, 성능, 시공 세부 사항과 같은 다른 요소 또한 고려합니다. 이 때문에 NEMA 유형은 IP와 비교할 만하지만 IP는 NEMA와 비교할 수 없습니다.

UL 표준 UL 50 및 UL 50E는 NEMA 250 표준을 기반으로 합니다. NEMA는 자체 인증을 허용하는 반면 UL은 제품이 제3자 시험 및 검사를 통과하도록 요구하여 규정 준수를 시행합니다.

표 2.3 비 위험 장소의 인클로저에 대한 NEMA 등급

NEMA	동일 레벨의 IP 등급	실내	실외	보호 대상
Type 1	IP10	X		위험 부위 접근 및 고체 이물질 침투(떨어지는 흙). 액체에 대한 보호 효과 없음.

표 2.3. 비 위험 장소의 인클로저에 대한 NEMA 등급 (계속)

Type 3	IP54	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 바람에 날린 먼지). 물 침투(빗물, 진눈깨비, 눈). 인클로저 외부에 생기는 얼음에 의해 손상되지 않음.
Type 3R	IP14	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙). 물 침투(빗물, 진눈깨비, 눈). 인클로저 외부에 생기는 얼음에 의해 손상되지 않음.
Type 3S	IP54	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 바람에 날린 먼지). 물 침투(빗물, 진눈깨비, 눈). 외부 기계 장치에 얼음이 많아도 작동할 수 있음.
Type 4	IP56	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 바람에 날린 먼지). 물 침투(빗물, 진눈깨비, 눈, 튀는 물, 호스로 뿌린 물). 인클로저 외부에 생기는 얼음에 의해 손상되지 않음.
Type 4X	IP56	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 바람에 날린 먼지). 물 침투(빗물, 진눈깨비, 눈, 튀는 물, 호스로 뿌린 물). 부식에 대한 추가 방지 레벨 제공. 인클로저 외부에 생기는 얼음에 의해 손상되지 않음.
Type 6	IP67	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙). 물 침투(호스로 뿌려진 물 및 때때로 제한된 깊이로 잠깐 동안의 침수로 인한 물 유입). 인클로저 외부에 생기는 얼음에 의해 손상되지 않음.
Type 6P	IP67	X	X	위험 부위 접근 및 고체 이물질 침투(떨어지는 흙). 물 침투(호스로 뿌려진 물 및 제한된 깊이로 지속된 침수로 인한 물 유입). 부식에 대한 추가 방지 레벨 제공. 인클로저 외부에 생기는 얼음에 의해 손상되지 않음.
Type 12	IP52	X		녹아웃 제외. 위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 순환하는 먼지, 보풀, 섬유). 물 침투(낙수 및 살짝 튀는 물).
Type 12K	IP52	X		녹아웃 포함. 위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 순환하는 먼지, 보풀, 섬유). 물 침투(낙수 및 살짝 튀는 물).
Type 13	IP54	X		위험 부위 접근 및 고체 이물질 침투(떨어지는 흙 및 순환하는 먼지, 보풀, 섬유). 물 침투(낙수 및 살짝 튀는 물). 오일 및 비 부식성 냉각수 분무, 튀, 침투.

NEMA TS 2는 교통 신호 장비에 적용되는 설계 가이드입니다.

- NEMA TS 2-2.2.7 시험 절차: 과도 전류, 온도, 전압, 습도
- NEMA TS 2-2.2.8 진동 시험
- NEMA TS 2-2.2.9 충격(충돌) 시험



### 2.3.4 IK 등급

IK 등급은 외부 기계적 충격에 대한 보호 수준을 지정하는 국제 표준인 IEC/EN 62262에서 확인할 수 있습니다. 원래 1994년에 유럽 표준 EN 50102로 승인되었으며 2002년에 국제 표준으로 채택되었습니다.

많은 제조업체가 제품 수명 기간 동안 견고성을 보장하기 위해 제품의 가장 약한 부분을 시험하도록 선택합니다.

레벨	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK11*
충격 에너지 (Joule)	0.14	0.2	0.35	0.5	0.7	1	2	5	10	20	50*
질량 (kg)	<0.2	<0.2	0.2	0.2	0.2	0.5	0.5	1.7	5	5	
낙하 높이 (mm)	56	80	140	200	280	400	400	300	200	400	

\*최대 50 J의 충격. 제조업체는 타격 요소의 에너지, 질량 및 낙하 높이를 표시해야 합니다.

