White Paper

Kurzanleitung zu Axis Datenblättern

Zulassungen, Zertifikate und Protokolle

März 2021

AXIS COMMUNICATIONS

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 Abkürzungen, Zulassungen, Zertifikate und Protokolle.

In der aktuellen Version enthält dieses Dokument Informationen zu den Datenblatt-Abschnitten, die im nachfolgend abgebildeten Datenblatt markiert und vergrößert sind. Darüber hinaus behandeln wir die Nom EN 62676 (Anwendungsregeln).

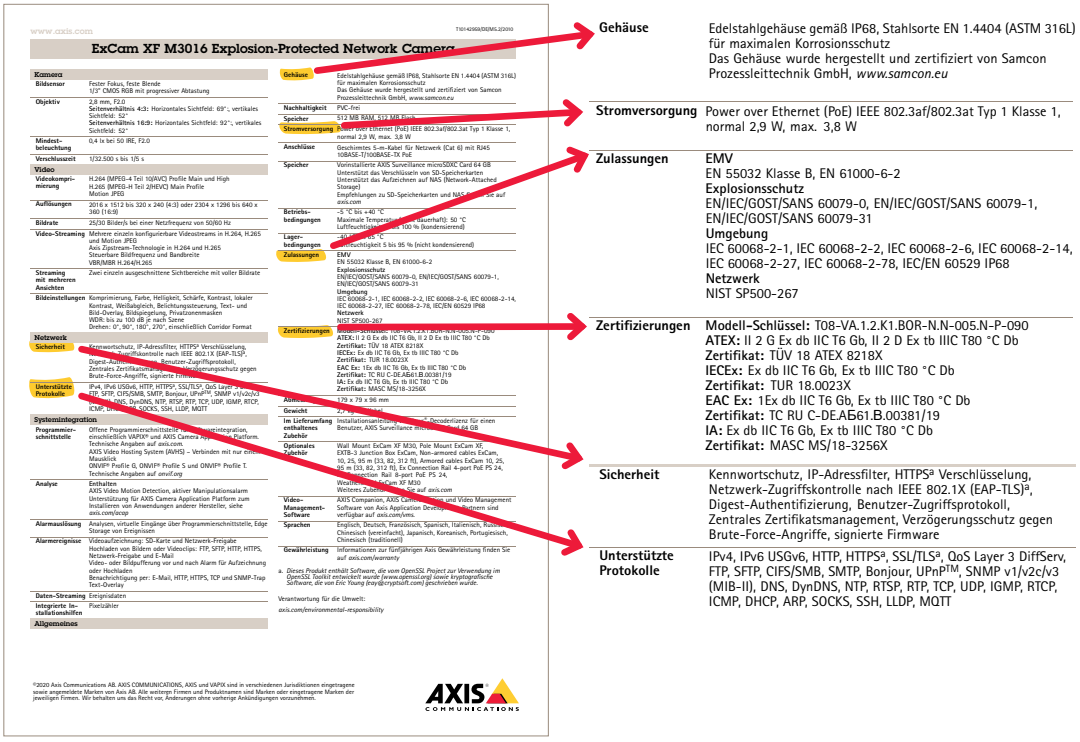

Abbildung 1. Markierung der Axis Datenblatt-Abschnitte, die im vorliegenden Dokument behandelt werden.

2. Zulassungen

Der Abschnitt Zulassungen in den Datenblättern von Axis betrifft die Einhaltung verschiedener Normen und Standards. Dieser Abschnitt ist häufig in die Unterabschnitte zu EMV, Sicherheit, Umwelt und Sonstiges unterteilt, wobei sich „Sonstiges" z. B. auf den Explosionsschutz oder die Sicherheit bei der Zutrittskontrolle beziehen 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. Obwohl die Hersteller eine solche Bescheinigung unter bestimmten Umständen auch selbst ausstellen können, beauftragen die meisten Hersteller akkreditierte Prüflabore, die die Einhaltung in Form von Prüfberichten nachweisen. EMV-Zulassungen bestehen aus zwei Teilen: Emissionen und Störfestigkeit, siehe unten.

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 die globalen Richtlinien nicht mit einem einzelnen Test überprüft werden können, kann für jede Region/Anwendung ein anderer Code gelten.

