



001

À
CÂMARA MUNICIPAL DE SUMARÉ
ESTADO DE SÃO PAULO
(Rua Barbara Blumer, nº 41 – Jardim Alvorada)

PREGÃO PRESENCIAL Nº 14/2024
PROCESSO ADMINISTRATIVO Nº 458/2024

TIPO: MENOR PREÇO GLOBAL

Objeto: Contratação de empresa especializada para execução do Projeto de Sistema de Videomonitoramento inteligente, e prestação de serviços de locação de equipamentos, incluindo toda a infraestrutura física e interligação dos prédios sede, Anexo e Escola do Legislativo, da Camara Municipal de Sumaré.

EM BRANCO

[Handwritten signatures and marks]

“ENVELOPE Nº 01”
PROPOSTA COMERCIAL

[Handwritten signatures and marks]



002

À
CÂMARA MUNICIPAL DE SUMARÉ
ESTADO DE SÃO PAULO
(Rua Barbara Blumer, nº 41 – Jardim Alvorada)

PREGÃO PRESENCIAL Nº 14/2024
PROCESSO ADMINISTRATIVO Nº 458/2024

TIPO: MENOR PREÇO GLOBAL

EM BRANCO

Handwritten signature and initials in blue ink.

CARTA DE APRESENTAÇÃO

Handwritten signature and initials in blue ink.

A
CÂMARA MUNICIPAL DE SUMARÉ
REF.:PREGAO PRESENCIAL N° 014/2024
PROCESSO ADMINISTRATIVO N° 458/2024

OBJETO: Contratação de empresa especializada para Execução do Projeto de Sistema de Videomonitoramento Inteligente, e prestação de serviços de locação de equipamentos, incluindo toda a infraestrutura física e interligação dos prédios Sede, Anexo e Escola do Legislativo, da Câmara Municipal de Sumaré

CARTA DE APRESENTAÇÃO

A empresa **TALENTECH-TECNOLOGIA LTDA**, inscrita no CNPJ sob n. 15.773.416/0001-10, com sede na avenida Presidente Altino, 1925 – Galpão 2 - Bloco C – Jaguaré – CEP: 05.323-002, no município de São Paulo, estado de São Paulo, por seu representante legal, o **Sr. João Batista Alves Junior**, portador do RG nº 29.112.325-9 SSP-SP, devidamente inscrito no C.P.F sob o nº 292.350.078-44, Diretor e por seu procuradora o **Sr. Adriano Rogério de Souza**, portador do RG nº 33.284.586-2 SSP/SP, inscrito no C.P.F sob o nº 284.939.248-06, **DECLARA**, tem a satisfação de encaminhar para apreciação e análise desta respeitosa comissão, sua “**PROPOSTA DE PREÇO**” para fins de participação no **PREGAO PRESENCIAL**, acima mencionado, para tanto, **DECLARA** que:

- a) Não se encontra em estado de falência;
- b) Não foi declarada inidônea por qualquer órgão da Administração Pública, direta ou indireta; federal, estadual ou municipal, bem como a que esteja punida com suspensão do direito de contratar ou licitar com a Administração Municipal, Lei Federal nº 14.133/21;
- c) Não possui em seu quadro servidor de qualquer órgão ou entidade vinculada a **CÂMARA MUNICIPAL DE SUMARÉ**, bem assim a empresa da qual tal servidor seja sócio, dirigente ou responsável técnico;
- d) Não está impedida de licitar e contratar;
- e) Não é empresa estrangeira;
- f) Não é autora do Termo de Referência, do projeto básico ou executivo, pessoa física ou jurídica;
- g) Declara não violar qualquer lei, norma e/ou regulamento nacional ou internacional anticorrupção, inclusive, mas não se limitando, aos termos da Lei Federal nº 12.846/2013, ainda, que se compromete a observar e cumprir rigorosamente todas as leis anticorrupção cabíveis, incluindo a legislação antes citada; e
- h) Declara que possui Programa de Integridade e Compliance implantado que consiste no conjunto de mecanismos e procedimentos internos de integridade, auditoria, controle e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública.

Nestes termos coloca-se à disposição para quaisquer esclarecimentos que se fizerem necessários.


Sendo só para o momento, subscreve-se.

São Paulo, 09 de outubro de 2024.



