

# Krótki przewodnik po arkuszach danych Axis

Aprobaty, świadectwa i protokoły

Maj 2022

# Spis treści

1	Wprowadzenie	3
2	Aprobaty	3
	2.1 EMC (kompatybilność elektromagnetyczna)	3
	2.2 Bezpieczeństwo	5
	2.3 Środowisko	5
	2.4 Inne aprobaty	9
3	Świadectwa	9
4	Zasilanie	10
	4.1 Klasy Power over Ethernet (PoE)	10
5	Sieć	11
	5.1 Ochrona i sterowanie zabezpieczeniami	11
	5.2 Obsługiwane protokoły	12



Wymagania w zakresie *emisji* dotyczą zdolności urządzenia do zadowalającego działania bez emitowania zbyt dużej energii elektromagnetycznej, która mogłaby zakłócać działanie innych urządzeń w tym samym środowisku.

*Odporność* jest miarą zdolności produktów elektronicznych do tolerowania wpływu zjawisk elektromagnetycznych i energii elektrycznej (przekazywanej przez promieniowanie lub przewodzenie) pochodzącej z innych produktów elektronicznych. W Europie wymagania w zakresie EMC są uwzględnione w warunkach oznakowania CE, które z kolei wynikają ze zharmonizowanego ustawodawstwa UE.

Normy wymienione poniżej określają ograniczenia i metody badania emisji oraz odporności elektromagnetycznej. Ponieważ nie istnieje jedna metoda badania, która weryfikowałaby wymagania obowiązujące we wszystkich regionach świata, dla różnych regionów i zastosowań mogą obowiązywać różne kody.

### **2.1.1 Normy dotyczące urządzeń techniki informacyjnej (ITE)**

Te normy mają zastosowanie do urządzeń multimedialnych (MME), których znamionowa wartość skuteczna napięcia zasilania AC lub napięcia zasilania DC nie przekracza 600 V. Urządzenie multimedialne (MME) jest zdefiniowane jako urządzenie techniki informacyjnej (ITE), urządzenie audio, urządzenie wideo, odbiornik sygnałów emitowanych przez nadawców lub urządzenie do sterowania oświetleniem o zastosowaniu rozrywkowym.

- EN 55032, klasa A: norma emisji (w środowiskach prowadzenia działalności handlowej i innej działalności gospodarczej, w tym przemysłowych), zharmonizowana z normami międzynarodowymi
- EN 55032, klasa B: norma emisji (w środowiskach mieszkalnych), zharmonizowana z normami międzynarodowymi
- EN 55035: norma odporności, zharmonizowana z normami międzynarodowymi

### **2.1.2 Normy zharmonizowane z podziałem na kraje/regiony**

- EN 61000-6-1 i EN 61000-6-2: normy ogólne (Europa)
- Punkt B Części 15 przepisów FCC w zakresie klasy A i B: Federalna Komisja Łączności (FCC) formułuje i egzekwuje w Stanach Zjednoczonych reguły i przepisy obowiązujące w odniesieniu do emisji (nie odporności) urządzeń telekomunikacyjnych
- ICES-3 (A i B) / NMB-3 (A i B) (Kanada)
- VCCI, klasa A i B (Japonia)
- KS C 9832, klasa A i B, KS C 9835, KS C 9547, KS C 9815 (Korea)
- RCM AS/NZS CISPR 32, klasa A i B (Australia / Nowa Zelandia)

### **2.1.3 Dodatkowe normy wg zastosowania/produktu**

- EN 50121-4, IEC 62236-4: określa kryteria jakości pracy dla urządzeń sterowania ruchem kolejowym i urządzeń telekomunikacyjnych (S&T), które mogą zaburzać pracę innych urządzeń w środowisku kolejowym
- EN 50130-4: określa wymagania dotyczące urządzeń systemów alarmowych, w tym systemów kontroli dostępu, CCTV, wykrywania pożaru i sygnalizacji pożaru, sygnalizacji włamania, sygnalizacji napadu i zagrożeń w domu