2.1.1 Normen zu informationstechnischen Einrichtungen (ITE)

> EN 55022 Class A: Emissionsnorm (kommerziell, industriell, geschäftlich), mit internationalen Normen harmonisiert

> EN 55022 Class B: Emissionsnorm (Wohnbereich), mit internationalen Normen harmonisiert

> EN 55024 Class A: Störfestigkeitsnorm (kommerziell, industriell), mit internationalen Normen harmonisiert

> EN 55024 Class B: Störfestigkeitsnorm (Wohnbereich), mit internationalen Normen harmonisiert

2.1.2 Harmonisierte Normen nach Land/Region

> EN 61000-6: Allgemeine Standards zur Einhaltung (Europa)

> FCC Part 15 Subpart B Klasse A und B: Die FCC legt Regeln und Richtlinien für Telekommunikationsgeräte fest. Diese betreffen die Abstrahlung, nicht die Störfestigkeit (USA).

> ICES-003 Klasse A und B (Kanada)

> VCCI (Japan)

> KN22, KN24, KN32, KN35 (Korea)

> CISPR 22 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 Komponenten von Alarmsystemen einschließlich Zutrittskontrollsystemen, CCTV-Systemen, Branderkennungs- und Feueralarmsystemen, Überfall- und Einbruchmeldeanlagen und Hausnotrufsystemen.

> EN 55032 (Emission) – EN 55035 (Störfestigkeit): Gilt für Multimediageräte (MME) mit einer AC- oder DC-Spannungsversorgung bis einschließlich 600 V. Multimediageräte (MME) sind informationstechnische Einrichtungen (ITE), Audioanlagen, Videoanlagen, Rundfunkempfangsgeräte, Studio-Lichtsteuereinrichtungen.

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 60950-1: Nachweisprüfung von Netzwerk-Kameras, Encodern, Netzteilen gegenüber Anforderungen zur Verringerung der Gefahr von Feuer, Elektroschocks oder Verletzungen jeglicher Personen, die das Gerät berühren.

> IEC/EN/UL 60950-22: Spezifische Sicherheitsanforderungen für Outdoor-Produkte und Gehäuse für Außenaufstellung.

> IEC/EN 62471: Anforderungen für Expositionsgrenzwerte, verhindert eine Gefährdung von Augen und Haut.

> EN 62368-1: Ersetzt die Norm EN 60950, bis 2019 existieren beide noch nebeneinander. IEC und UL entwickeln Schwesternormen mit denselben Nummern.

> EN/UL/CSA 60065: Gilt für elektronische Geräte, die von der Hauptstromversorgung, von einer Versorgungsvorrichtung, aus Batterien oder Fernspeisung mit Strom versorgt werden und für den Empfang, die Erzeugung, Aufzeichnung bzw. Reproduktion von Audio, Video und den zugehörigen Signalen vorgesehen sind.

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 1. IP-Schutzarten, erste Kennziffer (IP**x**y) – feste Fremdkörper

Stufe (x)	Schutz vor	Wirksamkeit
0	Kein Schutz	Kein Schutz
1	Fremdkörper über 50 mm	Große Oberfläche des Körpers, wie ein Handrücken, allerdings kein Schutz gegen absichtlichen Kontakt mit einem Körperteil.
2	Fremdkörper über 12,5 mm	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.
3	Fremdkörper über 2,5 mm	Gegenstände wie Werkzeug und dicke Kabel dürfen überhaupt nicht eindringen.
4	Fremdkörper über 1 mm	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. IP-Schutzart, zweite Kennziffer (IPx**y**) – Flüssigkeiten

Stufe (y)	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 kein Wasser in schädlichen Mengen 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 für IPX7 (siehe oben).
9	Wasser von Hochdruck- und Dampfstrahlreinigung	Wasser, das aus jeder Richtung unter stark erhöhtem Druck gegen das Gehäuse gerichtet ist, darf keine schädliche Wirkung haben.

2.3.2 Weitere relevante IEC-Normen

> Die Norm IEC 60068-2 beschreibt Verfahren zur Prüfung elektronischer Geräte und Produkte, die deren Funktionstüchtigkeit unter bestimmten Umgebungseinflüssen bewerten, wie z. B. extremer Kälte und trockener Wärme. In der Regel sind die nachfolgend aufgeführten Verfahren dieser Norm für Objekte vorgesehen, die während des Prüfverfahrens temperaturstabil sind.

