DOCUMENTO TECNICO

Guida rapida alle schede tecniche Axis

Approvazioni, certificazioni e protocolli

Novembre 2021

Sommario

1 Introduzione

Axis Communications rispetta le normative di settore e di conformità per tutti i prodotti che immette sul mercato. Il presente documento integra le schede dati Axis con brevi definizioni e descrizioni delle sigle, delle approvazioni, delle certificazioni e dei protocolli riportati.

Il documento fornisce informazioni sulle sezioni delle schede tecniche evidenziate e ingrandite di seguito.

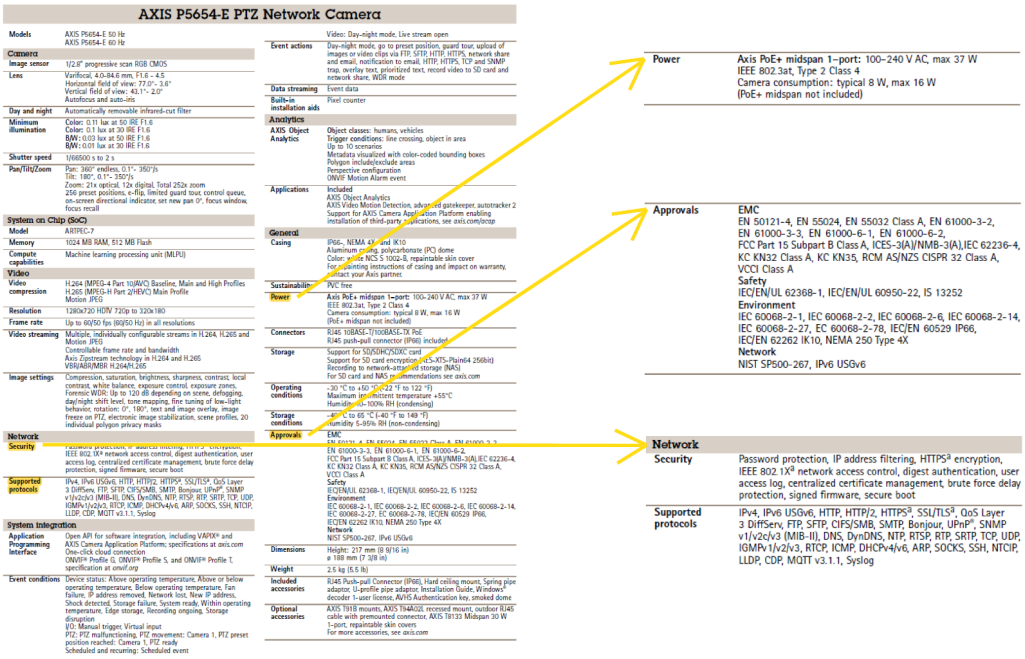

Figure 1. In evidenza: sezioni delle schede tecniche Axis descritte nel presente documento.

2 Approvazioni

La sezione Approvazioni delle schede tecniche Axis si riferisce alla conformità a varie norme. In genere, questa sezione è suddivisa in sottosezioni come EMC, Sicurezza, Ambiente, rete e Altro. Quest'ultima può riferirsi alla protezione contro le esplosioni o alla sicurezza nel controllo accessi. Inoltre, può contenere una sottosezione per le approvazioni che riguardano il midspan, qualora sia venduto insieme al prodotto.

2.1 EMC (compatibilità elettromagnetica)

Tutti i produttori devono dichiarare la compatibilità elettromagnetica dei loro prodotti video di rete. In alcune circostanze, i produttori possono autocertificarsi, ma la maggior parte si affida a laboratori accreditati che forniscono un referto di conformità. Le approvazioni EMC sono divise in due parti: emissioni e immunità.

Emissioni indica la capacità delle apparecchiature di funzionare in modo soddisfacente senza emettere troppa energia elettromagnetica, che può disturbare altri apparecchi nello stesso ambiente.

Immunità misura la capacità dei prodotti elettronici di tollerare l'influsso dei fenomeni elettromagnetici e dell'energia elettrica irradiata o condotta da altri prodotti elettronici. In Europa, la certificazione EMC è inclusa nel marchio CE, che a sua volta è incluso nella legislazione sull'armonizzazione dell'Unione europea.

Le norme elencate di seguito definiscono i limiti e i metodi di verifica delle emissioni elettromagnetiche e delle prove di immunità. Poiché non esiste un test di conformità a livello internazionale, possono esserci codici diversi per aree geografiche o applicazioni diverse.