## 2.2 Bezpieczeństwo

- Dyrektywa dotycząca sprzętu elektrycznego do stosowania w określonych granicach napięcia (2014/35/UE): zawiera szeroko sformułowane cele w dziedzinie bezpieczeństwa sprzętu elektrycznego. Przestrzeganie jej zapewnia możliwość bezpiecznego używania produktów bez ryzyka odniesienia obrażeń lub uszkodzenia mienia.
- IEC/EN/UL 62368-1: określa wymagania, jakie muszą spełniać kamery sieciowe, kodery i zasilacze, aby ograniczone było ryzyko pożaru, porażenia prądem elektrycznym lub odniesienia obrażeń ciała przez osoby mające kontakt z tym sprzętem
- IEC/EN/UL 60950-22: konkretne wymagania w zakresie bezpieczeństwa produktów i obudów przeznaczonych do instalowania na zewnątrz budynków
- IEC/EN 62471-1: wymagania w zakresie bezpieczeństwa fotobiologicznego lamp i systemów lampowych, z określeniem wartości granicznych ekspozycji; służy ochronie oczu i skóry
- EN/UL/CSA 60065: dotyczy sprzętu elektronicznego, zasilanego z sieci, przez zasilacze, z baterii lub z zasilaczy zewnętrznych, przeznaczonego do odbioru, wytwarzania, zapisywania lub odtwarzania odpowiednio sygnałów audio, video i towarzyszących
- IS 13252: określa obowiązujące w Indiach wymagania, jakie muszą spełniać kamery sieciowe, kodery i zasilacze, aby ograniczone było ryzyko pożaru, porażenia prądem elektrycznym lub odniesienia obrażeń ciała przez osoby mające kontakt z tym sprzętem

## 2.3 Środowisko

### 2.3.1 Klasa IP

Norma IEC 60529 wydana przez Międzynarodową Komisję Elektrotechniczną definiuje klasyfikację IP (ochrona przed penetracją / międzynarodowa norma ochrony) w postaci zbioru dwucyfrowych kodów. Każdy kod określa stopień ochrony urządzeń elektrycznych przed wnikaniem ciał stałych lub kurzu, przypadkowym kontaktem i wodą.

*Tabela 2.1 Stopnie IP – pierwsza cyfra IP: ciała stałe*

Sto- pień	Ochrona przed	Skuteczność wobec
0	Brak ochrony	Brak ochrony
1	Przedmiotami większymi niż 50 mm	Dużych powierzchni ciała, takich jak wierzch dłoni, ale brak ochrony przed umyślnym kontaktem z częścią ciała.
2	Przedmiotami większymi niż 12,5 mm	Palce i inne przedmioty mogą spenetrować sprzęt na głębokość maksymalnie 80 mm, przy założeniu, że do tej głębokości nie występuje zagrożenie ze strony niebezpiecznych części. Przedmioty o średnicy 12,5 mm nie spenetrują w całości sprzętu.
3	Przedmiotami większymi niż 2,5 mm	Takie przedmioty, jak narzędzia i grube druty, nie spenetrują sprzętu.
4	Przedmiotami większymi niż 1 mm	Takie przedmioty, jak druty i śruby, nie spenetrują sprzętu.

Tabela 2.1. Stopnie IP – pierwsza cyfra IP: ciała stałe (Kontynuacja)

5	Ochrona przed kurzem i pyłem	Brak całkowitej ochrony przed penetracją przez kurz, jednak ilość kurzu wnika do obudowy jest na tyle mała, że nie zakłóca prawidłowego działania sprzętu.
6	Całkowita ochrona przed kurzem	Kurz nie wnika do wnętrza obudowy.

Tabela 2.2 Stopnie IP – druga cyfra po IP: ciecze

Stopień	Ochrona przed	Skuteczność wobec
0	Brak ochrony	Brak szczególnej ochrony
1	Kapiącą wodą	Kapiąca woda (pionowo spadające krople) nie wywołuje szkodliwych skutków.
2	Wodą kapiącą pod kątem do 15°	Pionowo kapiąca woda nie wywołuje szkodliwych skutków, gdy obudowa jest pochylona pod kątem do 15° względem położenia normalnego.
3	Rozpylaną wodą	Woda rozpylana pod kątem do 60° względem pionu nie wywołuje szkodliwych skutków.
4	Bryzgającą wodą	Bryzgi wodne niezależnie od kierunku nie wywołują szkodliwych skutków.
5	Strumieniami wody	Strumień wodny z dyszy skierowany na obudowę z dowolnego kierunku nie wywołuje szkodliwych skutków.
6	Silnymi strumieniami wody	Woda z silnych fal ani woda kierowana pod bardzo wysokim ciśnieniem nie wnika do obudowy w ilościach powodujących szkody.
7	Krótkotrwałym zanurzeniem w wodzie	Woda nie może dostać się do obudowy, jeśli jest ona zanurzona z uwzględnieniem wskazanych warunków czasowych i ciśnieniowych.
8	Ciągłym zanurzeniem w wodzie	Urządzenie można trwale zanurzyć w wodzie z uwzględnieniem warunków wskazanych przez producenta. Warunki te muszą być trudniejsze niż określone dla stopnia IPX7 (patrz wyżej).
9	Wodą z myjek ciśnieniowych, w tym parowych	Woda kierowana na obudowę pod dowolnym kątem i bardzo wysokim ciśnieniem nie wywołuje szkodliwych skutków.