- 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 60068-2-30: Feuchte Wärme (zyklisch)
- IEC 60068-2-64: Schwingen (Breitbandrauschen)
- IEC 60068-2-78: Feuchte Wärme (konstant)

> Die Norm IEC 60825 Klasse I stellt sicher, dass der verwendete Lasertyp im Laser-Fokussiermodul unter normalen Anwendungsbedingungen sicher ist.

2.3.3 NEMA-Schutzart

Die NEMA (National Electrical Manufacturers Association) ist eine amerikanische Vereinigung, die Normen für Gehäuse elektrischer Geräte herausgibt. Die NEMA hat weltweit ihre eigene Norm NEMA 250 eingeführt. Über das American National Standards Institute (ANSI) hat die NEMA mit der ANSI/IEC 60529 außerdem eine harmonisierte IP-Norm 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 dem Normenwerk NEMA 250. Die NEMA lässt eine Selbstzertifizierung zu, während die Einhaltung der UL-Normen durch externe Test- und Prüfverfahren nachzuweisen ist.

Tabelle 3. NEMA-Schutzarten für Gehäuse in nicht explosionsgefährdeten Bereichen

NEMA	Äquivalente IP-Schutzart	Innen-bereich	Außen-bereich	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.
NEMA 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.
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.

2.3.4 IK-Schutzart

Die IK-Schutzarten sind in der internationalen Norm IEC/EN 62262 festgelegt, die den Schutz gegen äußere mechanische Beanspruchung definiert. Das erstmals 1994 als europäische Norm EN 50102 angenommene Regelwerk wurde 2002 zur internationalen Norm.

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

Tabelle 4. IK-Schutzarten

Stufe	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
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	

*Schlag mit bis zu 50 J. Der Hersteller muss Schlagenergie, Masse und Fallhöhe des Schlagelements 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 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.

2.4.2 Midspan-Zulassungen

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, der die internationale Norm IECEx entspricht.

Kennzeichnung explosionsgefährdeter Betriebsmittel nach ATEX 2014/34/EU

Einteilung und Kennzeichnung explosionsgefährdeter Bereiche

Brennbare Stoffe	Temporäres Verhalten brennbarer Stoffe im Ex-Bereich, Explosionsfähiges Medium	Einteilung explosionsgefährdeter Bereiche	Kennzeichnung der Betriebsmittel: Gerätegruppe	Kennzeichnung der Betriebsmittel: Gerätekategorie	Geräteschutzniveau (EPL)
Gase Nebel Dämpfe	ist ständig, langzeitig oder häufig vorhanden	Zone 0	II	1G	Ga
	tritt gelegentlich auf	Zone 1	II	2G	Gb
	tritt wahrscheinlich nicht auf, und wenn, dann nur selten oder kurzfristig	Zone 2	II	3G	Gc
Stäube	ist ständig, langzeitig oder häufig vorhanden	Zone 20	II	1D	Da
	tritt gelegentlich auf	Zone 21	II	2D	Db
	tritt durch aufgewirbelten Staub wahrscheinlich nicht auf bzw. selten/kurzzeitig	Zone 22	II	3D	Dc

Notifizierte Stellen

Kennnummer	Notifizierte Stelle
0102	PTB (Deutschland)
0158	EXAM (Deutschland)

Einteilung in Explosionsgruppen und Temperaturklassen

Explosionsgruppe	Verschiedene Beispiele in Abhängigkeit der - Explosionsgruppe - Temperaturklasse					
IIA	Ammoniak Methan Ethan Propan	Ethylalkohol Cyclohexan n-Butan	Benzin Diesel Heizöl n-Hexan	Acetaldehyd		
IIB	Stadtgas Acrylnitril	Ethylen Ethylenoxid	Ethylglycol Schwefelwasserstoff	Ethylether		
IIC	Wasserstoff	Acetylen				Schwefelkohlenstoff

Achtung: die Liste ist nur ein Auszug explosionsfähiger Stoffe!