TALENTECH – TECNOLOGIA LTDA



João Batista Alves Júnior
Diretor
RG: 29.112.325-9 SSP/ SP
CPF: 292.350.078-44



Adriano Rogério de Souza
Procurador
RG: 33.284.586-2 SSP/SP
CPF: 284.939.248-06



TALENTECH – TECNOLOGIA LTDA.

Av. Presidente Altino, 1925 – Galpão 2 Bloco C – Jaguaré - São Paulo – SP – CEP: 05.323-002 – Brasil
Telefone: 55 (11) 3831-6032 - E-mail: licitacoes@tecnologiagto.com.br



004

À
CÂMARA MUNICIPAL DE SUMARÉ
ESTADO DE SÃO PAULO
(Rua Barbara Blumer, nº 41 – Jardim Alvorada)

PREGÃO PRESENCIAL Nº 14/2024
PROCESSO ADMINISTRATIVO Nº 458/2024

TIPO: MENOR PREÇO GLOBAL

EM BRANCO

[Handwritten signature]

[Handwritten mark]

[Handwritten mark]

PROPOSTA DE PREÇO

[Handwritten signature]
[Handwritten signature]
[Handwritten signature]



006

VALIDADE DA PROPOSTA: Será de 60 (sessenta) dias a contar da data de sua apresentação nesta licitação.

INDICAÇÃO DO RESPONSÁVEL PARA ASSINATURA DO CONTRATO

Representante Legal (Nome Legível): João Batista Alves Junior

() Sócio (x) Procurador Profissão: Administrador

RG: 29.112.325-9 – SSP – SP - CPF: 292.350.078-44

Nacionalidade: Estado Civil: Divorciado

Endereço: Alameda doS Cravos, 83 – Morada das Flores – Aldeia da Serra – Santana de Parnaíba – SP – CEP. 06519-500

Telefone: (11) 3831-6032 - E-mail: licitacoes@tecnologiagto.com.br

Representante Legal (Nome Legível): Cláudia Felix Lousa

() Sócio (x) Procurador Profissão: Administradora

RG: 392.642 – SSP – SP - CPF: 692.317.451-15

Nacionalidade: Estado Civil: Divorciada

Endereço: SQS 114 – BLOCO G – Apto 208 – Brasília – DF – CEP.: 70.377 - 070

Telefone: (11) 3831-6032 - E-mail: licitacoes@tecnologiagto.com.br

REPRESENTANTE RESPONSÁVEL PELA EXECUÇÃO DO CONTRATO

Representante: Charbel Rodrigues Calil Daher

Cargo: Responsável Técnico

RG: 28.933.256 – 6 - CPF: 301.636.278-35

Telefone: (11) 3831 – 6032 - E-mail: licitacoes@tecnologiagto.com.br

DADOS BANCÁRIOS

Banco: 237 – Bradesco

Agência: 502

Conta para depósito: 020060-1

Titular: TALENTECH – TECNOLOGIA LTDA

São Paulo, 09 de outubro de 2024

TALENTECH – TECNOLOGIA LTDA.

João Batista Alves Junior

Diretor

RG: 29.112.325 – SSP/SP

CPF: 292.350.078-44

Adriano Rogério de Souza

Procurador

RG: 33.284.586-2 – SSP/SP

CPF: 284.939.248-06

TALENTECH – TECNOLOGIA LTDA.

Av. Presidente Altino, 1925 – Galpão 2 Bloco C – Jaguaré - São Paulo – SP – CEP: 05.323-002 – Brasil
Telefone: 55 (11) 3831-6032 - E-mail: licitacoes@tecnologiagto.com.br



Série 800 - CLAMPER Ethernet CAT5e

Especialista na proteção contra raios e surtos elétricos

Descrição

Dispositivo de Proteção contra Surtos (DPS), categoria 5e (CAT5e), com conector RJ45 blindado, para a proteção de equipamentos eletroeletrônicos conectados à rede Ethernet de até 1 Gbps, com ou sem a funcionalidade de Power over Ethernet (PoE), com ou sem o acompanhamento do kit de aterramento.

Características

- Velocidade de até 1 GHz;
- Modo A e B;
- Corrente de carga de 1 A;
- Todas as linhas protegidas;
- Tempo de resposta da ordem de pico segundos;
- Alta capacidade de dreno de corrente.