### 2.3.2 Inne istotne normy IEC

- IEC 60068-2: norma badań środowiskowych urządzeń elektronicznych i innych produktów pod względem zdolności do działania w warunkach środowiskowych obejmujących skrajne zimno i suche gorąco. Poniższe procedury określone w tej normie zwykle stosowane są wobec przedmiotów, których temperatura stabilizuje się w trakcie próby.
  - IEC 60068-2-1: zimno
  - IEC 60068-2-2: suche gorąco
  - IEC 60068-2-6: wibracje (ciągłe)

- IEC 60068-2-14: zmiana temperatury
  - IEC 60068-2-27: wstrząs
  - IEC 60068-2-30: wilgotne gorąco (cykliczne)
  - IEC 60068-2-64: wibracje (szerokopasmowe przypadkowe)
  - IEC 60068-2-78: wilgotne gorąco (stan ustalony)
- IEC 60825, klasa I: norma stosowana do zapewnienia bezpieczeństwa użytkowania lasera w module ogniskowania w każdych warunkach zwykłej eksploatacji.

### 2.3.3 Klasyfikacja NEMA

NEMA (National Electrical Manufacturers Association) to mające siedzibę w USA stowarzyszenie opracowujące normy dotyczące obudów sprzętu elektrycznego. Stowarzyszenie NEMA wprowadziło swoją własną normę NEMA 250 na całym świecie. Ponadto przyjęło i opublikowało normę harmonizującą swoje wymagania z klasyfikacją IP, ANSI/IEC 60529, za pośrednictwem American National Standards Institute (ANSI).

Klasyfikacja NEMA 250 dotyczy nie tylko ochrony przed penetracją, ale uwzględnia także dodatkowe czynniki, takie jak odporność na korozję, skuteczność i szczegóły konstrukcyjne. Dlatego typ NEMA można odnieść do stopnia IP, ale stopnia IP nie można odnieść do typu NEMA.

Normy UL 50 i UL 50E są oparte na normie NEMA 250. NEMA dopuszcza samocertyfikację, natomiast UL wymaga uzyskania świadectwa na podstawie prób i kontroli wykonywanych przez niezależny podmiot.

*Tabela 2.3 Klasyfikacja NEMA obudów do miejsc niebędących miejscami niebezpiecznymi*

NEMA	Równoważny stopień IP	Do montażu wewnątrz budynków	Do montażu na zewnątrz	Ochrona przed
Typ 1	IP10	X		Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające zanieczyszczenia stałe). Brak ochrony przed cieczami.
Typ 3	IP54	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i nawiewane zanieczyszczenia stałe). Penetracją przez wodę (deszcz, śnieg z deszczem, śnieg). Zewnętrzne oblodzenie obudowy nie spowoduje uszkodzenia.
Typ 3R	IP14	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające zanieczyszczenia stałe). Penetracją przez wodę (deszcz, śnieg z deszczem, śnieg). Zewnętrzne oblodzenie obudowy nie spowoduje uszkodzenia.
Typ 3S	IP54	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i nawiewane zanieczyszczenia stałe). Penetracją przez wodę (deszcz, śnieg z deszczem, śnieg). Zewnętrzne mechanizmy działają mimo oblodzenia.

Tabela 2.3. Klasyfikacja NEMA obudów do miejsc niebędących miejscami niebezpiecznymi (Kontynuacja)

Typ 4	IP56	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i nawiewane zanieczyszczenia stałe). Penetracją przez wodę (deszcz, deszcz ze śniegiem, śnieg, rozpryski wody i woda kierowana z węża). Zewnętrzne oblodzenie obudowy nie spowoduje uszkodzenia.
NEMA 4X	IP56	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i nawiewane zanieczyszczenia stałe). Penetracją przez wodę (deszcz, deszcz ze śniegiem, śnieg, rozpryski wody i woda kierowana z węża). Zapewnia dodatkowy poziom ochrony przed korozją. Zewnętrzne oblodzenie obudowy nie spowoduje uszkodzenia.
Typ 6	IP67	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające zanieczyszczenia stałe). Penetracją przez wodę (woda kierowana z węża i wniknięcie wody podczas sporadycznych, przejściowych zanurzeń na ograniczoną głębokość). Zewnętrzne oblodzenie obudowy nie spowoduje uszkodzenia.
Typ 6P	IP67	X	X	Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające zanieczyszczenia stałe). Penetracją przez wodę (woda kierowana z węża i wniknięcie wody podczas długotrwałego zanurzenia na ograniczoną głębokość). Zapewnia dodatkowy poziom ochrony przed korozją. Zewnętrzne oblodzenie obudowy nie spowoduje uszkodzenia.
Typ 12	IP52	X		Bez zaślepek do wybicia. Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i krążące: kurz, kłaczki, włókna i cząstki unoszące się). Penetracją przez wodę (kapiącą i słabo rozpryskiwaną).
Typ 12K	IP52	X		Z zaślepkami do wybicia. Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i krążące: kurz, kłaczki, włókna i cząstki unoszące się). Penetracją przez wodę (kapiącą i słabo rozpryskiwaną).
Typ 13	IP54	X		Dostępem do niebezpiecznych części i penetracją przez ciała stałe (opadające i krążące: kurz, kłaczki, włókna i cząstki unoszące się). Penetracją przez wodę (kapiącą i słabo rozpryskiwaną). Natryskiwaniem, rozpryskiwaniem lub sączeniem się olejów i niekorozyjnych chłodziw.