Temperaturklassen	
T1	<450 °C
T2	<300 °C
T3	<200 °C
T4	<135 °C
T5	<100 °C
T6	<85 °C

Einsetzbarkeit des Betriebsmittels bei Temperaturklassen T1 bis T6. Die Temperaturklasse zeigt die höchstzulässige Oberflächentemperatur des Betriebsmittels. Beim Staubexplosionsschutz wird die max. Oberflächentemperatur direkt angegeben (z. B. T80 °C).

Beispiel:

CE 0158 Ex

II 2 G	Ex	db	IIC	T6	Gb	NB 12 ATEX 1007 X
II 2 D	Ex	tb	IIIC	T80°C	Db	

Schutzprinzip	Zündschutzart	Kennzeichnung	Einsatz in Zone	CENELEC
Übertragung einer Explosion nach aussen wird ausgeschlossen	druckfeste Kapselung	Ex d	a b c	0, 1, 2 1, 2 2	EN 60079-1
Vermeidung von Funken und zu hohen Temperaturen	erhöhte Sicherheit	Ex e	b c	1, 2 2	EN 60079-7
Energiebegrenzung des Stromkreises, von Funken und Temperaturen	Eigensicherheit	Ex i	a b c	0, 1, 2, 20, 21, 22 1, 2, 21, 22 2, 22	EN 60079-11
Ex-Atmosphäre wird von der Zündquelle ferngehalten	Überdruck-Kapselung	Ex p	xb yb zc	1, 2, 21, 22 1, 2, 21, 22 2, 22	EN 60079-2
Ex-Atmosphäre wird von der Zündquelle ferngehalten	Vergussmasse	Ex m	a b c	0, 1, 2, 20, 21, 22 1, 2, 21, 22 2, 22	EN 60079-18
Ex-Atmosphäre wird von der Zündquelle ferngehalten	Ölkapselung	Ex o	b c	1, 2 2	EN 60079-6
Übertragung einer Explosion nach aussen wird ausgeschlossen	Sandkapselung	Ex q	b	1, 2	EN 60079-5
Jeweils wie vor, jedoch für Einsatz in Zone 2	Zündschutzart "n"	Ex n	C R	2 2	EN 60079-15
Staubexplosionsschutz	Schutz durch Gehäuse	Ex t	a b c	20, 21, 22 21, 22 22	EN 60079-31

Schutzprinzip – Zündschutzarten – Normen – EN 60079-0 Allgemeine Anforderungen

Kennzeichnung	Staubgruppen
IIIA	brennbare Flusen
IIIB	nicht leitfähiger Staub
IIIC	leitfähiger Staub

IP	Berührungs- und Fremdkörperschutz	Wasserschutz
8	-	dauerndes Untertauchen
7	-	zeitweiliges Untertauchen
6	staubdicht	starkes Strahlwasser
5	staubgeschützt	geschützt gegen Strahlwasser
4	Fremdkörper > Ø 1 mm	geschützt gegen Spritzwasser
3	Fremdkörper > Ø 2,5 mm	geschützt gegen Spritzwasser
2	Fremdkörper > Ø 12,5 mm	Tropfwasser mit 15° Neigung
1	Fremdkörper > Ø 50 mm	geschützt gegen Tropfwasser
0	nicht geschützt	nicht geschützt

Gehäuseschutz IEC EN 60529

Bedingungen	Kennzeichnung
Das Betriebsmittel ist ohne Einschränkung einsetzbar	-
Beim Einsatz des Betriebsmittels sind besondere Bedingungen zu beachten	X
Das Betriebsmittel ist ein Ex-Bauteil mit Teilbescheinigung und somit alleine nicht einsatzfähig Die CE-Konformität wird mit dem Einbau in ein komplettes Betriebsmittel bescheinigt	U

Zusatzinformation

4. Power (Strom)

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 6. PoE-Klassen

Klasse	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	4,0 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 4, 802.3bt	100 W	71,3 W

* Dieser Typ wird auch als PoE+ bezeichnet.

5. Network (Netzwerk)

5.1 Schutz- und Sicherheitsmaßnahmen

Es gibt verschiedene Möglichkeiten, möglichen Bedrohungen von Systemen entgegenzuwirken. Manche Bedrohungen stellen Risiken für Geräte dar, andere für Netzwerke bzw. für gespeicherte oder übertragene Daten. Beispiele für mögliche Sicherheitsmaßnahmen zum Schutz von Geräten und Netzwerken:

> 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-Filterung (Firewall) reduziert die lokale Netzwerk-Exposition von Geräten und schützt diese so vor dem Zugriff durch unautorisierte Clients. Dies mindert die Risiken bei einer nicht mehr gegebenen Kennwortsicherheit und bei Erkennung einer neuen kritischen Sicherheitslücke.