## 2.4 기타 승인

### 2.4.1 방폭

- IEC/EN/UL/SANS/CSA 60079-0: 폭발성 환경에서 사용할 목적의 Ex 장비 및 Ex 구성 요소의 시공, 시험 및 표시에 대한 일반 요건.
- IEC/EN/UL/SANS/CSA 60079-1: 폭발성 가스 환경에서 사용할 목적의 보호 내화 인클로저 유형 "d"를 포함하는 전기 장비의 시공 및 시험에 대한 특정 요건.

방폭에 대한 더 자세한 표준 및 규정 목록은 *여기*에서 인증을 참조하십시오.

### 2.4.2 미드스팬용 승인

미드스팬이 제품에 포함된 경우, 미드스팬에 관련된 승인이 데이터시트의 이 섹션에 나열되어 있습니다. 설명은 현재 문서의 이전 섹션에 나와있습니다.

### 2.4.3 접근 제어의 보안

- UL 294: 접근 제어 시스템의 시공, 성능, 운영과 관련된 요건을 정의합니다.

## 3 인증

폭발 가능성이 있는 환경에 카메라를 설치할 경우, 하우징이 매우 구체적인 안전 표준을 충족해야 합니다. 카메라 및 기타 장비의 잠재적 발화 원인으로부터 환경을 보호해야 합니다.

유럽 제품은 ATEX 지침을 준수해야 하며 해당 국제 표준은 IECEx입니다. 북미에서는 ATEX 및 IECEx에 설명된 Zone 시스템에 대해 주로 NFPA70(National Electric Code, NEC) 및 CSA C22.1(Canadian Electric Code, CEC)의 Class/Division 등급을 사용합니다.

표 3.1 인증

규정/인증	지역/국가
ATEX	EU
CCC Ex	중국
cMETus/cULus	캐나다 및 미국
IA 인증	남아프리카 공화국
IECEx	위험 장소에서 사용되는 장비에 대한 국제 인증
INMETRO	브라질
JPEX	일본
KCs	한국
OSHA Taiwan	대만
PESO	인도

표 3.2 방폭 등급

Class / Division	대기	정의	Zone (IECEx 및 ATEX)
Class I / Division 1	가스	폭발성 혼합물이 지속적으로 존재하거나 장기간 존재하는 구역.	Zone 0
Class I / Division 1	가스	일반 작동 상태에서 폭발성 혼합물이 발생하기 쉬운 구역.	Zone 1
Class I / Division 2	가스	일반 작동 상태에서 폭발성 혼합물이 발생하기 쉽지 않고, 발생하더라도 짧은 시간 동안만 존재하는 구역.	Zone 2
Class II / Division 1	먼지	폭발성 혼합물이 지속적으로 존재하거나 장기간 존재하는 구역.	Zone 20
Class II / Division 1	먼지	일반 작동 상태에서 폭발성 혼합물이 발생하기 쉬운 구역.	Zone 21
Class II / Division 2	먼지	일반 작동 상태에서 폭발성 혼합물이 발생하기 쉽지 않고, 발생하더라도 짧은 시간 동안만 존재하는 구역.	Zone 22

## 4 전원

### 4.1 PoE(Power over Ethernet) class

PoE class는 전력 장치(PD, powered device)에 필요한 전력량을 지정하여 효율적인 전력 분배를 보장합니다.

표 4.1 PoE class

등급	Type	전원 공급 장비(PSE: Power Sourcing Equipment)에 보장된 전력 레벨	전력 장치(PD)가 사용하는 최대 전력 레벨
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

\*이 유형을 PoE+ 라고도 합니다.

## 5 네트워크

### 5.1 보호 및 보안 컨트롤

시스템 자산에 대한 위협에 대응하는 몇 가지 방법이 있습니다. 일부 위협은 장치에 위협을 초래하는 반면 다른 위협은 네트워크 또는 전송/저장 중인 데이터에 위협을 초래합니다. 장치 및 네트워크에 적용할 수 있는 몇 가지 선택된 보안 제어:

- 자격 증명(사용자/ 암호)은 비디오에 대한 무단 액세스로부터 보호하고 장치 구성에 대한 무단 액세스를 방지합니다. 계정 권한 수준이 다르면 누가 무엇에 액세스할 수 있는지 제어할 수 있습니다.
- IP 주소 필터링(방화벽)은 장치의 로컬 네트워크 노출을 줄여서 허가되지 않은 클라이언트가 액세스할 수 없도록 보호합니다. 이렇게 하면 장치 암호가 훼손될 위험이 줄어들고, 새로운 심각한 취약점이 발견될 때에도 위험이 완화됩니다.
- IEEE 802.1x: 허가되지 않은 클라이언트로부터 네트워크를 보호합니다. 802.1x는 관리형 스위치 및 RADIUS 서버를 사용하는 네트워크 인프라 보호입니다. 장치의 802.1x 클라이언트는 네트워크에 있는 장치에 대한 인증을 제공합니다.