2.1.1 Norme ITE (Information Technology Equipment)

Queste norme valgono per le apparecchiature multimediali (MME) alimentate con una tensione CA o CC non superiore a 600 V. Le apparecchiature multimediali (MME) sono definite apparecchiature informatiche (ITE), apparecchiature audio, apparecchiature video, apparecchiature di ricezione televisiva e apparecchiature di controllo dell'illuminazione per intrattenimento.

- EN 55032 Classe A: norma sulle emissioni (a livello commerciale, industriale e aziendale) armonizzata con le norme internazionali
- EN 55032 Classe B: norma sulle emissioni (a livello residenziale) armonizzata con le norme internazionali
- EN 55035: norma sull'immunità, armonizzata con le norme internazionali

2.1.2 Norme armonizzate per nazione/territorio

- EN 61000-6-1 e EN 61000-6-2: norme generiche di conformità (Europa)
- FCC Part 15 Subpart B, Classe A e B: regole e norme stipulate dalla FCC (Federal Communications Commission) per i dispositivi di telecomunicazione, riferite alle emissioni ma non all'immunità (Stati Uniti)
- ICES-3(A e B)/NMB-3(A e B) (Canada)
- VCCI Classe A e B (Giappone)
- KS C 9832 Classe A e B, KS C 9835, KS C 9547, KS C 9815 (Corea)
- RCM AS/NZS CISPR 32 Classe A e B (Australia/Nuova Zelanda)

2.1.3 Norme supplementari per applicazione/prodotto

- EN 50121-4, IEC 62236-4: illustra i criteri prestazionali degli apparati di segnalazione e telecomunicazione che possono interferire con altri apparati in ambiente ferroviario
- EN 50130-4: riguarda i componenti dei sistemi di allarme, tra cui: sistemi di controllo accessi, sistemi TVCC, sistemi di rilevamento e allarme antincendio, sistemi di allarme antiaggressione, sistemi di allarme antintrusione, sistemi di allarme sociale

2.2 Sicurezza

- Direttiva Bassa Tensione (2014/35/UE): indica gli obiettivi generici per la sicurezza delle apparecchiature elettriche. Garantisce l'uso sicuro dei prodotti senza il rischio di infortuni o danni materiali.
- IEC/EN/UL 62368-1: conformità di telecamere di rete, codificatori e alimentatori ai requisiti previsti per ridurre il rischio di incendi, scosse elettriche o infortuni a tutte le persone che possano entrare a contatto con le apparecchiature.

- IEC/EN/UL 60950-22: requisiti specifici di sicurezza per prodotti e involucri da utilizzare in ambienti esterni
- IEC/EN 62471-1: sicurezza fotobiologica delle lampade e requisiti per i sistemi di lampade riguardanti i limiti di esposizione, in modo da prevenire pericoli per gli occhi e la pelle
- EN/UL/CSA 60065: riguarda gli apparati elettronici alimentati dalla rete elettrica, da un alimentatore, da batterie o da un'alimentazione remota e destinati alla ricezione, generazione, registrazione o riproduzione di audio, video e segnali correlati
- IS 13252 (specifica per l'India): conformità di telecamere di rete, codificatori e alimentatori ai requisiti previsti per ridurre il rischio di incendi, scosse elettriche o infortuni a tutte le persone che possano entrare a contatto con le apparecchiature.

2.3 Ambiente

2.3.1 Classificazione IP

La norma IEC 60529 (International Electrotechnical Commission) definisce le classi IP (Ingress Protection o International Protection) con un codice di due cifre. Il codice definisce il livello di protezione delle apparecchiature elettriche contro l'ingresso di corpi solidi o polvere, il contatto accidentale e l'acqua.

Tabella 2.1 Classificazioni IP - prima cifra dopo IP: corpi estranei solidi

Livello	Protetto da	Efficace contro
0	Non protetto	Nessuna protezione.
1	Corpi più grandi di 50 mm	Grandi superfici del corpo, come il dorso della mano, ma senza alcuna protezione contro il contatto intenzionale con una parte del corpo.
2	Corpi più grandi di 12,5 mm	Dita o altri corpi in grado di penetrare fino a 80 mm lontano da parti pericolose. Corpi con un diametro di 12,5 mm non sono in grado di penetrare totalmente.
3	Corpi più grandi di 2,5 mm	Corpi come attrezzi e fili spessi non possono penetrare assolutamente.
4	Corpi più grandi di 1 mm	Corpi come fili e viti non possono penetrare assolutamente.
5	Protetto dalla polvere	L'ingresso della polvere non è totalmente escluso, ma la quantità di polvere che può penetrare all'interno del dispositivo non ne pregiudica il funzionamento.
6	A prova di polvere	Nessun ingresso di polvere.