> 802.1X schützt das Netzwerk vor unautorisierten Clients. 802.1X schützt mithilfe von verwaltbaren Switches und eines RADIUS-Servers die Netzwerkinfrastruktur. Der 802.1X-Client im Gerät sorgt im Netzwerk für die Authentifizierung gegenüber dem Gerät.

> HTTPS (Hypertext Transfer Protocol Secure) schützt Daten (Videomaterial) vor unberechtigtem Abhören im Netzwerk. Anhand signierter Zertifikate in HTTPS erkennen Video-Clients, ob sie auf eine legitime Kamera oder einen angreifenden Computer zugreifen, der als Kamera getarnt ist.

Weitere Informationen zum Thema Cybersicherheit finden Sie unter www.axis.com/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.

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

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.

Beispiele
> Telnet
> Apple Filing Protocol

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.

Beispiele
> Remote Procedure Call (RPC)
> Network File System (NFS)

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.

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

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 Netzwerkgrenzen hinaus. Den Daten in dieser Schicht sind Ziel- und Quelladressen zugeordnet, die als Grundlage für die zielgerichtete Wegführung dienen.

Beispiele
> IP (Internet-Protokoll): Eine individuelle öffentliche Adresse, die für die Kommunikation Internet-fähiger Geräte benötigt wird
> IPv4: Ursprüngliche IP-Version, verwendet 32-Bit-Adressen
> IPv6: Jüngste IP-Version, verwendet 128-Bit-Adressen, die in acht Gruppen zu je vier Hexadezimalziffern eingeteilt sind.
> Routing Information Protocol
> Internet Protocol Security (IPSec)

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 Unter-Schichten (Sub Layers) unterteilt. Die obere Schicht entspricht der LLC (Logical Link Control), die untere MAC (Media Access Control). LLC vereinfacht den Datenaustausch, MAC steuert den Zugriff auf das Übertragungsmedium.

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

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 7. Referenzmodelle im Vergleich

OSI-Modell	TCP/IP-Modell
Schicht 7 – Anwendung	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 zur Verwaltung von IP-Adressen

DHCP (Dynamic Host Configuration Protocol): Automatische Zuweisung und Verwaltung von IP-Adressen

DNS (Domain Name System): Wandelt Domänennamen in die zugehörigen IP-Adressen um, operiert in der Transportschicht

DynDNS (Dynamic Domain Name System): Zur Nachverfolgung der Verknüpfung eines Domänennamens mit wechselnden IPv4-Adressen

UPnP (Universal Plug and Play): Microsoft-Betriebssysteme können Ressourcen (Axis Geräte) in einem Netzwerk automatisch erkennen.

Zeroconf: Weist einem Netzwerkgerät automatisch eine ungenutzte IP-Adresse zwischen 169.254.1.0 und 169.254.254.255 zu.

Bonjour: Kann zur Erkennung von Netzwerk-Videoprodukten über Mac-Computer oder als Discovery Protocol für neue Geräte in einem beliebigen Netzwerk verwendet werden.

ARP (Address Resolution Protocol): Zur Erkennung der MAC-Adresse des Zielgeräts.

5.2.3 Protokolle der Anwendungsschicht

HTTP (Hypertext Transfer Protocol): Dient vorrangig zum Laden von Text und Bildern von einer Webseite in einen Webbrowser. Netzwerkvideosysteme bieten einen HTTP-Serverdienst, der Zugang zu den Systemen zum Herunterladen von Konfigurationen oder Livebildern über Webbrowser gewährt.

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.

FTP (File Transfer Protocol): Dient hauptsächlich für die 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.

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.

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.

SNMP (Simple Network Management Protocol): Dient zur Fernüberwachung und -Verwaltung von vernetzten Geräten wie Switches, Router und Netzwerk-Kameras. Netzwerk-Kameras mit SNMP-Unterstützung können über Open-Source-Tools verwaltet werden.