Principais aplicações

- Pontos de acesso de rede sem fio;
- Câmeras de rede PoE;
- Switches remotos PoE;
- Dispositivos embarcados.



Características técnicas	Unid.	Série 800 - CLAMPER Ethernet CAT5e			
Norma aplicável	-	IEC 61643-21 Ato 1120 da ANATEL			
Código CLAMPER	-	013201	013202	017190	017198
Modelos	-	S800 CLAMPER Ethernet CAT5e	S800 CLAMPER Ethernet CAT5e + PoE	S800 CLAMPER Ethernet CAT5e*	S800 CLAMPER Ethernet CAT5e+PoE*
Conexão de terra	-	Parafuso M3		Parafuso M5	
Kit de aterramento	-	Não incluído		Incluído	
Tecnologia de proteção	-	Diodo de Avalanche de Silício (SAD) e Centelhador a Gás (GDT)			
Tempo de resposta típico	ps	1			
Corrente de carga nominal - I _L	A	1			
Número de condutores protegidos	-	8			
Máxima tensão de operação contínua (linha-linha) - U _C	V	6			
Máxima tensão de operação contínua (linha-terra) - U _C	V	150			
Máxima tensão de operação contínua (PoE) - U _C	V	-	50	-	50
Tensão residual (linha-linha) @ 100 A 8/20 μs - U _{res}	V	20			
Tensão residual (linha-linha) @ 15 A 10/100 μs - U _{res}	V	97			
Tensão de disparo sob impulso (linha-terra) @ 100 V/μs	V	< 600			
Corrente de descarga máxima (linha-linha) @ 8/20 μs - I _{max}	A	100			
Corrente de descarga nominal (linha-terra) @ 8/20 μs - I _n	kA	10			
Corrente total de descarga nominal (linha-terra) @ 8/20 μs - I _n	kA	40			
Capacitância máxima (linha-linha) à 1 MHz	pF	12			
Capacitância máxima (linha-terra) à 1 MHz	pF	13,5			
Velocidade de transmissão	Gbps	1			
Temperatura de operação	°C	-40 ... +70			
Conexão de entrada e saída	-	Conector RJ45 CAT5e Fêmea blindado			
Acondicionamento	-	Materiais com características de não propagação e auto-extinção do fogo			
Grau de proteção	-	IP20			
Peso aproximado	g	42	47	50**	55**
Dimensões	mm	81 x 57 x 22,3 (C x L x A)			

*Versões acompanhadas com kit de aterramento.

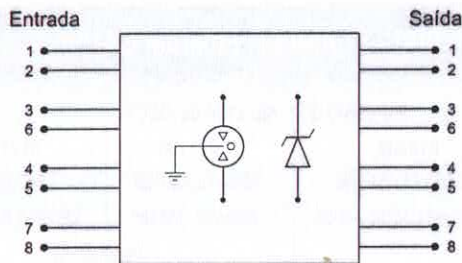
** O peso apresentado não inclui o kit de aterramento

Especialista na proteção contra raios e surtos elétricos

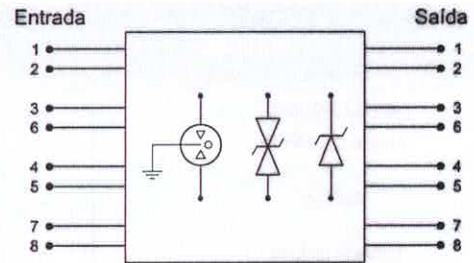
Kit de aterramento:

Quantidade	Unid.	Descrição
1,8	mt	Cabo flexível Isolado 750V Verde 16mm ² Classe 4
2	pç	Arruela de Pressão M5 Zincado Claro
2	pç	Porca Sextavada M5 bicromatizada
2	pç	Parafuso Cabeça Painel Rosca Métrica Bicromatizado Fenda Combinada M5x14mm
2	pç	Terminal Anel 10-35mm ² Furo M5 com Isolação

Circuito elétrico:

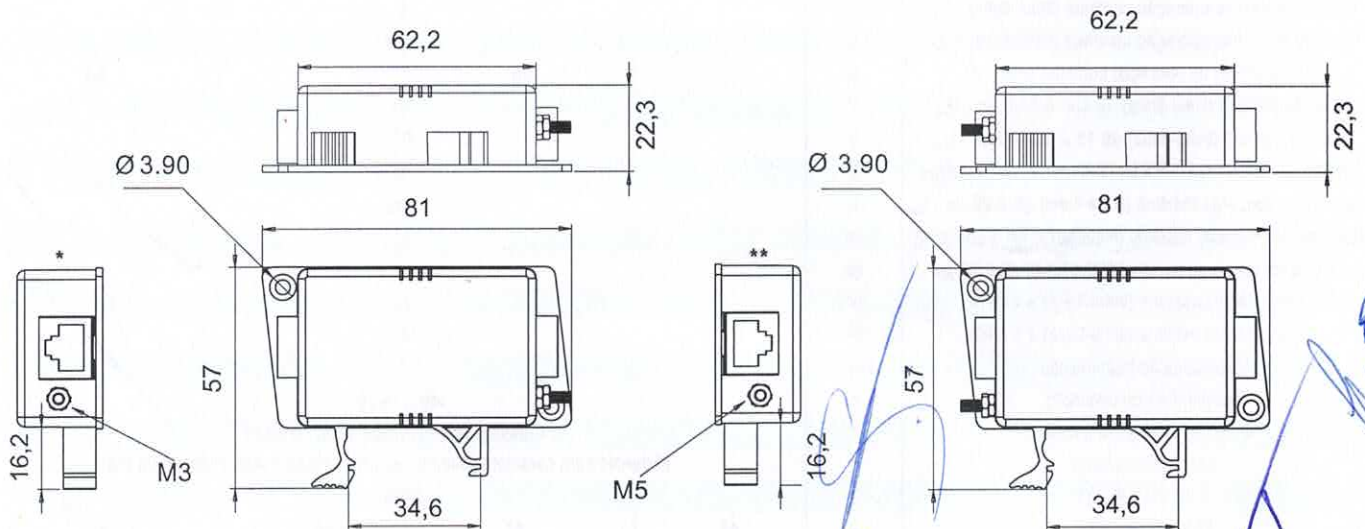


S800 CLAMPER Ethernet CAT5e



S800 CLAMPER Ethernet CAT5e + PoE

Desenho mecânico:



*Versão sem kit aterramento

**Versão com kit aterramento

Dimensões dadas em mm.

EPS 301

Dispositivo de proteção contra surtos elétricos bivolt



O EPS 301 é um dispositivo de proteção contra surtos de tensão provenientes da rede elétrica. O produto ainda conta com proteções essenciais para seu eletro, como curto-circuito e sobrecarga. Também possui filtro de linha para atenuação de ruídos EMI/RFI.

- » Dispositivo de proteção contra surtos de tensão nos três condutores de entrada (Fase, Neutro e Terra)
- » Proteções contra curto-circuito e sobrecarga
- » Proteção térmica do DPS, prevenindo aumento excessivo de temperatura durante surtos da rede
- » Filtro de linha para atenuação de ruídos EMI/RFI
- » LED indicativo de proteção ativa do dispositivo conectado ao EPS 301
- » 100 a 240 Vac bivolt automático – 50/60 Hz
- » Disponível nas cores branca e preta

Especificações técnicas

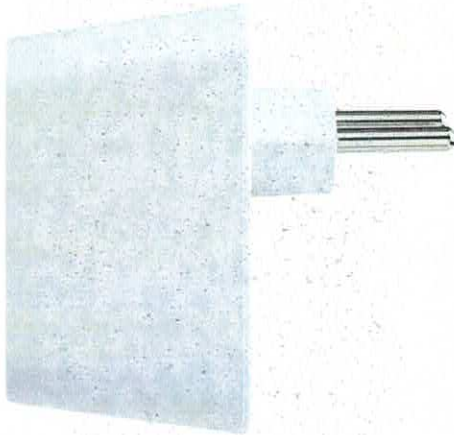
Tensão nominal	100 ~ 240 Vac
Corrente máxima	10 A
Potência máxima de operação	1.270 W (127V) e 2.200 W (220 V)
Frequência da rede elétrica	50 ou 60 Hz
Conexão de entrada	Plugue 2P + T (NBR 14136) 10 A
Quantidade de tomadas	1 tomada 2P + T (NBR 14136) 10 A
Temperatura de operação	0 ~ 40 °C
Grau de proteção	IP 20
Peso	72 g
Dimensões	66 x 56 x 70 mm
Proteção	
Tecnologias de proteção	Varistor: proteção contra surtos de tensão nos três condutores (Fase, Neutro e Terra)