Tabella 2.2 Classificazioni IP - seconda cifra dopo IP: liquidi

Livello	Protetto da	Efficace contro
0	Non protetto	Nessuna protezione specifica.
1	Gocciolamenti d'acqua	I gocciolamenti d'acqua (gocce a caduta verticale) non hanno effetti dannosi.

Tabella 2.2. Classificazioni IP - seconda cifra dopo IP: liquidi (Continuo)

2	Gocciolamenti d'acqua fino ad inclinazioni di 15°	La caduta verticale di gocce d'acqua non ha effetti dannosi se l'involucro viene inclinato ad un'angolazione massima di 15° rispetto alla sua posizione normale.
3	Acqua vaporizzata	L'acqua vaporizzata ad angolazioni massime di 60° rispetto alla posizione verticale non ha effetti dannosi.
4	Schizzi d'acqua	Gli schizzi d'acqua contro l'involucro da qualsiasi direzione non hanno effetti dannosi.
5	Getti d'acqua	L'acqua spruzzata da un ugello contro l'involucro da qualsiasi direzione non ha effetti dannosi.
6	Ondate e getti d'acqua potenti	I getti potenti d'acqua, anche causati dal mare mosso, non possono penetrare nell'involucro in quantità dannose.
7	Immersione breve in acqua	L'acqua non è in grado di penetrare in quantità dannose con l'involucro immerso in condizioni prestabilite di pressione e tempo.
8	Immersione continua in acqua	Il dispositivo è idoneo all'immersione continua in acqua alle condizioni specificate dal produttore. Le condizioni devono essere più gravose rispetto alla classe IPX7 (vedere codice precedente).
9	Acqua espulsa da apparecchi di pulizia ad alta pressione o a getto di vapore	L'acqua diretta verso l'involucro da qualsiasi angolazione e a una pressione molto elevata non ha effetti dannosi.

2.3.2 Altre norme IEC pertinenti

- IEC 60068-2: norma per la verifica delle apparecchiature e dei prodotti elettronici che valuta le prestazioni in varie condizioni ambientali, tra cui freddo estremo e caldo secco. In genere, le procedure della norma descritte di seguito presuppongono una certa stabilità degli oggetti alla temperatura durante le prove.
  - IEC 60068-2-1: freddo
  - IEC 60068-2-2: caldo secco
  - IEC 60068-2-6: vibrazioni (continue)
  - IEC 60068-2-14: variazioni di temperatura
  - IEC 60068-2-27: urti
  - IEC 60068-2-30: caldo umido (ciclico)
  - IEC 60068-2-64: vibrazione (aleatorie a larga banda)
  - IEC 60068-2-78: caldo umido (regime stazionario)
- IEC 60825 Classe I: norma che verifica che il tipo di laser utilizzato nel modulo di messa a fuoco laser sia sicuro in tutte le condizioni di normale utilizzo.

2.3.3 Classificazione NEMA

NEMA (National Electrical Manufacturers Association) è un'associazione con sede negli Stati Uniti che emette norme per gli involucri delle apparecchiature elettriche. NEMA ha diffuso la norma NEMA 250 in tutto il mondo. Inoltre, ha adottato e pubblicato una norma di armonizzazione IP, ANSI/IEC 60529, tramite l'American National Standards Institute (ANSI).

La norma NEMA 250 classifica la protezione contro l'ingresso di corpi estranei e liquidi, ma anche altri fattori come la resistenza alla corrosione, le prestazioni e i dettagli costruttivi. Per questo, NEMA è comparabile a IP, ma IP non è comparabile a NEMA.

Le norme UL 50 e UL 50E si basano sulle norme NEMA 250. NEMA consente l'autocertificazione, mentre UL obbliga alla conformità richiedendo che i prodotti superino verifiche e ispezioni condotte da terze parti.