NEMA TS 2 to wytyczna projektowa mająca zastosowanie do urządzeń sygnalizacyjnych do kierowania ruchem.

### 2.3.4 Stopień IK

Stopnie IK zdefiniowano w normie międzynarodowej IEC/EN 62262 jako stopnie ochrony przed zewnętrznymi uderzeniami mechanicznymi. Norma ta została pierwotnie przyjęta w roku 1994 jako norma europejska EN 50102, a w roku 2002 stała się normą międzynarodową.

Wielu producentów decyduje się na badanie najślabszej części produktu, aby mieć pewność co do jego wytrzymałości w całym okresie eksploatacji.



Stopień	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
Energia uderzenia (J)	0.14	0,2	0.35	0.5	0.7	1	2	5	10	20	50*
Masa (kg)	<0,2	<0,2	0,2	0,2	0,2	0.5	0.5	1.7	5	5	
Wysokość upadku (mm)	56	80	140	200	280	400	400	300	200	400	

\*Energia uderzenia do 50 J. Producent musi podać energię, masę elementu uderzającego i wysokość, z jakiej on spada.

## 2.4 Inne próby

### 2.4.1 Ochrona przeciwwybuchowa

- IEC/EN/UL/SANS/CSA 60079-0: wymagania ogólne dotyczące konstrukcji, badań i znakowania urządzeń Ex oraz komponentów Ex przeznaczonych do stosowania w atmosferach wybuchowych.
- IEC/EN/UL/SANS/CSA 60079-1: konkretne wymagania dotyczące konstrukcji i badań urządzeń elektrycznych z obudową ognioszczelną „d”, przewidzianych do eksploatacji w atmosferach gazów wybuchowych.

### 2.4.2 Próby dla zasilaczy midspan

Jeśli do produktu dołączony jest zasilacz midspan, w tej sekcji arkusza danych wymienione są próby dotyczące wyłącznie tego zasilacza. Objaśnienia znajdują się w poprzednich sekcjach niniejszego dokumentu.

### 2.4.3 Bezpieczeństwo w kontroli dostępu

- UL 294: definiuje wymagania dotyczące konstrukcji, skuteczności i działania systemów kontroli dostępu.

## 3 Świadectwa

Gdy kamera jest zainstalowana w środowisku potencjalnie zagrożonym wybuchem, jej obudowa musi spełniać bardzo konkretne wymagania norm bezpieczeństwa. Otoczenie musi być chronione przed potencjalnymi źródłami zapłonu obecnymi w kamerze lub innych urządzeniach.

Produkty europejskie muszą spełniać wymagania określone w dyrektywie ATEX, a odpowiadająca im norma międzynarodowa to IECEx. W Ameryce Północnej system stref opisany w ATEX i IECEx jest mniej powszechny, natomiast używa się przede wszystkim klas/grup NFPA70 (Krajowy Kodeks Elektryczny USA (NEC, National Electric Code)) i CSA C22.1 (Kanadyjski Kodeks Elektryczny (CEC, Canadian Electric Code)).

Tabela 3.1 Klasy ochrony przeciwwybuchowej

Klasa / Grupa	Atmosfera	Definicja	Strefa (IECEX i ATEX)
Klasa I / Grupa 1	Gaz	Obszar, w którym mieszanina wybuchowa jest obecna stale lub przez długie okresy.	Strefa 0
Klasa I / Grupa 1	Gaz	Obszar, w którym prawdopodobna jest obecność mieszaniny wybuchowej podczas normalnej pracy.	Strefa 1
Klasa I / Grupa 2	Gaz	Obszar, w którym obecność mieszaniny wybuchowej podczas normalnej pracy jest mało prawdopodobna, a jeśli taka mieszanina jest obecna, to tylko przez krótki czas.	Strefa 2
Klasa II / Grupa 1	Pył	Obszar, w którym mieszanina wybuchowa jest obecna stale lub przez długie okresy.	Strefa 20
Klasa II / Grupa 1	Pył	Obszar, w którym prawdopodobna jest obecność mieszaniny wybuchowej podczas normalnej pracy.	Strefa 21
Klasa II / Grupa 2	Pył	Obszar, w którym obecność mieszaniny wybuchowej podczas normalnej pracy jest mało prawdopodobna, a jeśli taka mieszanina jest obecna, to tylko przez krótki czas.	Strefa 22

## 4 Zasilanie

### 4.1 Klasy Power over Ethernet (PoE)

Klasy PoE określają warunki sprawnego rozdziału zasilania poprzez wskazanie mocy wymaganej przez urządzenie zasilane (PD).