- HTTPS(Hypertext Transfer Protocol Secure): 네트워크 도청으로부터 데이터(비디오)를 보호합니다. HTTPS에서 서명된 인증서를 사용하면 비디오 클라이언트가 합법적인 카메라에 액세스하는지 아니면 카메라를 가장하는 악의적인 컴퓨터에 액세스하는지 감지할 수 있습니다.
- Signed Firmware: 소프트웨어 공급업체가 보안 유지되는 개인 키로 펌웨어 이미지에 서명하여 구현됩니다. 펌웨어에 이 서명이 첨부되어 있으면 장치는 펌웨어 설치를 수락하기 전에 펌웨어의 유효성을 검사합니다. 장치가 펌웨어 무결성이 손상된 것을 감지하면 펌웨어 업그레이드를 거부합니다. Axis Signed Firmware는 업계에서 승인된 RSA 공개 키 암호화 방법을 기반으로 합니다.
- Secure Boot: 변경 불가능 메모리(부트 ROM)에서 시작하여 암호화로 검증된 소프트웨어의 손상되지 않은 체인으로 구성된 부트 프로세스입니다. Signed Firmware를 기반으로 하여 Secure Boot는 장치가 허가된 펌웨어로만 부팅할 수 있도록 합니다. Secure Boot는 Axis 장치가 공장 출하 시 기본 값으로 초기화한 후 발생 가능한 맬웨어로부터 완벽하게 보호되도록 보장합니다.
- TPM: 신뢰 받는 플랫폼 모듈은 무단 액세스로부터 정보를 보호하는 데 적합한 암호화 기능 집합을 제공하는 구성 요소입니다. 개인 키는 TPM에 저장되고 절대로 TPM 밖으로 전송되지 않습니다. 개인 키 사용이 필요한 모든 암호화 작업은 처리를 위해 TPM으로 전송됩니다. 이렇게 하면 보안 침입 시에도 인증서의 보안 부분이 안전하게 유지됩니다.
- Axis Edge Vault: Axis 장치 ID가 안전하고 영구적으로 설치 및 저장되는 보안 암호화 컴퓨팅 모듈 (보안 모듈 또는 보안 요소)입니다.

보다 많은 사이버 보안 관련 자료를 보시려면 다음 웹사이트를 참조하십시오: [axis.com/cybersecurity](https://axis.com/cybersecurity)

## 5.2 지원되는 프로토콜

데이터를 네트워크로 연결된 한 장치에서 다른 장치로 안전하게 전송할 때, 많은 프로토콜이 작동합니다.

### 5.2.1 프로토콜 참조 모델

여러 프로토콜이 상호 작용하는 방식을 이해하는 가장 좋은 방법은 OSI(개방형 시스템 상호 연결) 통신 모델을 조사하는 것입니다. 또한 TCP/IP 참조 모델도 있습니다.

#### 5.2.1.1 OSI 참조 모델

개방형 시스템 간의 데이터 통신을 설명해주는 모델. 각 계층은 서비스를 제공하기 위해 그 바로 아래에 있는 계층의 서비스를 사용합니다. 각 계층은 서비스를 수행하기 위해 특정 규칙 또는 프로토콜을 따라야 합니다.

#### 7 계층 - 애플리케이션

애플리케이션이 웹, 파일, 이메일 전송 같은 기능을 사용할 수 있게 합니다.

웹 브라우저나 이메일 프로그램 같은 실제 애플리케이션은 이 계층 위에 존재하며 OSI 모델에서 다루지 않습니다.

#### 6 계층 - 프레젠테이션 (데이터)

시스템의 애플리케이션 계층에서 보낸 데이터를 다른 시스템의 애플리케이션 계층에서 읽을 수 있도록 합니다. ASCII 같은 시스템 의존형 데이터 형식을 독립적인 형식으로 변환하여 서로 다른 시스템 간에 구문적으로 올바른 데이터 교환을 허용합니다.