	Fusíveis de classe especial: proteção contra curto-circuito, sobrecarga e proteção térmica do DPS
Máxima absorção de energia	125 J por par afetado no surto (F/N, F/T ou N/T)
Tempo máximo de resposta	25 ns
Tensão de circuito aberto – Uoc	Classe III – 6 KV
Nível de proteção de tensão – Up	0,9 KV
Máxima tensão de operação contínua – Uc	300 Vac
Frequência de operação do filtro de linha	150 kHz – 100 MHz
Máxima atenuação do filtro de linha	40 dB

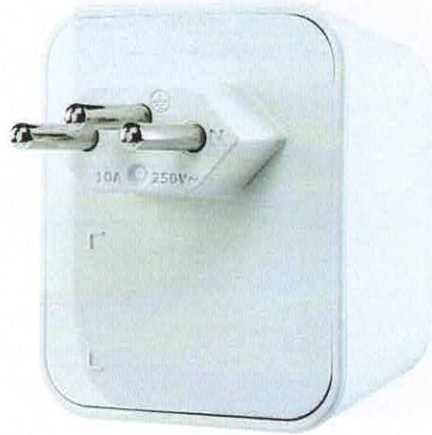
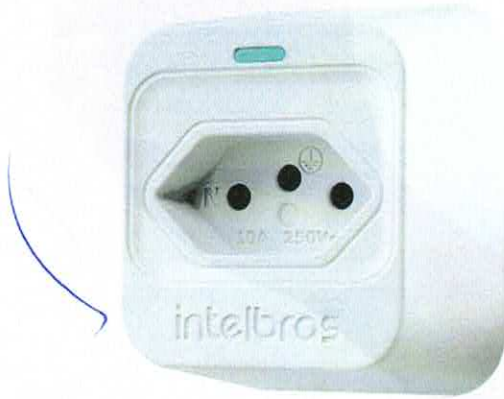
Fotos do produto



Handwritten signatures and initials in blue ink.



Handwritten signatures and marks in blue ink.



[Handwritten signature and scribbles in blue ink]

iDS-2CD7A47G0-XZHS(Y)(C)
4 MP DarkFighterS DeepinView Varifocal Bullet Camera

DarkFighter 

DeepinView^{series}



Hikvision has been dedicated to develop products with security since established. Hikvision always follows security by design principle and has adopted many methods of security technologies into our product development lifecycle, including terminal security, data security, application security, network security, and privacy protection. In the meantime, the security technologies used by Hikvision are all in compliance with local applicable laws and safety regulations. These security measures could enhance product's cyber security protection capability and protect your devices as well as your data from malicious cyber attacks.

- High quality imaging with 4 MP resolution
- Excellent low-light performance via DarkfighterS technology
- Clear imaging against strong back light due to 140 dB WDR technology
- Efficient H.265+ compression technology to save bandwidth and storage
- 5 streams to meet a wide variety of applications
- Water and dust resistant (IP67) and vandal proof (IK10)

▪ **Function**

Face Capture

With embedded deep learning based algorithms, the camera is able to give the best shot of a target face through detecting, capturing, grading and selecting. The camera uses face exposure function to dynamically adjust face area exposure of captures and ensures high face picture quality.

Perimeter Protection

With embedded deep learning based target detection and classification algorithms, the camera carries out the duty of perimeter protection, monitoring the actions of line crossing, intrusion, region entrance, and region exiting. The algorithms greatly filter out the mistaken alarm caused by the interference of leaves, lights, animal, flag, etc.

Multi-Target-Type Detection

With the embedded deep learning algorithms, the camera detects and captures the face, human body, vehicle in the specified region.

Queue Management

With embedded deep learning based algorithms, the camera detects queuing-up people number and waiting time of each person. It can generate reports to compare the efficiency of different queuing-ups and display the changing status of one queue, and supports raw data export for further analysis.

Regional People Counting

With the embedded deep learning algorithms, the camera supports people density detection and will upload detection data through scheduled uploading, number of people change uploading and congestion level uploading. It also supports number of people exception detection and waiting time exception detection.

