WHITEPAPER

Kurzanleitung zu Axis Datenblättern

Zulassungen, Zertifikate und Protokolle

Oktober 2023

Inhalt

1 Einführung

Axis Communications beachtet die geltenden Branchen- und Compliance-Standards im Hinblick auf alle vermarkteten Produkte. Dieses Dokument ergänzt die Axis-Datenblätter um Definitionen und Kurzbeschreibungen der darin enthaltenen Akronyme, Zulassungen, Zertifikate und Protokolle.

Dieses Dokument liefert Informationen zu den unten hervorgehobenen Abschnitten der Datenblätter.

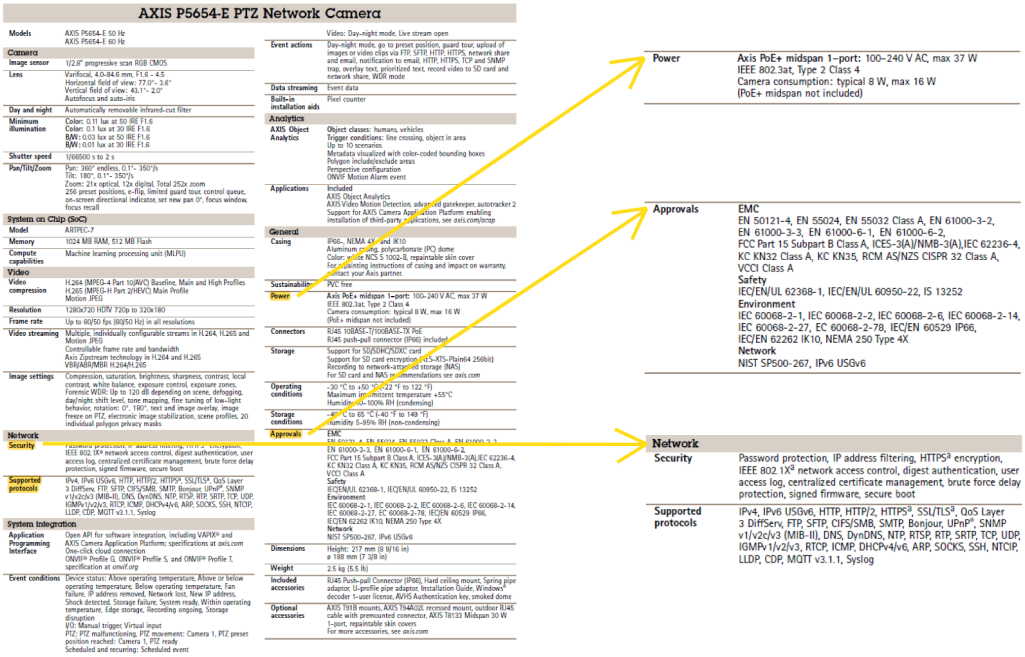

Figure 1. Markierung der Axis Datenblatt-Abschnitte, die in diesem Dokument behandelt werden.

2 Zulassungen

Der Abschnitt Zulassungen in den Datenblättern von Axis betrifft die Einhaltung verschiedener Normen und Standards. Dieser Abschnitt ist üblicherweise in die Unterabschnitte zu EMV, Sicherheit, Umwelt, Netzwerk und Sonstiges unterteilt, wobei „Sonstiges" z. B. den Explosionsschutz oder die Sicherheit bei der Zutrittskontrolle bezeichnen kann. Wenn ein Midspan zum Lieferumfang des jeweiligen Produkts gehört, kann hier auch ein Unterabschnitt mit Zulassungen zum Midspan erscheinen.

2.1 EMV – (Elektromagnetische Verträglichkeit)

Alle Hersteller von Netzwerk-Videoprodukten müssen die EMV ihrer Produkte angeben. Unter bestimmten Umständen kann sich der Hersteller selbst zertifizieren, doch die meisten Hersteller nutzen akkreditierte Prüflabore, die in einem Bericht die Compliance bestätigen. EMV-Genehmigung bestehen aus zwei Teilen: Emissionen und Störfestigkeit.

Mit *Emissionen* wird die Fähigkeit eines Geräts bezeichnet, zu funktionieren, ohne dabei zu viel elektromagnetische Energie abzugeben, die andere Geräte in seiner Umgebung stören kann.

Die *Störfestigkeit* beschreibt die Fähigkeit elektronischer Produkte, den Einfluss elektromagnetischer Erscheinungen und von anderen elektronischen Produkten abgegebener elektrischer Energie (Strahlung oder leitergebunden) zu tolerieren. In Europa ist die EMV im CE-Kennzeichen enthalten, das wiederum Bestandteil der EU-Rechtsvorschriften zur Harmonisierung ist.

Die nachfolgend aufgeführten Normen legen die Grenzwerte und Prüfverfahren für elektromagnetische Emissionen und Störfestigkeitstests fest. Da es keinen Test für die Compliance weltweit gibt, kann es in den verschiedenen Regionen und Anwendungen unterschiedliche Codes geben.

2.1.1 Normen zu informationstechnischen Einrichtungen (ITE)

Diese Standards gelten für Multimedia-Ausrüstung (multimedia equipment, MME) mit einer Wechsel- oder Gleichstromversorgung von maximal 600 V. Multimedia-Ausrüstung ist definiert als Informationstechnologie-Ausrüstung (ITE), Audioausrüstung, Videoausrüstung, Rundfunkempfängerausrüstung sowie Entertainment-Beleuchtungseinrichtungen.