**5 계층 - 세션 (피어 호스트 간의 지속적인 연결)**

애플리케이션 지향 서비스를 제공하며 두 시스템 간의 프로세스 통신을 처리합니다. 프로세스 통신은 두 시스템 간의 가상 연결을 위한 기반을 제공하는 세션 설정으로 시작됩니다.

**4 계층 - 전송 (엔드 투 엔드 전송(연결 지향 프로토콜))**

5 계층 이상의 계층에 신뢰할 수 있는 데이터 전송 서비스를 제공합니다(흐름 제어 및 오류 제어를 통해).

**3 계층 - 네트워크 (패킷 (주소 지정/단편화))**

시스템 간에 데이터 패킷을 라우팅하고 전달하여 실제 데이터를 전송합니다. 라우팅 테이블을 만들고 관리하며, 네트워크 경계를 넘어 통신할 수 있는 옵션을 제공합니다. 이 계층의 데이터에는 대상 라우팅의 기준으로 사용되는 대상 및 소스 주소가 지정됩니다.

**2 계층 - 데이터 링크 (프레임)**

프레임 단위로 데이터를 결합하여 데이터를 전송하고 전송 매체에 대한 액세스를 제어합니다. 2 계층은 두 개의 하위 계층으로 나뉘는데, 상위 영역은 LLC(Logical Link Control)에 해당하고 하위 영역은 MAC(Media Access Control)에 해당합니다. LLC는 데이터 교환을 단순화하는 반면 MAC은 전송 매체에 대한 액세스를 제어합니다.

**1 계층 - 물리 (비트)**

유선 또는 무선 전송 링크 등 매체를 통한 비트스트림인 데이터 전송을 지원하는 서비스를 제공합니다.

**5.2.1.2 TCP/IP 참조 모델**

TCP/IP 참조 모델은 프로토콜과 통신이 이루어지는 방식을 이해하는 데 사용되는 또 다른 모델입니다. TCP/IP 참조 모델은 아래와 같이 OSI 참조 모델에 해당하는 4가지 다른 계층으로 분류됩니다.

*표 5.1 참조 모델 비교*

OSI 모델	TCP/IP 모델
7 계층 - 애플리케이션	4 계층 - 애플리케이션
6 계층 - 프레젠테이션	
5 계층 - 세션	
4 계층 - 전송	3 계층 - 전송
3 계층 - 네트워크	2 계층 - 인터넷워크
2 계층 - 데이터 링크	1 계층 - 네트워크 인터페이스
1 계층 - 물리	

## 5.2.2 애플리케이션 계층 프로토콜

- **CIFS/SMB**(Common Internet File System/Server Message Block: 공통 인터넷 파일 시스템/서버 메시지 블록): 주로 파일, 프린터, 시리얼 포트에 대한 공유 액세스 및 네트워크 노드 간의 기타 통신을 제공하는 데 사용됩니다.
- **DDNS**(Dynamic Domain Name System: 동적 도메인 네임 시스템): IPv4 주소 변경에 대한 도메인 이름의 링크를 추적하는 데 사용됩니다.
- **DHCPv4/v6**(Dynamic Host Configuration Protocol: 동적 호스트 구성 프로토콜): IP 주소 자동 할당 및 관리.
- **DNS/DNSv6**(Domain Name System: 도메인 네임 시스템): 도메인 이름을 연결된 IP 주소로 변환됩니다.
- **FTP**(File Transfer Protocol: 파일 전송 프로토콜): 주로 서버에서 클라이언트(다운로드) 또는 클라이언트에서 서버(업로드)로 파일을 전송하는 데 사용됩니다. 또한 디렉토리를 만들고 선택하고, 디렉토리 및 파일의 이름을 변경하거나 삭제하는 데 사용할 수 있습니다.
- **HTTP**(Hypertext Transfer Protocol: 하이퍼텍스트 전송 프로토콜): 주로 텍스트와 이미지를 웹 사이트에서 웹 브라우저에 로드하는 데 사용됩니다. 네트워크 비디오 시스템은 구성 또는 실시간 이미지를 다운로드하기 위해 웹 브라우저를 통해 시스템에 액세스할 수 있는 HTTP 서버 서비스를 제공합니다.
- **HTTP/2**: RFC 7540에 정의되어 있고 2015년 2월에 릴리스된 HTTP 프로토콜의 주요 개정 버전입니다.
- **HTTPS**(HTTP Secure): 컴퓨터 네트워크를 통한 보안 통신을 위해 HTTP를 개조한 것이며 인터넷에서 널리 사용됩니다. HTTPS에서 통신 프로토콜은 TLS(전송 계층 보안)로 암호화됩니다.
- **MQTT**(Message Queuing Telemetry Transport): 사물 인터넷(IoT)을 위한 표준 메시징 프로토콜입니다. 단순화된 IoT 통합을 위해 설계되었으며 작은 코드 공간(small code footprint)과 최소 네트워크 대역폭으로 원격 장치를 연결하기 위해 다양한 산업에서 사용됩니다.
- **NTP**(Network Time Protocol: 네트워크 시간 프로토콜): 컴퓨터 클라이언트 또는 서버의 시간을 다른 서버와 동기화하는 데 사용됩니다.
- **RTP**(Real-Time Transport Protocol: 실시간 전송 프로토콜): 시스템 엔드 포인트 간에 실시간 데이터 전송을 허용합니다.
- **RTCP**(Real-Time Control Protocol: 실시간 제어 프로토콜): RTP 세션에 대한 대역 외 통계 및 제어 정보를 제공합니다. 멀티미디어 데이터의 전송 및 패키징 시 RTP와 협력하지만 미디어 데이터는 전송하지 않습니다.
- **RTSP**(Real-Time Streaming Protocol: 실시간 스트리밍 프로토콜): 실시간 미디어 전송에 대한 확장된 제어.
- **SFTP**(Secure File Transfer Protocol: 보안 파일 전송 프로토콜): 신뢰할 수 있는 데이터 스트림을 통해 파일 액세스, 파일 전송 및 파일 관리를 제공합니다.
- **SIP**(Session Initiation Protocol: 세션 개시 프로토콜): 멀티미디어 통신 세션을 시그널링하고 제어하기 위한 통신 프로토콜.
- **SIPS**(Session Initiation Protocol Secure): SIP의 암호화된 버전입니다.