On/Off Duty Detection

With the embedded deep learning algorithms, the camera supports absence detection and on/off duty detection. It can detect the on/off duty status and people number changes in a predefined area.

Heat Map

The camera can generate a graphic description of visits (by calculating amount of people or amount of dwell time) in a configured area.

Multi-Dimension People Counting

With the embedded deep learning algorithms, the camera integrates multiple intelligences. It counts persons and compares them with the built-in face picture library to remove duplicates. It counts persons and reports an alarm simultaneously to achieve both the entrance control and people counting.

Hard Hat Detection

With the embedded deep learning algorithms, the camera detects the persons in the specified region. It detects whether the person is wearing a hard hat, and reports an alarm if not.

[Handwritten signatures and initials in blue ink]

▪ Specification

Camera	
Image Sensor	1/1.8" Progressive Scan CMOS
Max. Resolution	2688 × 1520
Min. Illumination	Color: 0.0003 Lux @ (F1.0, AGC ON), B/W: 0.0001 Lux @ (F1.0, AGC ON), 0 Lux with light
Shutter Time	1 s to 1/100,000 s
Day & Night	IR cut filter, Blue glass module (less ghost phenomenon)
Angle Adjustment	Pan: 0° to 355°, tilt: 0° to 90°, rotate: 0° to 360°
Lens	
Focal Length & FOV	2.8 to 12 mm, horizontal FOV 99.8° to 44.1°, vertical FOV 54.6° to 24.8°, diagonal FOV 113.8° to 51.1°
Focus	Auto, Semi-auto, Manual
Iris Type	P-iris
Aperture	F1.0 to F1.2
DORI	
DORI	Wide: D (Detect): 63.4 m, O (Observe): 25.2 m, R (Recognize): 12.7 m, I (Identify): 6.3 m Tele: D (Detect): 140.7 m, O (Observe): 55.8 m, R (Recognize): 28.1 m, I (Identify): 14.1 m
Illuminator	
Supplement Light Type	Hybrid (IR and White Light)
Supplement Light Range	Up to 50 m
Smart Supplement Light	Yes
IR Wavelength	850 nm
AI Open Platform	
Model Specification	Up to 4 models, Model type: detection model, classification model, mixed model (detection model and classification model)
Video	
Main Stream	50 Hz: 25 fps (2688 × 1520, 2560 × 1440, 1920 × 1080, 1280 × 720) 50 fps (2560 × 1440, 1920 × 1080, 1280 × 720) 60 Hz: 30 fps (2688 × 1520, 2560 × 1440, 1920 × 1080, 1280 × 720) 60 fps (2560 × 1440, 1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (704 × 576, 640 × 480) 60 Hz: 30 fps (704 × 480, 640 × 480)
Third Stream	50 Hz: 25 fps (1920 × 1080, 1280 × 720, 704 × 576, 640 × 480) 60 Hz: 30 fps (1920 × 1080, 1280 × 720, 704 × 480, 640 × 480)
Fourth Stream	50 Hz: 25 fps (704 × 576, 640 × 480) 60 Hz: 30 fps (704 × 480, 640 × 480)
Fifth Stream	50 Hz: 25 fps (704 × 576, 640 × 480) 60 Hz: 30 fps (704 × 480, 640 × 480)

Handwritten signatures and initials in blue ink, including 'JL', 'PM', and 'H'.