Tabella 2.3 Classificazione NEMA per involucri in luoghi non pericolosi

NEMA	Classe IP equiv-alente	Per interni	Per esterni	Protetto da
Tipo 1	IP10	X		Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia). Nessuna protezione contro i liquidi.
Tipo 3	IP54	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere trasportata dal vento). Ingresso d'acqua (pioggia, nevischio, neve). Nessun danno causato dalla formazione esterna di ghiaccio sull'involucro.
Tipo 3R	IP14	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia). Ingresso d'acqua (pioggia, nevischio, neve). Nessun danno causato dalla formazione esterna di ghiaccio sull'involucro.
Tipo 3S	IP54	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere trasportata dal vento). Ingresso d'acqua (pioggia, nevischio, neve). I meccanismi esterni rimangono operativi anche se cosparsi di ghiaccio.
Tipo 4	IP56	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere trasportata dal vento). Ingresso d'acqua (pioggia, nevischio, neve, schizzi d'acqua e getti d'acqua con lancia). Nessun danno causato dalla formazione esterna di ghiaccio sull'involucro.
NEMA 4X	IP56	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere trasportata dal vento). Ingresso d'acqua (pioggia, nevischio, neve, schizzi d'acqua e getti d'acqua con lancia). Offre una protezione supplementare contro la corrosione. Nessun danno causato dalla formazione esterna di ghiaccio sull'involucro.
Tipo 6	IP67	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia). Ingresso d'acqua (getti d'acqua con lancia e ingresso d'acqua durante l'immersione occasionale e temporanea a profondità limitata). Nessun danno causato dalla formazione esterna di ghiaccio sull'involucro.

Tabella 2.3. Classificazione NEMA per involucri in luoghi non pericolosi (Continuo)

Tipo 6P	IP67	X	X	Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia). Ingresso d'acqua (getti d'acqua con lancia e ingresso d'acqua durante l'immersione prolungata a profondità limitata). Offre una protezione supplementare contro la corrosione. Nessun danno causato dalla formazione esterna di ghiaccio sull'involucro.
Tipo 12	IP52	X		Senza punti di uscita. Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere, lanugine, fibre e particelle volatili). Ingresso d'acqua (gocciolamenti e schizzi leggeri).
Tipo 12K	IP52	X		Con punti di uscita. Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere, lanugine, fibre e particelle volatili). Ingresso d'acqua (gocciolamenti e schizzi leggeri).
Tipo 13	IP54	X		Accesso a parti pericolose e ingresso di corpi estranei solidi (cadute di sporcizia e polvere, lanugine, fibre e particelle volatili). Ingresso d'acqua (gocciolamenti e schizzi leggeri). Spruzzi, schizzi e infiltrazioni di olio e refrigeranti non corrosivi.

NEMA TS 2 è una guida alla progettazione per apparecchiature di segnalazione del traffico.

2.3.4 Classificazione IK

Le classificazioni IK si trovano nella norma internazionale IEC/EN 62262, che specifica il grado di protezione dagli urti meccanici esterni. Originariamente approvata nel 1994 come norma europea EN 50102, è stata adottata a livello internazionale nel 2002.

Molti produttori scelgono di verificare la parte più debole di un prodotto per garantirne la resistenza durante tutto il suo ciclo di vita.

Livello	**IK01**	**IK02**	**IK03**	**IK04**	**IK05**	**IK06**	**IK07**	**IK08**	**IK09**	**IK10**	**IK10+***
Energia d'urto (Joule)	0,14	0,2	0,35	0,5	0,7	1	2	5	10	20	50*
Massa (kg)	<0,2	<0,2	0,2	0,2	0,2	0,5	0,5	1,7	5	5	
Altezza di caduta (mm)	56	80	140	200	280	400	400	300	200	400	

*Urto fino a 50 J. Il produttore deve indicare l'energia, la massa e l'altezza di caduta dell'elemento battente.

2.4 Altre approvazioni

2.4.1 Protezione contro le esplosioni

- IEC/EN/UL/SANS/CSA 60079-0: requisiti generali per la costruzione, la verifica e la marcatura di apparecchiature Ex e componenti Ex destinati all'uso in atmosfere esplosive.
- IEC/EN/UL/SANS/CSA 60079-1: requisiti specifici per la costruzione e la verifica di apparecchi elettrici con involucro ininfiammabile di tipo "d" destinati all'uso in atmosfere gassose esplosive.

2.4.2 Approvazioni per i midspan

Se con il prodotto è incluso un midspan, la scheda tecnica contiene una sezione con le approvazioni specifiche per il midspan. Per le spiegazioni, leggere i precedenti capitoli del presente documento.

2.4.3 Sicurezza nel controllo accessi

- UL 294: definisce i requisiti relativi alla struttura, alle prestazioni e al funzionamento dei sistemi di controllo accessi.