Tabela 4.1 Klasy PoE

Klasa	Typ	Gwarantowana moc w urządzeniu działającym jako źródło zasilania (PSE)	Maksymalna moc wykorzystywana przez urządzenie zasilane (PD)
0	Typ 1, 802.3af	15.4 W	0,44 W–12,95 W
1	Typ 1, 802.3af	40.0 W	0,44 W–3,84 W
2	Typ 1, 802.3af	7.0 W	3,84 W–6,49 W
3	Typ 1, 802.3af	15.4 W	6,49 W–12,95 W
4	Typ 2, 802.3at*	30 W	12,95 W–25,5 W
6	Typ 3, 802.3bt	60 W	51 W
8	Typ 3, 802.3bt	100 W	71.3 W

\*Ten typ jest także określany mianem PoE+.

# 5 Sieć

## 5.1 Ochrona i sterowanie zabezpieczeniami

Istnieje kilka metod ochrony zasobów systemowych przed zagrożeniami. Niektóre zagrożenia stwarzają ryzyko dla urządzeń, natomiast inne stwarzają ryzyko dla sieci lub przesyłanych/przechowywanych danych. Aby chronić urządzenia i sieci, można stosować kilka mechanizmów zabezpieczających:

- Poświadczenia (nazwa użytkownika / hasło) uniemożliwiają osobom nieupoważnionym dostęp do materiału wideo i konfiguracji urządzeń. Przyznając kontom różne poziomy uprawnień, można selektywnie przyznawać różnym użytkownikom dostęp do różnych zasobów.
- Filtrowanie adresów IP (zapora) zmniejsza ekspozycję urządzenia w sieci i chroni je przed dostępem nieupoważnionych klientów. Ogranicza w ten sposób ewentualne skutki ujawnienia hasła i pojawienia się nowej krytycznej luki w zabezpieczeniach.
- IEEE 802.1x: chroni sieć przed nieautoryzowanymi klientami. 802.1x to standard ochrony infrastruktury sieciowej przy wykorzystaniu zarządzanych przełączników i serwera RADIUS. Klient 802.1x w urządzeniu realizuje usługę uwierzytelniania na rzecz urządzenia w sieci.
- HTTPS (Hypertext transfer protocol secure): chroni dane (wideo) przed podsłuchem w sieci. Dzięki podpisanym certyfikatom używanym w ramach protokołu HTTPS klient wideo może upewnić się, że uzyskuje dostęp do zaufanej kamery, a nie do komputera, który podszywa się pod kamerę.
- Podpisane oprogramowanie sprzętowe jest wdrażane przez dostawcę oprogramowania poprzez podpisanie obrazu oprogramowania sprzętowego za pomocą klucza prywatnego, który nie jest ujawniany. Urządzenie będzie sprawdzać podpis oprogramowania sprzętowego przed jego zaakceptowaniem i zainstalowaniem. Jeśli urządzenie wykryje, że integralność oprogramowania sprzętowego została naruszona, nie pozwoli na jego uaktualnienie. Podpisy oprogramowania sprzętowego stosowane przez firmę Axis są oparte na powszechnie przyjętej w branży metodzie szyfrowania RSA.
- Bezpieczny start to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki wykorzystaniu podpisanego oprogramowania sprzętowego bezpieczny start gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem sprzętowym. Bezpieczny start gwarantuje, że urządzenie Axis jest całkowicie wolne od szkodliwego oprogramowania po przywróceniu ustawień fabrycznych.
- TPM, czyli Trusted Platform Module, to składnik udostępniający zestaw funkcji kryptograficznych umożliwiający ochronę informacji przed dostępem osób nieupoważnionych. Klucz prywatny jest przechowywany w module TPM i nigdy go nie opuszcza. Wszystkie operacje kryptograficzne wymagające użycia klucza prywatnego są kierowane do modułu TPM i wykonywane wewnątrz niego. Dzięki temu tajna część certyfikatu pozostaje bezpieczna nawet w przypadku naruszenia zabezpieczeń.
- Axis Edge Vault to bezpieczny kryptograficzny moduł obliczeniowy (bezpieczny moduł lub bezpieczny element), w którym identyfikator urządzenia Axis jest bezpiecznie i na stałe zainstalowany i przechowywany.