- **SMTP**(Simple Mail Transfer Protocol: 단순 메일 전송 프로토콜): 인터넷을 통해 이메일을 전송하는 표준. 네트워크 카메라는 SMTP를 지원하여 이메일 경로를 전송할 수 있습니다.
- **SNMPv1/v2/v3**(Simple Network Management Protocol: 단순 네트워크 관리 프로토콜): 스위치, 라우터 및 네트워크 카메라와 같은 네트워크 장비를 원격으로 모니터링하고 관리하는 데 사용됩니다. SNMP 지원을 통해 네트워크 카메라를 오픈 소스 도구로 관리할 수 있습니다.
- **SOCKS**: 원격 네트워크 프록시를 통해 클라이언트와 서버 간의 네트워크 패킷 전송을 허용합니다.
- **SRTP**(Secure Real-Time Transport Protocol: 실시간 전송 보안 프로토콜): 시스템 엔드 포인트 간에 실시간 데이터의 암호화된 전송을 허용하므로 RTP의 보안 변종입니다.
- **SSH**(Secure Shell): 보안되지 않은 네트워크를 통해 네트워크 장치에 대한 관리 및 디버그 액세스를 안전하게 허용합니다.
- **TLSv1.2/v1.3**(Transport Layer Security: 전송 계층 보안): 클라이언트와 서버 간의 신뢰할 수 있는 비공개 연결을 협상합니다.

### 5.2.3 전송 계층 프로토콜

- **TCP**(Transmission Control Protocol: 전송 제어 프로토콜): 데이터 스트림의 연결 지향, 신뢰성 및 순차적 전송. 데이터 전송을 위한 가장 보편적인 프로토콜.
- **UDP**(User Datagram Protocol: 사용자 데이터그램 프로토콜): 비 연결형 전송 서비스, 신뢰성 보다 적시에 데이터를 제공하는 것을 선호.
- **ICMP**(Internet Control Message Protocol: 인터넷 제어 메시지 프로토콜): 요청된 서비스를 사용할 수 없거나 호스트 또는 라우터에 도달할 수 없음을 나타내는 오류 메시지 및 작동 정보를 전송합니다.