3 Certificazioni

Se una telecamera è installata in un ambiente potenzialmente esplosivo, la custodia deve rispettare norme di sicurezza molto specifiche. Deve proteggere l'ambiente da potenziali mezzi di accensione presenti sulla telecamera o su altri apparecchi.

I prodotti europei devono essere conformi alla direttiva ATEX, la cui normativa internazionale corrispondente è IECEx. Nel Nord America si utilizzano principalmente le categorie Classe/Divisione NFPA70 (National Electric Code, NEC) e CSA C22.1 (Canadian Electric Code, CEC) rispetto al sistema a Zone descritto in ATEX e IECEx.

Tabella 3.1 Classi di protezione contro le esplosioni

Classe / Divisione	Atmosfera	Definizione	Zone (IECEx e ATEX)
Classe I / Divisione 1	Gas	Area in cui la miscela esplosiva è presente in modo continuativo o per lunghi periodi.	Zona 0
Classe I / Divisione 1	Gas	Area in cui è probabile la formazione di una miscela esplosiva in condizioni di funzionamento normali.	Zona 1
Classe I / Divisione 2	Gas	Area in cui la formazione di una miscela esplosiva non è probabile in condizioni di funzionamento normali e, se presente, permane solo per breve tempo.	Zona 2
Classe II / Divisione 1	Polvere	Area in cui la miscela esplosiva è presente in modo continuativo o per lunghi periodi.	Zona 20
Classe II / Divisione 1	Polvere	Area in cui è probabile la formazione di una miscela esplosiva in condizioni di funzionamento normali.	Zona 21
Classe II / Divisione 2	Polvere	Area in cui la formazione di una miscela esplosiva non è probabile in condizioni di funzionamento normali e, se presente, permane solo per breve tempo.	Zona 22

4 Alimentazione

4.1 Classi Power over Ethernet (PoE)

Le classi PoE garantiscono una distribuzione efficiente della potenza specificandone la quantità richiesta da un dispositivo alimentato (PD).

Tabella 4.1 Classi PoE

Classe	Tipo	Potenza garantita dall'apparecchio di alimentazione (PSE)	Potenza massima utilizzata dal dispositivo alimentato (PD)
0	Tipo 1, 802.3af	15,4 W	0,44 W - 12,95 W
1	Tipo 1, 802.3af	40,0 W	0,44 W - 3,84 W
2	Tipo 1, 802.3af	7,0 W	3,84 W - 6,49 W
3	Tipo 1, 802.3af	15,4 W	6,49 W - 12,95 W
4	Tipo 2, 802.3at*	30 W	12,95 W - 25,5 W
6	Tipo 3, 802.3bt	60 W	51 W
8	Tipo 3, 802.3bt	100 W	71,3 W

*Questo tipo è indicato anche con PoE+.

5 Rete

5.1 Protezione e controlli di sicurezza

Esistono diversi modi per contrastare le minacce alle risorse del sistema. Alcune minacce mettono a rischio i dispositivi, mentre altre mettono a rischio le reti o i dati in transito/archivio. Di seguito vengono elencati alcuni controlli di sicurezza che possono essere applicati ai dispositivi e alle reti:

- Le credenziali (nome utente/password) proteggono dagli accessi non autorizzati al video e prevengono gli accessi non autorizzati alla configurazione del dispositivo. Configurando privilegi diversi per i vari account, è possibile controllare le categorie di utenti e i contenuti a cui possono accedere.
- Il filtro indirizzi IP (firewall) riduce l'esposizione della rete locale di un dispositivo, evitando che sia accessibile da client non autorizzati. In questo modo si riducono i rischi qualora la password di un dispositivo sia violata o sia scoperta una nuova vulnerabilità critica.
- IEEE 802.1x: protegge la rete dai client non autorizzati. 802.1x è una protezione dell'infrastruttura di rete mediante switch gestiti e server RADIUS. Il client 802.1x del dispositivo fornisce l'autenticazione al dispositivo in rete.
- HTTPS (Hypertext Transfer Protocol Secure): protegge i dati (video) dall'intercettazione in rete. L'uso dei certificati firmati in HTTPS consente a un client video di rilevare se stia accedendo a una vera telecamera o a un computer dannoso che finge di essere una telecamera.
- Firmware firmato: è implementato dal fornitore del software, che firma l'immagine del firmware con una chiave privata e segreta. Collegando la firma a un firmware, un dispositivo convalida il firmware

prima di accettare di installarlo. Il dispositivo rifiuta l'aggiornamento del firmware se rileva che ne è stata compromessa l'integrità. Il firmware con firma digitale di Axis si basa sul metodo di crittografia a chiave pubblica RSA accettato dal settore.

- Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati eseguita da una memoria non modificabile (bootrom). Essendo basato sul firmware con firma digitale, Secure Boot assicura che un dispositivo possa essere avviato solo con firmware autorizzato. Secure Boot garantisce che il dispositivo Axis sia completamente privo di eventuali malware dopo un ripristino delle impostazioni di fabbrica.
- TPM (Trusted Platform Module): componente che fornisce una serie di funzioni di crittografia adatte alla protezione delle informazioni da accessi non autorizzati. La chiave privata viene memorizzata nel TPM e non lo lascia mai. Tutte le operazioni di crittografia che richiedono l'utilizzo della chiave privata vengono inviate al TPM per essere elaborate. In questo modo, la parte segreta del certificato rimane protetta anche in caso di violazione di sicurezza.
- Axis Edge Vault: modulo di calcolo criptogenico sicuro (modulo sicuro o elemento protetto) per l'installazione e l'archiviazione sicure e permanenti dell'ID del dispositivo Axis.

Per consultare altri documenti sulla cybersecurity, vedere *axis.com/cybersecurity*

5.2 Protocolli supportati

Per il trasferimento sicuro dei dati da un dispositivo di rete a un altro entrano in gioco molti protocolli.

5.2.1 Modelli di riferimento dei protocolli

Il modo migliore per capire l'interazione tra i vari protocolli è fare riferimento al modello di comunicazione Open Systems Interconnection (OSI). È anche disponibile il modello di riferimento TCP/IP.

5.2.1.1 Modello di riferimento OSI

Modello che descrive la comunicazione dati tra sistemi aperti. Per fornire un servizio, ogni livello utilizza i servizi del livello immediatamente sottostante. Ogni livello deve seguire determinate regole, o protocolli, per svolgere i servizi.

Livello 7 – Applicazione

Rende disponibili funzioni come web, file e trasferimento e-mail alle applicazioni.

Le applicazioni effettive, come i browser web o i programmi e-mail, si trovano sopra questo livello e non rientrano nel modello OSI.

Livello 6 – Presentazione (dati)

Garantisce che i dati inviati dal livello applicazione di un sistema possano essere letti dal livello applicazione di un altro sistema. Converte i formati dati dipendenti dai sistemi, come ASCII, in un formato indipendente, consentendo uno scambio di dati sintatticamente corretto tra sistemi diversi.

Livello 5 – Sessione (connessione persistente tra host peer)

Svolge un servizio orientato alle applicazioni ed è preposto alla comunicazione dei processi tra due sistemi. La comunicazione dei processi comincia instaurando una sessione, che è alla base di una connessione virtuale tra due sistemi.

Livello 4 – Trasporto (trasporto end-to-end (protocollo orientato alle connessioni))

Svolge un servizio di trasferimento dati attendibile (attraverso il controllo dei flussi e il controllo degli errori) a livello 5 e superiori.

Livello 3 – Rete (Pacchetti (indirizzamento/frammentazione))

Esegue il trasferimento dati effettivo instradando e inoltrando i pacchetti dati tra i sistemi. Crea e amministra le tabelle di routing e offre opzioni per la comunicazione oltre i limiti della rete. I dati di questo livello sono destinazioni assegnate e indirizzi di origine, utilizzati come base per un routing mirato.

Livello 2 – collegamento dati (Frame)

È incaricato della trasmissione dati e controlla l'accesso al mezzo di trasmissione, combinando i dati in unità dette frame. Il Livello 2 è diviso in due sottolivelli: quello superiore, corrispondente a Logical Link Control (LLC), e quello inferiore, corrispondente a Media Access Control (MAC). LLC semplifica lo scambio di dati, mentre MAC controlla l'accesso al mezzo di trasmissione.

Livello 1 – Fisico (Bit)

Svolge servizi che supportano la trasmissione di dati come flusso di bit su un mezzo, per esempio un collegamento di trasmissione cablato o wireless.

5.2.1.2 Modello di riferimento TCP/IP (Transmission Control Protocol/Internet Protocol)

Il modello di riferimento TCP/IP è un altro modello utilizzato per capire i protocolli e il modo in cui si svolge la comunicazione. Il modello di riferimento TCP/IP è suddiviso in quattro livelli, che corrispondono al modello di riferimento OSI come indicato di seguito.