- EN 55032 Klasse A: Emissionsnorm (kommerziell, industriell, geschäftlich), mit internationalen Normen harmonisiert
- EN 55032 Klasse B: Emissionsnorm (Wohnbereich), mit internationalen Normen harmonisiert
- EN 55035: Standard zur Störfestigkeit, mit internationalen Normen harmonisiert

2.1.2 Harmonisierte Normen nach Land/Region

- EN 61000-6-1 und EN 61000-6-2: Zu beachtende allgemeine Standards (Europa)
- FCC Teil 15 Abschnitt B Klasse A und B: Die FCC legt Regeln und Richtlinien für Telekommunikationsgeräte fest. Diese betreffen die Abstrahlung, nicht die Störfestigkeit (USA).
- ICES-3 (A und B)/NMB-3 (A und B) (Kanada)
- VCCI Klasse A und B (Japan)
- KS C 9832 Klasse A und B, KS C 9835, KS C 9547, KS C 9815 (Korea)
- RCM AS/NZS CISPR 32 Klasse A und B (Australien/Neuseeland)

2.1.3 Weitere Normen nach Anwendung/Produkt

- EN 50121-4, IEC 62236-4: Enthält Leistungskriterien für Signal- und Telekommunikationsanlagen, die andere Geräte in der Eisenbahnumgebung stören könnten.
- EN 50130-4: Gilt für die Komponenten von Alarmsystemen, wozu auch Zutrittskontrollsysteme, CCTV-Systeme, Branderkennungs- und Brandmeldesysteme, Überfall- und Einbruchmeldeanlagen sowie Hausnotrufsysteme zählen.
- EN 50121-3-2: Gilt für elektromagnetische Verträglichkeit, d. h. Störfestigkeits- und Emissionsschutzanforderungen an elektrische und elektronische Geräte, die in Bahnanwendungen zum Einsatz kommen.

2.2 Sicherheit

- Niederspannungsrichtlinie (2014/35/EU): Legt übergreifende Ziele für die Sicherheit von Elektrogeräten fest. Stellt sicher, dass die Produkte gebrauchssicher sind und keine Gefahr von Personen- oder Sachschäden bergen.
- IEC/EN/UL 62368-1: Einhaltung der Sicherheitsanforderungen bei Netzwerk-Kameras, Encodern und Netzteilen im Hinblick auf die Verringerung der Gefahr von Brand, Stromschlägen oder Verletzungen aller Personen, die das Gerät berühren. Diese Sicherheitsanforderung gilt für Geräte sowohl im Innen- als auch im Außenbereich.
- IEC/EN 62471-1: Photobiologische Sicherheit von Lampen und Lampensystemen; Anforderungen für Expositionsgrenzwerte, verhindert Verletzungen der Augen und Haut.
- IS 13252: Indischer Standard mit Sicherheitsanforderungen an Netzwerk-Kameras, Encoder und Netzteile im Hinblick auf die Verringerung der Gefahr von Feuer, Elektroschocks oder Verletzungen aller Personen, die das Gerät berühren.
- UN ECE R118: garantiert Brandschutz durch spezifische Normanforderungen an Geräte, die in Fahrzeugen eingesetzt und verbaut werden.
- EN 45545-2: Diese Norm gewährleistet, dass Materialien und Bauteile, die in Bahnanwendungen zum Einsatz kommen, spezifische Anforderungen an ihr Brandverhalten erfüllen. Sie umfasst je nach Typ von Bahn, Anwendung und Positionierung (außen oder innen) verschiedene Prüfverfahren.
- NFPA 130.: Brandschutznorm für Schienenfahrzeuge in den Vereinigten Staaten, welche die Sicherheitsnormanforderungen an Bahnsysteme einschließlich Bahnhöfen, Fahrzeugen, Notfallverfahren, Kommunikationssystemen und Bahnübergängen garantiert.
- NOM-001-SCFI-2018: Sicherheitsanforderungen und Prüfverfahren für elektronische Geräte, die in Mexiko hergestellt, importiert, verkauft oder vertrieben werden.
- CSA/UL 62368-1:2019: Sicherheitsnorm für elektrische und elektronische Audio-, Video- oder Informations- und Kommunikationstechnologieausrüstung mit einer maximalen Spannung von 600 V.

2.3 Umgebung

2.3.1 IP-Schutzklasse

Die Norm IEC 60529 der IEC (Internationale Elektrotechnische Kommission) definiert die IP-Schutzart (IP für „International Protection" oder „Ingress protection", zu Deutsch Schutz gegen Eindringen) als zweistelligen Code. Dieser Code gibt an, in welchem Grad elektrische Geräte gegen das Eindringen von Fremdkörpern oder Staub, Wasser oder gegen versehentliche Berührung geschützt sind.

Tabelle 2.1 IP-Schutzklassen, erste Ziffer nach IP: feste Fremdkörper

Stufe	Schutz vor	Wirksamkeit
0	Kein Schutz	Kein Schutz
1	Fremdkörper über 50 mm Größe	Große Oberfläche des Körpers, wie ein Handrücken, allerdings kein Schutz gegen absichtlichen Kontakt mit einem Körperteil.
2	Fremdkörper über 12,5 mm Größe	Finger oder andere Gegenstände dürfen bis zu 80 mm eindringen, sofern gefährliche Teile abgesichert sind. Fremdkörper ab 12,5 mm Durchmesser dürfen nicht voll eindringen.