### 5.2.4 네트워크 계층 프로토콜

- **IGMPv1/v2/v3**(Internet Group Management Protocol: 인터넷 그룹 관리 프로토콜): IPv4 네트워크의 호스트 및 인접 라우터가 멀티캐스트 그룹 멤버십을 설정하는 데 사용되며, 이러한 유형의 애플리케이션을 지원할 때 리소스를 보다 효율적으로 사용할 수 있습니다.
- **IPv4/IPv6**(Internet Protocol: 인터넷 프로토콜): 인터넷 지원 장치가 통신하는 데 필요한 개별 공용 주소입니다. IPv4는 원래의 버전이며 32비트 주소를 사용합니다. IPv6은 가장 최신 버전이며 128비트 주소를 사용하며 4개의 16진수로 구성된 8개의 그룹으로 나뉩니다.
- **USGv6**: IPv6 지원 네트워크 장치를 조달할 때 호환성을 보장하기 위해 미국 정부에서 정의한 IPv6에 대한 기술 표준 프로파일입니다.

### 5.2.5 데이터 링크 계층 프로토콜

- **ARP**(Address Resolution Protocol: 주소 결정 프로토콜): 대상 호스트의 MAC 주소를 검색하는 데 사용됩니다.
- **CDP**(Cisco Discovery Protocol: Cisco 검색 프로토콜): 연결된 하드웨어 장치에 대한 정보를 검색하기 위해 LLDP의 대안으로 사용되는 고유한 Cisco 프로토콜입니다.

- **IEEE 802.3(i, u, ab)**: 트위스트 페어 케이블을 통한 10Mb/s(10Base-T), 100Mb/s(100Base-TX) 및 1Gb/s(1000Base-T) 데이터 통신을 정의하는 이더넷 표준입니다.
- **LLDP(Link Layer Discovery Protocol)**: 링크 계층 검색 프로토콜: 장치의 ID 및 기능뿐만 아니라 동일한 네트워크 내에 연결된 다른 장치를 알리는 데 사용됩니다.

### 5.2.6 검색 프로토콜

- **mDNS(Bonjour)**: Mac 컴퓨터를 사용하여 네트워크 비디오 제품을 검색하는 데 사용하거나 네트워크의 새로운 장치를 검색하는 프로토콜로 사용될 수 있습니다.
- **UPnP(Universal Plug and Play)**: 범용 플러그 앤 플레이: Microsoft 운영 체제는 네트워크에서 자동으로 리소스(Axis 장치)를 감지할 수 있습니다.
- **Zeroconf**: 169.254.1.0에서 169.254.254.255의 범위에서 사용되지 않는 IP 주소를 네트워크 장치에 자동으로 할당합니다.

### 5.2.7 서비스 품질(QoS)

IP 네트워크에서 각 서비스의 요구 사항을 충족하기 위해 네트워크 리소스를 공유하는 방법을 제어해야 합니다.

- **QoS(Quality of Service)**: 서비스 품질: 우선 순위가 낮은 플로우보다 중요한 플로우가 먼저 제공될 수 있도록 네트워크 트래픽의 우선 순위를 지정하는 기능. 애플리케이션이 사용할 수 있는 대역폭을 제어하고 애플리케이션 간 대역폭 경쟁을 제어하는 기능을 제공하여 네트워크의 안정성을 향상시킵니다.
- **DiffServ**: 네트워크가 각 패킷에 의해 지정된 QoS에 기반하여 특정 서비스를 전달하려고 시도합니다.

### 5.2.8 데이터 전송 방법

컴퓨터 네트워크에서 데이터를 전송하는 방법은 세 가지가 있습니다.

- **유니캐스트**: 가장 일반적이고, 송신자 및 수신자가 지점 간(point-to-point) 통신을 합니다. 데이터 패커가 한 명의 수신자에게만 전송되며 다른 클라이언트는 해당 정보를 수신하지 않습니다.
- **멀티캐스트**: 네트워크의 단일 송신자와 다중 수신자 간 통신. 하나의 정보 스트림을 여러 수신자에게 제공하여 네트워크 트래픽을 줄입니다.
- **브로드캐스트**: 송신자가 네트워크의 다른 모든 서버에 동일한 정보를 보냅니다. 네트워크의 모든 호스트가 메시지를 수신하고 일부를 처리합니다.





# Axis Communications 정보

Axis는 보안 및 새로운 비즈니스 성과를 개선하기 위한 솔루션을 창조하여 더 스마트하고 안전한 세상을 가능하게 합니다. 네트워크 기술 회사이자 업계 리더인 Axis는 비디오 감시, 접근 제어, 인터콤, 오디오 시스템 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 향상되고, 고품질 교육의 지원을 받습니다.

Axis에서는 50개 이상의 나라에 약 4,000명의 전담 직원이 있으며 전 세계 기술 및 시스템 통합 파트너와 협력하여 고객 솔루션을 제공합니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다