Tabella 5.1 Confronto tra modelli di riferimento

Modello OSI	Modello TCP/IP
Livello 7 – Applicazione	Livello 4 - Applicazione
Livello 6 - Presentazione	
Livello 5 - Sessione	
Livello 4 - Trasporto	Livello 3 - Trasporto
Livello 3 - Rete	Livello 2 - Internetwork
Livello 2 - Collegamento dati	Livello 1 - Interfaccia di rete
Livello 1 - Fisico	

5.2.2 Protocolli del livello Applicazione

- **CIFS/SMB** (Common Internet File System/Server Message Block): è utilizzato principalmente per consentire l'accesso condiviso a file, stampanti e porte seriali e comunicazioni varie tra i nodi di una rete.
- **DDNS** (Dynamic Domain Name System): è utilizzato per controllare il collegamento di un nome di dominio a indirizzi IPv4 che cambiano.
- **DHCPv4/v6** (Dynamic Host Configuration Protocol): assegnazione e gestione automatiche degli indirizzi IP.
- **DNS/DNSv6** (Domain Name System): converte i nomi di dominio negli indirizzi IP associati.

- **FTP** (File Transfer Protocol): è utilizzato principalmente per trasmettere file da un server a un client (download) o da un client a un server (upload). Può essere utilizzato anche per creare e selezionare directory e rinominare o eliminare directory e file.
- **HTTP** (Hypertext Transfer Protocol): è utilizzato principalmente per caricare testi e immagini da un sito a un browser web. I sistemi video di rete offrono un servizio di server HTTP che consente l'accesso ai sistemi attraverso browser web, per scaricare le configurazioni o le immagini dal vivo.
- **HTTP/2**: importante revisione del protocollo HTTP definita nella norma RFC 7540 e pubblicata a febbraio 2015.
- **HTTPS** (HTTP Secure): adattamento di Hypertext Transfer Protocol (HTTP) per la comunicazione sicura su una rete informatica, è molto utilizzato su Internet. In HTTPS, il protocollo di comunicazione è crittografato da Transport Layer Security (TLS).
- **MQTT** (Message Queuing Telemetry Transport): protocollo di messaggistica standard per l'Internet of Things (IoT). È stato progettato per un'integrazione IoT semplificata ed è utilizzato in una vasta gamma di settori per collegare dispositivi remoti con un'impronta di codice ridotta e una larghezza di banda di rete minima.
- **NTP** (Network Time Protocol): è utilizzato per sincronizzare l'ora di un computer client o server con un altro server.
- **RTP** (Real-Time Transport Protocol): consente il trasferimento di dati in tempo reale tra endpoint del sistema.
- **RTCP** (Real-Time Control Protocol): fornisce statistiche fuori banda e informazioni di controllo per una sessione RTP. Lavora in sinergia con RTP per recapitare e creare dati multimediali, ma non li trasporta.
- **RTSP** (Real-Time Streaming Protocol): controllo avanzato della trasmissione di contenuti multimediali in tempo reale.
- **SFTP** (Secure File Transfer Protocol): consente l'accesso, il trasferimento e la gestione di file su un flusso dati attendibile.
- **SIP** (Session Initiation Protocol): protocollo di comunicazione per segnalare e controllare sessioni di comunicazione multimediali.
- **SIPS** (Session Initiation Protocol Secure): versione crittografata di SIP.
- **SMTP** (Simple Mail Transfer Protocol): standard di trasferimento e-mail su Internet. Le telecamere di rete supportano SMTP per consentire l'invio di avvisi tramite e-mail.
- **SNMPv1/v2/v3** (Simple Network Management Protocol): è utilizzato per monitorare e gestire da remoto apparecchiature connesse in rete come switch, router e telecamere di rete. Il supporto SNMP consente la gestione delle telecamere di rete con strumenti open source.
- **SOCKS**: consente il trasferimento dei pacchetti di rete tra client e server attraverso un proxy remoto.
- **SRTP** (Secure Real-Time Transport Protocol): consente il trasferimento crittografato dei dati in tempo reale tra endpoint del sistema, dunque è una variante sicura di RTP.
- **SSH** (Secure Shell): consente la gestione e l'accesso al debug di dispositivi di rete in sicurezza su una rete non protetta.
- **TLSv1.2/v1.3** (Transport Layer Security): negozia una connessione privata e attendibile tra client e server.