Tabelle 2.1. IP-Schutzklassen, erste Ziffer nach IP: feste Fremdkörper (Fortsetzung)

3	Fremdkörper über 2,5 mm Größe	Gegenstände wie Werkzeug und dicke Kabel dürfen überhaupt nicht eindringen.
4	Fremdkörper über 1 mm Größe	Gegenstände wie Drähte und Schrauben dürfen überhaupt nicht eindringen.
5	Staubgeschützt	Das Eindringen von Staub wird nicht vollständig verhindert, aber es dringt zu wenig Staub ein, um den akzeptablen Betrieb des Gerätes zu beeinträchtigen.
6	Staubdicht	Kein Eindringen von Staub.

Tabelle 2.2 IP-Schutzklassen, zweite Ziffer nach IP: Flüssigkeiten

Stufe	**Schutz vor**	**Wirksamkeit**
0	Kein Schutz	Kein besonderer Schutz
1	Tropfwasser	Tropfwasser (senkrecht fallende Tropfen) hat keine schädliche Wirkung.
2	Tropfwasser bei Gehäuseneigung bis 15°	Senkrecht fallendes Tropfwasser hat keine schädliche Wirkung, wenn das Gehäuse bis zu 15° von seiner Normalposition geneigt ist.
3	Sprühwasser	Fallendes Sprühwasser in einem Winkel bis 60° gegen die Senkrechte hat keine schädliche Wirkung.
4	Spritzwasser	Allseitiges Spritzwasser gegen das Gehäuse hat keine schädliche Wirkung.
5	Strahlwasser	Strahlwasser (Düse) aus einem beliebigen Winkel gegen das Gehäuse hat keine schädliche Wirkung.
6	Starkes Strahlwasser	Wasser durch Überflutung oder starkes Strahlwasser kann nicht in schädlichen Mengen in das Gehäuse eindringen.
7	Kurzzeitiges Eintauchen in Wasser	Es dringt keine schädliche Menge an Wasser ein, wenn das Gehäuse unter definierten Druck- und Zeitbedingungen unter Wasser getaucht wird.
8	Dauerhaftes Untertauchen in Wasser	Das Gerät eignet sich für dauerndes Untertauchen in Wasser unter den Bedingungen, die vom Hersteller anzugeben sind. Die Bedingungen müssen schwieriger sein als bei IPX7 (siehe oben).
9	Schutz vor heißem Wasser unter Hochdruck	Wasser, das aus jeder Richtung bei hoher Temperatur und unter stark erhöhtem Druck gegen das Gehäuse gerichtet ist, darf keine schädliche Wirkung haben.

2.3.2 Weitere relevante Normen

- IEC 60068-2: Eine Norm für Umgebungsprüfungen elektronischer Ausrüstungen und Produkte, zur Beurteilung, ob sie unter Umgebungsbedingungen einschließlich extremer Kälte und trockener Wärme funktionieren. Die folgenden Verfahren in dieser Norm sind in der Regel für Gegenstände vorgesehen, die während des Tests stabile Temperaturen erreichen.
  - IEC 60068-2-1: Kälte

- IEC 60068-2-2: Trockene Wärme
- IEC 60068-2-6: Schwingen (sinusförmig)
- IEC 60068-2-14: Temperaturwechsel
- IEC 60068-2-27: Schocken
- IEC 60068-2-64: Schwingen (Breitbandrauschen)
- IEC 60068-2-78: Feuchte Wärme (konstant)

- IEC 60825 Klasse I: Eine Norm, die sicherstellt, dass der verwendete Lasertyp im Laser-Fokussiermodul unter normalen Anwendungsbedingungen sicher ist.
- IEC TR 60721-3-5: klassifiziert die Umweltbedingungen von Produkten, die in einem Bodenfahrzeug installiert, jedoch nicht Teil des Fahrzeugs sind. Produkte wie beispielsweise Kommunikationssysteme, Funkgeräte und Fahrpreisanzeiger.
- EN 50155: Eine Norm für Bahnanwendungen zur Gewährleistung der Sicherheit, Konstruktion und Funktion elektronischer Geräte, die in Bahnfahrzeugen installiert werden, in Bereichen wie Temperatur und Feuchtigkeit.
- EN 61373: Eine Norm für die Stoß- und Vibrationsprüfung von Rollmaterialausrüstung, die in Bahnanwendungen zum Einsatz kommt. Sie bewertet die Angemessenheit und Fähigkeit der Ausrüstung, Vibrationen und Stößen infolge der Bahnbetriebsumgebung zu widerstehen.
- MIL-STD-810H: Eine Norm zur Bewertung von Produkten, mit der gewährleistet wird, dass diese Umweltbedingungen wie beispielsweise Vibration, Stößen, Feuchtigkeit, Staub sowie niedrigen und hohen Temperaturen standhalten können. Nachstehende Verfahren wurden zur Nachahmung der verschiedenen Umgebungsbedingungen entwickelt.
  - 501.7 – Hohe Temperaturen
  - 502.7 – Niedrige Temperaturen
  - 505.7 – Sonneneinstrahlung
  - 506.6: Regen
  - 507.6: Feuchtigkeit
  - 509.7 – Salznebel
  - 512.6: Immersion

2.3.3 NEMA-Schutzart

Die NEMA (National Electrical Manufacturers Association) ist eine US-amerikanische Vereinigung, die Normen für Gehäuse elektrischer Geräte entwickelt. Die NEMA hat ihren eigenen Standard NEMA 250 weltweit eingeführt. Außerdem hat sie den Standard zur IP-Harmonisierung ANSI/IEC 60529 über das American National Standards Institute (ANSI) übernommen und veröffentlicht.

NEMA 250 behandelt die Schutzart, berücksichtigt aber auch andere Faktoren wie Korrosionsschutz, Leistung und Konstruktionsmerkmale. Deshalb ist der NEMA-Typ vergleichbar mit IP, aber IP ist nicht mit NEMA zu vergleichen.