Więcej materiałów na temat cyberbezpieczeństwa można znaleźć na stronie [axis.com/cybersecurity](https://axis.com/cybersecurity)

## 5.2 Obsługiwane protokoły

W procesie bezpiecznego przesyłania danych między urządzeniami sieciowymi wykorzystuje się wiele różnych protokołów.

### 5.2.1 Modele referencyjne protokołów

Interakcje między poszczególnymi protokołami najłatwiej będzie zrozumieć, analizując model komunikacji Open Systems Interconnection (OSI). Stosowany jest także model referencyjny TCP/IP.

#### 5.2.1.1 Model referencyjny OSI

Model komunikacji między systemami otwartymi. Aby świadczyć jakąś usługę, każda warstwa korzysta z usług warstwy bezpośrednio niższej. Każda warstwa musi świadczyć usługi zgodnie z określonymi regułami (protokołami).

##### Warstwa 7 – Aplikacji

Udostępnia aplikacjom takie funkcje, jak przesyłanie danych WWW, plików i wiadomości e-mail.

Właściwe aplikacje, takie jak przeglądarki WWW lub programy pocztowe, funkcjonują ponad tą warstwą i model OSI ich nie obejmuje.

##### Warstwa 6 – Prezentacji (danych)

Sprawia, że dane wysłane przez warstwę aplikacji jednego systemu są czytelne dla warstwy aplikacji innego systemu. Przekształca formaty danych zależne od systemu, takie jak ASCII, w format niezależny, umożliwiając w ten sposób prawidłową pod względem składniowym wymianę danych między systemami.

##### Warstwa 5 – Sesji (trwałe połączenie między równorzędnymi hostami)

Realizuje usługę zorientowaną na aplikację i obsługuje proces komunikacji między dwoma systemami. Komunikacja rozpoczyna się od nawiązania sesji, która jest podstawą wirtualnego połączenia między dwoma systemami.

##### Warstwa 4 – Transportu (transport między punktami końcowymi, protokół połączeniowy)

Realizuje usługę niezawodnego przesyłania danych (poprzez zastosowanie sterowania przepływem i kontroli błędów) dla Warstwy 5 i wyższych.

##### Warstwa 3 – Sieciowa (pakiety (adresowanie / podział na fragmenty))

Realizuje właściwe przesyłanie danych, kierując i przekazując pakiety danych między systemami. Tworzy tabele routingu i administruje nimi oraz udostępnia możliwości komunikacji przekraczającej granice sieci. Do danych w tej warstwie są przypisywane adresy docelowe i źródłowe, stanowiące podstawę ukierunkowanego routingu.

##### Warstwa 2 – Łącza danych (ramki)

Zapewnia dostęp do medium transmisyjnego na potrzeby transmisji danych i sterowania, łącząc dane w jednostki nazywane ramkami. Warstwa 2 jest podzielona na dwie podwarstwy: wyższą odpowiedzialną za sterowanie łączem logicznym (LLC, Logical Link Control) i niższą odpowiedzialną za sterowanie dostępem do medium (MAC, Media Access Control). Podwarstwa LLC upraszcza wymianę danych, a podwarstwa MAC steruje dostępem do medium transmisyjnego.

##### Warstwa 1 – Fizyczna (bity)

Realizuje usługi umożliwiające przesyłanie danych w postaci strumienia bitów przez medium, takie jak przewodowe lub bezprzewodowe łącze transmisyjne.

### 5.2.1.2 Model referencyjny protokołów Transmission Control Protocol / Internet Protocol

Model referencyjny protokołów TCP/IP to kolejny model opisujący wzajemne relacje między protokołami i przebieg komunikacji. W modelu referencyjnym TCP/IP wyróżnia się cztery warstwy, które w poniższej tabeli odniesiono do modelu OSI.

Tabela 5.1 Porównanie modeli referencyjnych

Model OSI	Model TCP/IP
Warstwa 7 – Aplikacji	Warstwa 4 – Aplikacji
Warstwa 6 – Prezentacji	
Warstwa 5 – Sesji	
Warstwa 4 – Transportu	Warstwa 3 – Transportu
Warstwa 3 – Sieci	Warstwa 2 – Internetu
Warstwa 2 – Łącza danych	Warstwa 1 – Interfejsu sieciowego
Warstwa 1 – Fizyczna	