5.2.3 Protocolli del livello Trasporto

- **TCP** (Transmission Control Protocol): recapito orientato alla connessione, attendibile e ordinato di flussi dati. È il protocollo più comune per il trasporto di dati.
- **UDP** (User Datagram Protocol): servizio di trasmissione senza connessione, favorisce la puntualità di recapito dei dati rispetto all'attendibilità.
- **ICMP** (Internet Control Message Protocol): invia messaggi di errore e informazioni operative indicanti che un servizio richiesto non è disponibile o che un host o un router non sono raggiungibili.

5.2.4 Protocolli del livello Rete

- **IGMPv1/v2/v3** (Internet Group Management Protocol): è utilizzato da host e router adiacenti su reti IPv4 per attestare l'appartenenza a gruppi multicast. Quando si supportano questi tipi di applicazioni, consente un uso più efficiente delle risorse.
- **IPv4/IPv6** (Internet Protocol): indirizzo pubblico individuale necessario ai dispositivi per comunicare via Internet. IPv4 è la versione originale e utilizza indirizzi a 32 bit. IPv6 è la versione più recente e utilizza indirizzi a 128 bit divisi in otto gruppi da quattro cifre esadecimali.
- **USGv6**: profilo che descrive standard tecnici per IPv6. È definito dal governo degli Stati Uniti per garantire la compatibilità durante l'approvvigionamento di dispositivi di rete IPv6.

5.2.5 Protocolli del livello Collegamento dati

- **ARP** (Address Resolution Protocol): è utilizzato per individuare l'indirizzo MAC dell'host di destinazione.
- **CDP** (Cisco Discovery Protocol): protocollo proprietario di Cisco utilizzato in alternativa a LLDP per individuare informazioni sui dispositivi hardware connessi.
- **IEEE 802.3 (i, u, ab)**: standard Ethernet che definiscono la comunicazione dati a 10Mb/s (10Base-T), 100Mb/s (100Base-TX) e 1Gb/s (1000Base-T) su cavi a doppino intrecciato.
- **LLDP** (Link Layer Discovery Protocol): è utilizzato per annunciare l'identità di un dispositivo e le sue funzionalità, ma anche altri dispositivi connessi alla stessa rete.

5.2.6 Protocolli di individuazione

- **mDNS (Bonjour)**: può essere utilizzato per individuare prodotti video di rete che utilizzano computer Mac, oppure come protocollo di individuazione per nuovi dispositivi in qualsiasi rete.
- **UPnP** (Universal Plug and Play): i sistemi operativi Microsoft riescono a individuare automaticamente le risorse (dispositivi Axis) in rete.
- **Zeroconf**: assegna automaticamente un dispositivo di rete a un indirizzo IP non utilizzato nell'intervallo da 169.254.1.0 a 169.254.254.255.

5.2.7 Quality of Service

In una rete IP è necessario controllare le modalità di condivisione delle risorse di rete per soddisfare i requisiti di ciascun servizio.

- **QoS** (Quality of Service): capacità di assegnare priorità al traffico in rete, in modo da servire i flussi critici prima di quelli meno prioritari. Aumenta l'affidabilità in rete controllando la larghezza di

banda utilizzabile da un'applicazione e offrendo la possibilità di controllarne il consumo tra le varie applicazioni.

- **DiffServ** : la rete cerca di svolgere un servizio specifico in base al QoS specificato da ciascun pacchetto.

5.2.8 Metodi di trasmissione dei dati

I dati possono essere trasmessi in rete in tre modi diversi.

- **Unicast**: è il più comune. Il mittente e il destinatario comunicano utilizzando uno schema point-to-point. I pacchetti di dati vengono inviati a un solo destinatario e nessun altro client riceve le informazioni.
- **Multicast**: comunicazione tra un unico mittente e più destinatari connessi in rete. Riduce il traffico di rete consegnando un solo flusso di informazioni a più destinatari.
- **Broadcast**: il mittente invia le stesse informazioni a tutti gli altri server su una rete; tutti gli host in rete ricevono il messaggio e lo elaborano in qualche misura.

T10169734/IT/M1.10/2111

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni di rete che forniscono informazioni per migliorare la sicurezza e nuovi modi di condurre un'attività. In qualità di leader del settore nel video di rete, Axis offre prodotti e servizi per la videosorveglianza e l'analisi, controllo degli accessi, sistemi di citofoni e audio. Axis ha più di 3.800 dipendenti in oltre 50 paesi e collabora con partner di tutto il mondo per fornire soluzioni ai clienti. Axis è stata fondata nel 1984 e la sua sede principale si trova a Lund, in Svezia.

Per ulteriori informazioni su Axis, si prega di visitare il nostro sito Web *axis.com*.