Die UL-Normen UL 50 und UL 50E basieren auf der Norm NEMA 250. NEMA erlaubt eine Selbstzertifizierung, während UL für die Compliance externe Tests und Prüfungen voraussetzt.

Tabelle 2.3 NEMA-Schutzarten für Gehäuse in nicht explosionsgefährdeten Bereichen

NEMA	Äquivalente IP-Schutzart	Innenbereich	Außenbereich	Schutz vor
Typ 1	IP10	X		Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz). Kein Schutz gegen Flüssigkeiten.
Typ 3	IP54	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und windgetriebener Staub). Eindringen von Wasser (Regen, Schneeregen, Schnee). Die Bildung von Eis außen am Gehäuse hat keine Beschädigungen zur Folge.
Typ 3R	IP14	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz). Eindringen von Wasser (Regen, Schneeregen, Schnee). Die Bildung von Eis außen am Gehäuse hat keine Beschädigungen zur Folge.
Typ 3S	IP54	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und windgetriebener Staub). Eindringen von Wasser (Regen, Schneeregen, Schnee). Die externen Mechanismen sind auch bei Eisbildung bedienbar.
Typ 4	IP56	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und windgetriebener Staub). Eindringen von Wasser (Regen, Schneeregen, Schnee, Spritzwasser und Wasser aus Schläuchen). Die Bildung von Eis außen am Gehäuse hat keine Beschädigungen zur Folge.
Typ 4X	IP56	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und windgetriebener Staub). Eindringen von Wasser (Regen, Schneeregen, Schnee, Spritzwasser und Wasser aus Schläuchen). Stellt einen zusätzlichen Schutz gegenüber Korrosion bereit. Die Bildung von Eis außen am Gehäuse hat keine Beschädigungen zur Folge.
Typ 6	IP67	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz). Eindringen von Wasser (Wasser aus Schläuchen und eindringendes Wasser bei gelegentlichem kurzzeitigen Untertauchen in geringer Tiefe). Die Bildung von Eis außen am Gehäuse hat keine Beschädigungen zur Folge.
Typ 6P	IP67	X	X	Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz). Eindringen von Wasser (Wasser aus Schläuchen und eindringendes Wasser bei längerem Untertauchen in geringer Tiefe). Stellt einen zusätzlichen Schutz gegenüber Korrosion bereit. Die Bildung von Eis außen am Gehäuse hat keine Beschädigungen zur Folge.

Tabelle 2.3. NEMA-Schutzarten für Gehäuse in nicht explosionsgefährdeten Bereichen (Fortsetzung)

Typ 12	IP52	X		Ohne Öffnungen. Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und aufgewirbelter Staub, Flusen, Fasern und Späne). Eindringen von Wasser (Tropf- und leichtes Spritzwasser).
Typ 12K	IP52	X		Mit Öffnungen. Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und aufgewirbelter Staub, Flusen, Fasern und Späne). Eindringen von Wasser (Tropf- und leichtes Spritzwasser).
Typ 13	IP54	X		Zugang zu gefährlichen Teilen und Eindringen fester Fremdkörper (herabfallender Schmutz und aufgewirbelter Staub, Flusen, Fasern und Späne). Eindringen von Wasser (Tropf- und leichtes Spritzwasser). Besprühen, Bespritzen und Einsickern von Öl und nicht korrosiven Kühlmitteln.

NEMA TS 2 ist ein führender Designleitfaden für Ausrüstung zur Verkehrssignalisierung.

- NEMA TS 2–2.2.7 Prüfverfahren: Transienten, Temperatur, Spannung und Feuchtigkeit
- NEMA TS 2–2.2.8 Vibrationsprüfung
- NEMA TS 2–2.2.9 Stoßprüfung (Schlag)

2.3.4 IK-Schutzart

Die IK-Schutzarten sind in IEC/EN 62262 zu finden, einer internationalen Norm, die den Schutzgrad gegen mechanischen Aufprall von außen festlegt. Ursprünglich 1994 als Europanorm EN 50102 genehmigt, wurde sie 2002 als internationale Norm übernommen.

Viele Hersteller testen die für die Produktlebensdauer wirksame Widerstandsfähigkeit an dessen schwächstem Teil.

Stufe	**IK01**	**IK02**	**IK03**	**IK04**	**IK05**	**IK06**	**IK07**	**IK08**	**IK09**	**IK10**	**IK11***
Krafteinwirkung (Joule)	0,14	0,2	0,35	0,5	0,7	1	2	5	10	20	50*
Masse (kg)	<0,2	<0,2	0,2	0,2	0,2	0,5	0,5	1,7	5	5	
Fallhöhe (mm)	56	80	140	200	280	400	400	300	200	400	

*Aufprall bis 50 J. Der Hersteller muss Energie, Masse und Fallhöhe des auftreffenden Gegenstands angeben.

2.4 Sonstige Zulassungen

2.4.1 Explosionsschutz

- IEC/EN/UL/SANS/CSA 60079-0 enthält allgemeine Anforderungen für Bau, Prüfung und Kennzeichnung von Ex-Ausrüstung und Ex-Komponenten (Ex = Explosionsgeschützt) für die Verwendung in explosionsgefährdeten Umgebungen.
- IEC/EN/UL/SANS/CSA 60079-1: Spezielle Anforderungen für Bau und Prüfung von elektrischer Ausrüstung mit der Schutzart feuerfestes Gehäuse „d" für die Verwendung in explosiven gashaltigen Atmosphären.