SIP (Session Initiation Protocol): Kommunikationsprotokoll für die Signalisierung und Kontrolle von Multimedia-Kommunikationssitzungen.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Handelt eine überprüfte und verschlüsselte Verbindung zwischen dem Client und dem Server aus. SSL war der Vorgänger des aktuellen Standards TLS.
LLDP (Link Layer Discovery Protocol): Dient zur Bekanntgabe der Identität und Funktionen eines Geräts sowie anderer innerhalb desselben Netzwerks angeschlossener Geräte.

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.

NTP (Network Time Protocol): Zur Synchronisierung der Zeit eines Computer-Clients oder -Servers mit einem anderen Server.

SFTP (Secure File Transfer Protocol): Sorgt für Dateizugriff, Dateiübertragung und Dateiverwaltung über jeden zuverlässigen Datenstrom.

IGMP (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.

5.2.4 Datentransportprotokolle

TCP (Transmission Control Protocol): Verbindungsorientierte, zuverlässige und der Reihe nach erfolgende Lieferung von Datenströmen. 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.

5.2.5 Unicast, Broadcast und Multicast

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.

5.2.6 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.

6. Normgerechte Planung nach DIN EN 62676

Um eine nachhaltige Planung und Nutzung einer Videosicherheitsanlage sicherstellen zu können sind folgende Normen einzuhalten:

6.1 Videoüberwachungsanlagen für Sicherheitsanwendungen – Systemanforderungen – Allgemeines

Die DIN EN 62676-1-1 legt die Mindestanforderungen fest und gibt Empfehlungen für Videosicherheitsanlagen (VSS), die bisher als CCTV-Anlagen bezeichnet wurden und für Sicherungsaufgaben installiert werden. Diese Norm legt die Mindestanforderungen an die Leistung und Funktion fest, die zwischen Kunde, Polizei (sofern zutreffend) und Lieferer in Form der Leistungsbeschreibung zu vereinbaren sind, enthält aber keine Anforderungen an Entwurf, Planung, Installation, Prüfung, Betrieb oder Instandhaltung. Diese Norm schließt die Installation von fernüberwachten, detektoraktivierten VSS aus.

6.2 Videoüberwachungsanlagen für Sicherungsanwendungen – Systemanforderungen – Allgemeine Anforderungen an die Videoübertragung

Die DIN EN 62676-1-2 legt allgemeine Anforderungen an die Videoübertragung fest. Diese Norm behandelt die allgemeinen Anforderungen an die Videoübertragung hinsichtlich der Leistung, der Sicherheit und der Konformität bezüglich grundlegender IP-Konnektivität auf der Grundlage eingeführter internationaler Standards.

6.3 Videoüberwachungsanlagen für Sicherungsanwendungen – Anwendungsregeln

Die DIN EN 62676-4 enthält Empfehlungen und Anforderungen für die Auswahl, Planung, Errichtung, Inbetriebnahme, Instandhaltung und Prüfung von Videosicherheitsanlagen (VSS), welche Bildaufnahmeeinrichtung(en), Verbindung(en) und Bildverarbeitungseinrichtung(en) für die Verwendung in Sicherungsanwendungen umfassen.
Die Ziele dieses Teils der Normenreihe IEC 62676 sind

> die Bereitstellung eines Rahmenwerks zur Unterstützung von Kunden, Errichtern und Anwendern bei der Aufstellung ihrer Anforderungen
> die Unterstützung von Spezifikationserstellern und Anwendern bei der Bestimmung der zweckmäßigen Einrichtung, die für eine gegebene Anwendung erforderlich ist
> die Bereitstellung von Mitteln für die objektive Bewertung des Leistungsvermögens der VSS.

Eine der bekanntesten Punkte der Norm ist die Definition der Auflösung am Objekt in der Szene.

EN 62676-4 (Juli 2016)						
	Überwachen	Detektieren	Beobachten	Erkennen	Identifizieren	Begutachten
Szenenbreite (mm/Px)	80	40	16	8	4	1
Pixel / Meter*	12,5	25	62,5	125	250	1000
Pixel / 16cm* (Gesicht)	2	4	10	20	40	160

* ist nicht Bestandteil der Norm

DE/R1/2103

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videoüberwachung/-analyse und Zutrittskontrolle sowie Sprechanlagen und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen über Axis finden Sie unter www.axis.com