### 5.2.2 Protokoły warstwy aplikacji

- **CIFS/SMB** (Common Internet File System / Server Message Block): używany głównie do udostępniania plików, drukarek i portów szeregowych oraz realizacji różnych funkcji komunikacyjnych między węzłami w sieci.
- **DDNS** (Dynamic Domain Name System): służy do utrzymywania skojarzenia jednej nazwy domeny ze zmieniającymi się adresami IPv4.
- **DHCPv4/v6** (Dynamic Host Configuration Protocol): służy do automatycznego przypisywania adresów IP i zarządzania nimi.
- **DNS/DNSv6** (Domain Name System): przekształca nazwy domen w skojarzone z nimi adresy IP.
- **FTP** (File Transfer Protocol): używany głównie do przesyłania plików z serwera do klienta (pobieranie) lub z klienta do serwera (przekazywanie). Umożliwia także tworzenie i wybieranie katalogów oraz zmianę nazwy lub usuwanie katalogów i plików.
- **HTTP** (Hypertext Transfer Protocol): używany głównie do ładowania tekstów i obrazów z serwisu WWW do przeglądarki WWW. Sieciowe systemy wizyjne udostępniają serwery HTTP, które umożliwiają dostęp do systemów przez przeglądarki WWW i pobieranie w ten sposób konfiguracji lub odbieranie obrazów na żywo.
- **HTTP/2**: istotna modyfikacja protokołu HTTP zdefiniowana w dokumencie RFC 7540 i wydana w lutym 2015 r.
- **HTTPS** (HTTP Secure): adaptacja protokołu Hypertext Transfer Protocol (HTTP) do wymogów bezpiecznej komunikacji w sieciach komputerowych; szeroko stosowana w Internecie. W ramach protokołu HTTPS komunikacja HTTP jest szyfrowana przy użyciu protokołu Transport Layer Security (TLS).
- **MQTT** (Message Queuing Telemetry Transport): standardowy protokół przesyłania komunikatów w internecie rzeczy (IoT). Został zaprojektowany z myślą o uproszczeniu integracji IoT i jest

wykorzystywany w wielu branżach do podłączania urządzeń zdalnych przy jednoczesnej minimalizacji objętości kodu i obciążenia sieci.

- **NTP (Network Time Protocol):** służy do synchronizowania czasu na komputerze klienckim lub serwerze z czasem na innym serwerze.
- **RTP (Real-Time Transport Protocol):** umożliwia przesyłanie danych w czasie rzeczywistym między systemami w punktach końcowych.
- **RTCP (Real-Time Control Protocol):** przesyła w osobnym kanale informacje statystyczne i sterujące dla sesji RTP. Współdziała z protokołem RTP przy dostarczaniu i opakowywaniu danych multimedialnych, ale sam nie transportuje żadnych danych multimedialnych.
- **RTSP (Real-Time Streaming Protocol):** służy do zaawansowanego sterowania transmisją multimediiów w czasie rzeczywistym.
- **SFTP (Secure File Transfer Protocol):** zapewnia dostęp do plików, przesyłanie plików i zarządzanie plikami przez dowolny niezawodny strumień danych.
- **SIP (Session Initiation Protocol):** protokół komunikacyjny do sygnalizacji i sterowania w ramach sesji przesyłania multimediiów.
- **SIPS (Session Initiation Protocol Secure):** szyfrowana wersja protokołu SIP.
- **SMTP (Simple Mail Transfer Protocol):** standard przesyłania poczty elektronicznej (e-mail) w Internecie. Kamery sieciowe obsługują SMTP, aby móc wysyłać alerty jako wiadomości e-mail.
- **SNMPv1/v2/v3 (Simple Network Management Protocol):** służy do zdalnego monitorowania urządzeń sieciowych i zarządzania urządzeniami sieciowymi, takimi jak przełączniki, routery i kamery sieciowe. Dzięki zgodności z protokołem SNMP możliwe jest zarządzanie kamerami sieciowymi za pomocą narzędzi open source.
- **SOCKS:** umożliwia przesyłanie pakietów sieciowych między klientami i serwerami przez zdalne proxy sieciowe.
- **SRTP (Secure Real-Time Transport Protocol):** umożliwia przesyłanie w czasie rzeczywistym zaszyfrowanych danych między systemami w punktach końcowych, stanowi zatem zabezpieczony wariant protokołu RTP.
- **SSH (Secure Shell):** umożliwia bezpieczny dostęp do funkcji zarządzania i debugowania urządzeń sieciowych za pośrednictwem niezabezpieczonej sieci.
- **TLSv1.2/v1.3 (Transport Layer Security):** negocjuje prywatne, niezawodne połączenie między klientem a serwerem.

### 5.2.3 Protokoły warstwy transportu

- **TCP (Transmission Control Protocol):** połączeniowe, niezawodne dostarczanie strumieni danych z zachowaniem kolejności. Najczęściej spotykany protokół transportu danych.
- **UDP (User Datagram Protocol):** bezpołączeniowa usługa transmisji, przedkłada szybkość nad niezawodność dostarczania danych.
- **ICMP (Internet Control Message Protocol):** przesyła komunikaty o błędach i informacje operacyjne wskazujące na niedostępność żądanej usługi lub nieosiągalność hosta bądź routera.