Vollständige Liste der Normen und Vorschriften zum Explosionsschutz vgl. Zertifikate *hier*

2.4.2 Zulassungen für Midspans

Wenn im Lieferumfang eines Produkts ein Midspan enthalten ist, erscheinen in diesem Abschnitt des Datenblatts Zulassungen, die sich speziell auf den Midspan beziehen. Die entsprechenden Erklärungen finden Sie im vorstehenden Abschnitt dieses Dokuments.

2.4.3 Sicherheit bei der Zutrittskontrolle

- UL 294: Beschreibt die Anforderungen zu Konstruktion, Leistung und Betrieb von Systemen zur Zutrittskontrolle.

3 Zertifikate

Wird eine Kamera in einer potenziell explosionsgefährdeten Umgebung installiert, muss das Gehäuse spezielle Sicherheitsnormen erfüllen. Diese sollen die Umgebung vor potenziellen Zündquellen schützen, die von der Kamera oder anderen Geräten ausgehen.

Europäische Produkte müssen die ATEX-Richtlinie erfüllen; diese entspricht dem internationalen Standard IECEx. In Nordamerika werden hauptsächlich die Class/Division Ratings nach NFPA70 (National Electric Code, NEC) und CSA C22.1 (Canadian Electric Code, CEC) angewendet, im Gegensatz zum Zonensystem in ATEX und IECEx.

Tabelle 3.1 Zertifikate

Vorschrift / Zertifikat	Region / Land
ATEX	EU
CCC Ex	China
cMETus / cULus	Kanada und USA
Zertifikat IA	Südafrika
IECEx	Internationale Zertifizierung von Geräten, die in Gefahrenbereichen eingesetzt werden
INMETRO	Brasilien
JPEx	Japan
KCs	Korea

Tabelle 3.1. Zertifikate (Fortsetzung)

OSHA Taiwan	Taiwan
PESO	Indien

Tabelle 3.2 Explosionsschutzarten

Klasse / Bereich	Atmo-sphäre	Definition	Zone (IECEx und ATEX)
Klasse I / Division 1	Gas	Bereich, in dem eine gefährliche explosionsfähige Atmosphäre langzeitig oder häufig vorhanden ist.	Zone 0
Klasse I / Division 1	Gas	Bereich, in dem sich im Normalbetrieb gelegentlich eine explosionsfähige Atmosphäre bildet.	Zone 1
Klasse I / Division 2	Gas	Bereich, in dem im Normalbetrieb eine explosionsfähige Atmosphäre normalerweise nicht oder nur kurzzeitig auftritt.	Zone 2
Klasse II / Division 1	Staub	Bereich, in dem eine gefährliche explosionsfähige Atmosphäre langzeitig oder häufig vorhanden ist.	Zone 20
Klasse II / Division 1	Staub	Bereich, in dem sich im Normalbetrieb gelegentlich eine explosionsfähige Atmosphäre bildet.	Zone 21
Klasse II / Division 2	Staub	Bereich, in dem im Normalbetrieb eine explosionsfähige Atmosphäre normalerweise nicht oder nur kurzzeitig auftritt.	Zone 22

4 Stromversorgung

4.1 PoE-Klassen (Power over Ethernet)

PoE-Klassen sorgen für eine effiziente Leistungsverteilung, indem sie die Leistung für jedes betriebene Gerät (Powered Device, PD) festlegen.

Tabelle 4.1 PoE-Klassen

Class	Typ	Garantierte Leistung am Energieversorger (PSE)	Maximalleistung des betriebenen Geräts (PD)
0	Typ 1, 802.3af	15,4 W	0,44 W bis 12,95 W
1	Typ 1, 802.3af	40,0 W	0,44 W bis 3,84 W
2	Typ 1, 802.3af	7,0 W	3,84 W bis 6,49 W
3	Typ 1, 802.3af	15,4 W	6,49 W bis 12,95 W
4	Typ 2, 802.3at*	30 W	12,95 W bis 25,5 W
6	Typ 3, 802.3bt	60 W	51 W
8	Typ 3, 802.3bt	100 W	71,3 W

* Dieser Typ wird auch als PoE+ bezeichnet.

5 Netzwerk

5.1 Schutz- und Sicherheitsmaßnahmen

Es gibt mehrere Möglichkeiten, um Bedrohungen für Systemressourcen abzuwehren. Manche Bedrohungen gefährden Geräte, andere wiederum gefährden Netzwerke oder die übertragenen/gespeicherten Daten. Hier einige ausgewählte Sicherheitskontrollen, die für Geräte und Netzwerke angewendet werden können:

- Zugangsdaten (Benutzername/Kennwort) verhindern unberechtigte Zugriffe auf Videomaterial und die unberechtigte Konfiguration von Geräten. Mit verschiedenen Benutzerebenen lässt sich steuern, wer Zugang zu welchen Inhalten und Funktionen hat.
- Eine IP-Adressfilterung (Firewall) reduziert die lokale Netzwerk-Exposition von Geräten und schützt diese so vor dem Zugriff durch unautorisierte Clients. Dies mindert die Risiken, falls die Kennwortsicherheit nicht mehr gegeben ist und falls eine neue kritische Sicherheitslücke erkannt wird.
- IEEE 802.1x: Schützt das Netzwerk vor nicht autorisierten Clients. 802.1x ist ein Schutz für die Netzwerk-Infrastruktur mithilfe verwalteter Switches und RADIUS-Server. Der 802.1x-Client im Gerät sorgt für die Authentifizierung des Gerätes im Netzwerk.
- HTTPS (Hypertext Transfer Protocol Secure): Schützt Daten (Video) vor Abhören des Netzwerks. Mit signierten Zertifikaten in HTTPS kann ein Video-Client erkennen, ob er auf eine legitime Kamera oder auf einen schädlichen Computer zugreift, der sich als eine Kamera ausgibt.
- Signierte Firmware: Wird vom Softwarehersteller implementiert, indem er das Firmware-Image mit einem geheimen privaten Schlüssel signiert. Wenn eine Firmware mit dieser Signatur versehen ist, validiert ein Gerät die Firmware, bevor es die Firmware akzeptiert und installiert. Wenn das Gerät erkennt, dass die Integrität der Firmware gefährdet ist, lehnt es das Firmware-Upgrade ab. Die von Axis signierte Firmware basiert auf dem in der Branche anerkannten Public-Key-Verschlüsselungsverfahren RSA.
- Sicheres Booten: Ein Bootvorgang, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt. Da sicheres Booten auf signierter Firmware basiert, ist sichergestellt, dass ein Gerät nur mit autorisierter Firmware hochfahren kann. Sicheres Booten gewährleistet, dass das Axis Gerät nach dem Zurücksetzen auf die Werkseinstellungen vollständig von möglicher Malware gereinigt ist.
- TPM: Ein Trusted Platform Module ist eine Komponente mit einem bestimmten Satz von kryptographischen Merkmalen, die geeignet sind, Informationen vor unbefugtem Zugriff zu schützen. Der private Schlüssel wird im TPM gespeichert, wo er dauerhaft bleibt. Alle kryptographischen Operationen, die eine Verwendung des privaten Schlüssels erfordern, werden zur Verarbeitung an das TPM gesendet. So wird sichergestellt, dass der geheime Teil des Zertifikats auch im Falle einer Sicherheitsverletzung sicher bleibt.
- Axis Edge Vault: Ein sicheres kryptografisches Rechenmodul (sicheres Modul oder sicheres Element), in dem die Axis Geräte-ID sicher und dauerhaft installiert und gespeichert wird.

Weitere Informationen zum Thema Cybersicherheit finden Sie unter *www.axis.com/de-de/cybersecurity*.

5.2 Unterstützte Protokolle

Bei der sicheren Datenübertragung zwischen vernetzten Geräten kommen verschiedene Protokolle zum Tragen.

5.2.1 Protokoll-Referenzmodelle

Den besten Überblick über die Interaktion der verschiedenen Protokolle bietet das Kommunikationsmodell Open Systems Interconnection (OSI). Außerdem gibt es das Referenzmodell TCP/IP.

5.2.1.1 OSI-Referenzmodell

Ein Modell zur Beschreibung der Datenkommunikation zwischen offenen Systemen. Zur Bereitstellung eines Dienstes nutzt jede Schicht die Dienste der direkt darunterliegenden Schicht. Jede Schicht muss bei der Ausführung von Diensten bestimmte Regeln oder Protokolle beachten.

Schicht 7 – Anwendungsschicht (Application Layer)

Macht Funktionen wie Web-, Datei- und E-Mail-Übertragung für Anwendungen verfügbar.

Die eigentlichen Anwendungen, wie Webbrowser oder E-Mail-Programme, arbeiten oberhalb dieser Schicht und werden vom OSI-Modell nicht abgedeckt.

Schicht 6 – Darstellungsschicht (Presentation Layer) (Daten)

Stellt sicher, dass die von der Anwendungsschicht eines Systems gesendeten Daten von der Anwendungsschicht eines anderen Systems gelesen werden können. Wandelt systemabhängige Datenformate wie ASCII in ein unabhängiges Format um, um einen syntaktisch richtigen Datenaustausch zwischen verschiedenen Systemen zu erlauben.

Schicht 5 – Sitzungsschicht (Session Layer) (Permanente Verbindung zwischen gleichrangigen Hosts)

Stellt einen anwendungsorientierten Dienst bereit und sorgt für die Prozesskommunikation zwischen zwei Systemen. Prozesskommunikation beginnt mit der Einrichtung einer Sitzung, die wiederum die Grundlage für eine virtuelle Verbindung zwischen zwei Systemen bildet.

Schicht 4 – Transportschicht (Transport Layer) (Ende-zu-Ende-Transport, verbindungsorientiertes Protokoll)

Stellt einen zuverlässigen Datenübertragungsdienst (über Ablaufsteuerung und Fehlerkontrolle) zu Schicht 5 und höher bereit.

Schicht 3 – Vermittlungsschicht (Network Layer, Pakete (Adressierung/Fragmentierung))

Führt die eigentliche Datenübertragung aus, indem sie Datenpakete zwischen Systemen verschiebt und weiterleitet. Erstellt und verwaltet Routingtabellen und liefert Optionen für die Kommunikation über die Netzwerk-Grenzen hinaus. Den Daten in dieser Schicht sind Ziel- und Quelladressen zugeordnet, die als Grundlage für die zielgerichtete Wegführung dienen.

Schicht 2 – Sicherungsschicht (Data Link Layer) (Blöcke/Frames)

Sorgt für die Datenübertragung und steuert den Zugang zum Übertragungsmedium durch die Zusammenfassung in Einheiten, so genannte Blöcke (Frames). Schicht 2 ist in zwei Unterschichten eingeteilt. LLC (Logical Link Control) ist die obere Schicht, die untere Schicht regelt die MAC-Adressen (MAC=Media Access Control). LLC vereinfacht den Datenaustausch, während MAC den Zugriff auf das Übertragungsmedium regelt.

Schicht 1 – Bitübertragungsschicht (Physical Layer) (Bits)

Stellt Services zur Unterstützung der Datenübertragung als Bitstrom über ein Medium bereit, z. B. eine Drahtverbindung oder drahtlose Übertragungsstrecke.

5.2.1.2 Transmission Control Protocol/Internet Protocol Referenzmodell

Das Referenzmodell TCP/IP stellt ein weiteres Modell zur Veranschaulichung von Protokollen und der Abwicklung von Kommunikation dar. Das TCP/IP-Referenzmodell umfasst vier Schichten, die den folgenden Schichten im OSI-Referenzmodell entsprechen:

Tabelle 5.1 Referenzmodelle im Vergleich

OSI-Modell	**TCP/IP-Modell**
Schicht 7 – Anwendungsschicht (Application Layer)	Schicht 4 – Anwendung
Schicht 6 – Darstellung	
Schicht 5 – Sitzung	
Schicht 4 – Transport	Schicht 3 – Vermittlung
Schicht 3 – Netzwerk	Schicht 2 – Verbundnetz
Schicht 2 – Datenverbindung	Schicht 1 – Netzwerkschnittstelle
Schicht 1 – Bitübertragung	

5.2.2 Protokolle der Anwendungsschicht

- **CIFS/SMB** (Common Internet File System/Server Message Block): Wird hauptsächlich für einen gemeinsamen Zugriff auf Dateien, Drucker und serielle Schnittstellen sowie verschiedene Kommunikationsaktivitäten zwischen den Knoten in einem Netzwerk verwendet.
- **DDNS** (Dynamic Domain Name System): Zur Nachverfolgung der Verknüpfung eines Domänennamens mit wechselnden IPv4-Adressen
- **DHCPv4/v6**(Dynamic Host Configuration Protocol): Automatische Zuweisung und Verwaltung von IP-Adressen
- **DNS/DNSv6** (Domain Name System): wandelt Domänennamen in die zugeordneten IP-Adressen um.
- **FTP** (File Transfer Protocol): Dient hauptsächlich zur Dateiübertragung von einem Server zu einem Client (Download) oder von einem Client zu einem Server (Upload). Kann auch zum Erstellen und Auswählen von Verzeichnissen sowie zum Umbenennen oder Löschen von Verzeichnissen und Dateien verwendet werden.
- **HTTP** (Hypertext Transfer Protocol): Dient vorrangig zum Laden von Text und Bildern von einer Webseite in einen Webbrowser. Netzwerk-Videosysteme bieten einen HTTP-Serverdienst, der Zugang zu den Systemen zum Herunterladen von Konfigurationen oder Livebildern über Webbrowser gewährt.
- **HTTP/2:** eine umfangreiche Überarbeitung des HTTP-Protokolls, definiert in RFC 7540 und freigegeben im Februar 2015.
- **HTTPS** (HTTP Secure): Eine Ergänzung des Hypertext Transfer Protocol (HTTP) zur sicheren Kommunikation über ein Computernetzwerk, im Internet häufig verwendet. In HTTPS ist das Kommunikationsprotokoll über Transport Layer Security (TLS) verschlüsselt.
- **MQTT** (Message Queuing Telemetry Transport): ein Standardprotokoll für das Internet der Dinge (IoT). Es wurde für eine vereinfachte IoT-Integration entwickelt und wird in einer Vielzahl von Branchen zum Anschließen von Remote-Geräten mit kleinem Code-Footprint und minimaler Netzwerk-Bandbreite verwendet.

- **NTP** (Network Time Protocol): Zur Synchronisierung der Zeit eines Computer-Clients oder -Servers mit einem anderen Server.
- **RTP** (Real-Time Transport Protocol): Ermöglicht die Übertragung von Echtzeitdaten zwischen den Endpunkten von Systemen.
- **RTCP** (Real-Time Control Protocol): Liefert Out-of-Band-Statistiken und Steuerungsdaten für eine RTP-Sitzung. Arbeitet bei der Lieferung und Paketdatenverarbeitung von Multimediadaten mit RTP zusammen, überträgt selbst aber keine Mediendaten.
- **RTSP** (Real-Time Streaming Protocol): Erweiterte Kontrolle über die Echtzeit-Übertragung von Medien.
- **SFTP** (Secure File Transfer Protocol): Sorgt für Dateizugriff, Dateiübertragung und Dateiverwaltung über jeden zuverlässigen Datenstrom.
- **SIP** (Session Initiation Protocol): Kommunikationsprotokoll für die Signalisierung und Steuerung von Multimedia-Kommunikationssitzungen.
- **SIPS** (Session Initiation Protocol Secure): verschlüsselte Version von SIP.
- **SMTP** (Simple Mail Transfer Protocol): Der Standard für die Übertragung von E-Mails über das Internet. Netzwerk-Kameras unterstützen SMTP, um E-Mail-Warnungen senden zu können.
- **SNMPv1/v2/v3** (Simple Network Management Protocol): zur Remote-Überwachung und -Verwaltung vernetzter Ausrüstung wie Switches, Router und IP-Kameras. Mit SNMP-Unterstützung können IP-Kameras durch Open-Source-Tools verwaltet werden.
- **SOCKS:** Ermöglicht die Übertragung von Netzwerk-Paketen zwischen Client und Server über einen Remote Network Proxy.
- **SRTP** (Secure Real-Time Transport Protocol): Ermöglicht die verschlüsselte Übertragung von Echtzeitdaten zwischen den Endpunkten eines Systems und ist damit eine sichere Variante von RTP.
- **SSH** (Secure Shell): Ermöglicht einen sicheren Zugang zu Netzwerk-Vorrichtungen über ein ungesichertes Netzwerk für Verwaltung und Fehlerbehebung.
- **TLSv1.2/v1.3** (Transport Layer Security): Handelt eine private, zuverlässige Verbindung zwischen Client und Server aus.