#### 5.2.4 Protokoły warstwy sieciowej

- **IGMPv1/v2/v3** (Internet Group Management Protocol): używany przez hosty i sąsiadujące z nimi routery w sieciach IPv4 do ustanawiania członkostwa w grupach multiemisji. Pozwala na bardziej efektywne wykorzystanie zasobów w tego rodzaju aplikacjach.
- **IPv4/IPv6** (Internet Protocol): indywidualny adres publiczny potrzebny urządzeniom internetowym do komunikowania się. IPv4 jest pierwotną wersją protokołu z adresami 32-bitowymi. IPv6 jest najnowszą wersją z adresami 128-bitowymi, które są podzielone na osiem grup po cztery cyfry szesnastkowe.
- **USGv6**: profil standardów technicznych protokołu IPv6 zdefiniowany przez rząd USA w celu zapewnienia kompatybilności nabywanych urządzeń sieciowych korzystających z tego protokołu.

#### 5.2.5 Protokoły warstwy łącza danych

- **ARP** (Address Resolution Protocol): służy do wykrywania adresu MAC hosta docelowego.
- **CDP** (Cisco Discovery Protocol): protokół zastrzeżony firmy Cisco, używany jako alternatywa dla LLDP do pozyskiwania informacji o podłączonych urządzeniach sprzętowych.
- **IEEE 802.3 (i, u, ab)**: standardy sieci Ethernet definiujące zasady przesyłania danych z przepływnością 10 Mb/s (10Base-T), 100 Mb/s (100Base-TX) i 1 Gb/s (1000Base-T) przez okablowanie w postaci skrętki.
- **LLDP** (Link Layer Discovery Protocol): służy do ogłaszania tożsamości i możliwości urządzenia oraz innych urządzeń podłączonych do tej samej sieci.

#### 5.2.6 Protokoły wykrywania

- **mDNS (Bonjour)**: może być stosowany do wykrywania produktów z zakresu sieciowych systemów wizyjnych przy użyciu komputerów Mac lub jako protokół wykrywania nowych urządzeń w dowolnej sieci.
- **UPnP** (Universal Plug and Play): systemy operacyjne firmy Microsoft mogą automatycznie wykrywać zasoby (urządzenia Axis) w sieci.
- **Zeroconf**: automatycznie przydziela urządzeniu sieciowemu nieużywany adres IP z przedziału od 169.254.1.0 do 169.254.254.255.

#### 5.2.7 Jakość serwisu (QoS)

W sieci IP konieczne jest sterowanie udostępnianiem zasobów sieciowych w celu spełnienia wymagań poszczególnych usług.

- **QoS** (Quality of Service): jakość usług, zdolność do obsługi ruchu sieciowego o różnych priorytetach, tak by newralgiczne przepływy były realizowane przed przepływami o niższym priorytecie. Podnosi niezawodność sieci, sterując wielkością pasma, jaką aplikacja może wykorzystać, i ograniczając konkurencję o pasmo między aplikacjami.
- **DiffServ**: sieć próbuje realizować określoną usługę na podstawie jakości QoS określonej w każdym pakiecie.

#### 5.2.8 Metody transmisji danych

Wyróżnia się trzy różne sposoby transmisji danych w sieciach komputerowych.

- **Emisja pojedyncza:** najczęściej spotykany sposób, w którym nadawca i odbiorca komunikują się ze sobą na zasadzie punkt-punkt. Pakiety danych są wysyłane tylko do jednego odbiorcy; żadne inne klienty ich nie otrzymają.
- **Multiemisja:** komunikacja między jednym nadawcą a wieloma odbiorcami w sieci. Ta metoda zmniejsza natężenie ruchu w sieci, ponieważ jeden strumień informacji trafia do wielu odbiorców.
- **Rozgłaszanie:** nadawca wysyła tę samą informację do wszystkich innych serwerów w sieci, a wszystkie hosty w sieci odbierają komunikat i w jakimś stopniu go przetwarzają.





## O firmie Axis Communications

Firma Axis wspiera rozwój inteligentnego oraz bezpiecznego świata poprzez tworzenie rozwiązań sieciowych, które dostarczają wiedzę umożliwiającą poprawę bezpieczeństwa i wdrażanie nowych sposobów prowadzenia działalności. Jako lider rynku sieciowych systemów wizyjnych Axis oferuje produkty i usługi z zakresu dozoru wizyjnego i analiz wideo, kontroli dostępu, systemów domofonowych oraz systemów audio. Axis zatrudnia ponad 3800 wysoce zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma Axis została założona w 1984 roku i ma siedzibę w Lund w Szwecji.

Więcej informacji o firmie Axis można znaleźć na stronie internetowej firmy pod adresem [axis.com](https://axis.com).