5.2.3 Protokolle der Transportschicht

- **TCP** (Transmission Control Protocol): Verbindungsorientierte und zuverlässige Lieferung von Datenströmen in der richtigen Reihenfolge. Häufigstes Datentransportprotokoll.
- **UDP** (User Datagram Protocol): Verbindungsloser Übertragungsdienst, favorisiert die zeitnahe Datenlieferung gegenüber der Zuverlässigkeit.
- **ICMP** (Internet Control Message Protocol): Sendet Fehlermeldungen und Betriebsdaten, die anzeigen, wenn ein angeforderter Dienst nicht verfügbar oder ein Host oder Router nicht erreichbar ist.

5.2.4 Protokolle der Netzwerk-Ebene

- **IGMPv1/v2/v3** (Internet Group Management Protocol): Wird von Computern und angrenzenden Routern in IPv4-Netzwerken zur Herstellung von Multicast-Gruppenmitgliedschaften verwendet. Ermöglicht bei Unterstützung dieser Art von Anwendungen eine effizientere Ressourcennutzung.

- **IPv4/IPv6** (Internet Protocol): Eine individuelle öffentliche Adresse, die für die Kommunikation internetfähiger Geräte untereinander benötigt wird. Die ursprüngliche Version IPv4 verwendet 32-Bit-Adressen. IPv6 ist die jüngste Version. Sie verwendet 128-Bit-Adressen, die in acht Gruppen zu je vier Hexadezimalstellen eingeteilt sind.
- **USGv6:** Ein technisches Standardprofil für IPv6, definiert von der US-Regierung, um die Kompatibilität bei der Beschaffung von IPv6-kompatiblen Netzwerk-Geräten sicherzustellen.

5.2.5 Protokolle der Datenverbindungsschicht

- **ARP** (Address Resolution Protocol): Dient zur Erkennung der MAC-Adresse des Zielgeräts.
- **CDP** (Cisco Discovery Protocol): proprietäres Protokoll von Cisco als Alternative zu LLDP zur Ermittlung von Informationen über die angeschlossenen Hardwaregeräte.
- **IEEE 802.3 (i, u, ab):** Ethernet-Normen zur Festlegung der Datenkommunikation mit 10 Mbit/s (10Base-T), 100 Mbit/s (100Base-TX) und 1Gbit/s (1000Base-T) über verdrillte Doppelkabel.
- **LLDP** (Link Layer Discovery Protocol): Dient zur Bekanntgabe der Identität und Funktionen eines Geräts sowie anderer innerhalb desselben Netzwerks angeschlossener Geräte.

5.2.6 Protokolle zur Ermittlung

- **mDNS (Bonjour):** Kann zur Erkennung von Netzwerk-Videoprodukten über Mac-Computer oder als Discovery Protocol für neue Geräte in einem beliebigen Netzwerk verwendet werden.
- **UPnP** (Universal Plug and Play): Microsoft-Betriebssysteme können Ressourcen (Axis Geräte) in einem Netzwerk automatisch erkennen.
- **Zeroconf:** Weist einem Netzwerk-Gerät automatisch eine ungenutzte IP-Adresse zwischen 169.254.1.0 und 169.254.254.255 zu.

5.2.7 Quality of Service

In einem IP-Netzwerk muss die gemeinsame Nutzung der Netzwerkressourcen kontrolliert werden, damit die Anforderungen eines jeden Dienstes erfüllt werden.

- **QoS** (Quality of Service): Fähigkeit zur Priorisierung des Netzwerkverkehrs, bei der Datenströme mit hoher Priorität vor solchen mit niedrigerer Priorität gesendet werden. Durch eine Regelung der Bandbreitennutzung einzelner Anwendungen und die daraus folgende Konfliktvermeidung erhöht sich die Zuverlässigkeit innerhalb des Netzwerks.
- **DiffServ:** Das Netzwerk versucht, einen bestimmten Service basierend auf der von jedem Paket festgelegten QoS zu leisten.

5.2.8 Datenübertragungsverfahren

Es gibt drei Methoden zur Übertragung von Daten über ein Computernetzwerk.

- **Unicasting:** Häufigste Methode, bei der Sender und Empfänger auf Punkt-zu-Punkt-Basis kommunizieren. Die Datenpakete werden nur an einen Empfänger gesendet, keine anderen Geräte erhalten diese Informationen.
- **Multicasting:** Ein einzelner Sender kommuniziert mit mehreren Empfängern in einem Netzwerk. Reduziert die Netzwerkauslastung, indem ein einzelner Datenstrom an viele Empfänger gesendet wird.

- **Broadcast:** Der Absender sendet dieselben Informationen an alle anderen Server in einem Netzwerk. Alle Netzwerk-Hosts erhalten die Nachricht und übernehmen einen Teil der Verarbeitung.

Über Axis Communications

Axis ermöglicht eine intelligente und sichere Welt durch Lösungen zur Verbesserung der Sicherheit und Geschäftsperformance. Als Unternehmen für Netzwerktechnologie und Branchenführer bietet Axis Lösungen in den Bereichen Videosicherheit, Zutrittskontrolle sowie Intercoms und Audiosysteme. Sie werden verstärkt durch intelligente Analyseanwendungen und unterstützt durch gute Schulungen.

Axis beschäftigt rund 4.000 engagierte Mitarbeiter in über 50 Ländern und arbeitet weltweit mit Technologie- und Systemintegrationspartnern zusammen, um den Kunden Lösungen anbieten zu können. Axis wurde 1984 gegründet und der Hauptsitz befindet sich in Lund, Schweden