Video Compression	Main stream: H.265+/H.265/H.264+/H.264, Sub-stream: H.265/H.264/MJPEG, Third stream: H.265/H.264, Fourth stream: H.265/H.264/MJPEG, Fifth stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 8 Mbps
H.264 Type	Baseline Profile,Main Profile,High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR,VBR
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	4 fixed regions for each stream
Target Cropping	Yes
e-PTZ	Support Patrol and Auto Tracking settings
Audio	
Audio Type	Mono sound
Audio Compression	G.711/G.722.1/G.726/MP2L2/PCM/MP3/AAC-LC
Audio Bit Rate	64 Kbps (G.711ulaw/G.711alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 192 Kbps (MP2L2)/8 to 320 Kbps (MP3)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	8 kHz/16 kHz/32 kHz/44.1 kHz/48 kHz
Environment Noise Filtering	Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, Filter IP, HTTPS, FTP, SFTP, DHCP, DNS, DDNS, SRTP, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv4, IPv6, UDP, Bonjour, SSL/TLS, ARP, WebSocket, WebSockets
Simultaneous Live View	Up to 20 channels
API	Open Network Video Interface (Profile S, Profile G, Profile T, Profile M),ISAPI,SDK,ISUP
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Security	Password protection, complicated password, HTTPS encryption, 802.1X authentication (EAP-TLS, EAP-LEAP, EAP-MD5), watermark, IP address filter, basic and digest authentication for HTTP/HTTPS, Protocol DDoS e anti Phishing, WSSE and digest authentication for Open Network Video Interface, RTP/RTSP OVER HTTPS, Control Timeout Settings, Security Audit Log, TLS 1.2, TLS 1.3, TPM 2.0 (FIPS 140-2 level 2), AES128/256
Network Storage	NAS (NFS, SMB/CIFS),Auto Network Replenishment (ANR), Together with high-end Hikvision memory card, memory card encryption and health detection are supported.
Client	iVMS-4200,Hik-Connect,Hik-Central
Web Browser	Plug-in required live view: IE 10, IE 11, Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Edge 89+, Safari 11+ Local service: Chrome 57.0+, Firefox 52.0+, Edge 89+
Image	
Image Parameters Switch	Yes
Image Settings	Rotate mode,saturation,brightness,contrast,sharpness,white balance,AGC,adjustable by client software or web browser

Day/Night Switch	Day,Night,Auto,Schedule,Alarm Trigger,Video Trigger
Wide Dynamic Range (WDR)	140 dB
Image Enhancement	BLC,HLC,3D DNR,Distortion Correction,Defog
Privacy Mask	8 programmable polygon privacy masks
SNR	≥ 52 dB
Picture Overlay	LOGO picture can be overlaid on video with 128 × 128 24 bit bmp format.
Image Stabilization	EIS
Interface	
Video Output	1 Vp-p Composite Output (75 Ω/CVBS) (Only for debugging)
Ethernet Interface	1 RJ45 10 M/100 M/1000 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 1 TB
Alarm	2 inputs, 2 outputs (max. 24 VDC, 1 A)
Audio	1 input (line in), 3.5 mm connector, three-contact, max. input amplitude: 3.3 Vpp, input impedance: 4.7 KΩ, interface type: non-equilibrium, 1 output (line out), 3.5 mm connector, three-contact, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω, interface type: non-equilibrium, mono sound
RS-485	1 RS-485 (Half duplex, HIKVISION, Pelco-P, Pelco-D, self-adaptive)
Reset Key	Yes
Power Output	12 VDC, max. 100 mA
Event	
Basic Event	Motion detection (support alarm triggering by specified target types (human and vehicle)),video tampering alarm,video quality diagnosis,exception (network disconnected, IP address conflict, illegal login, abnormal restart, HDD full, HDD error),vibration detection
Smart Event	scene change detection,audio exception detection,defocus detection
Linkage	Upload to FTP/NAS/memory card,notify surveillance center,send email,trigger alarm output,trigger recording,trigger capture,audible warning
Deep Learning Function	
Multi-target-type Detection	Supports simultaneous detection and capture of human body, face and vehicle, Obtains 7 facial characteristics, mask, gender, type and color of clothing, hat, glasses, Gets 13 characteristics of the human body, Gets vehicle resources, vehicle color, vehicle type and vehicle brand, Supports counting the number of targets crossing the line by type, including human body, non-motorized vehicle, motorized vehicle,tip Supports dynamic tiling mask
Face Capture	Detects up to 120 faces simultaneously, captures up to 40 face pictures per frame simultaneously and uploads up to 10 face pictures per second, Supports swing left and right from -60° to 60°, tilt up and down from -30° to 30°, Uploads face with background and closed-up face pictures, Supports best shot and quick shot for capture mode, Supports dynamic mosaic mask, Gets 7 face features
Face Comparison	Up to 10 face libraries. 30,000 faces for each library. 150,000 faces in total, Supports face library encryption

Handwritten signatures and initials in blue ink.

<p>People Counting</p>	<p>Supports Multi-Dimension People Counting, Supports counting, displaying and exporting the people flow data of entering, exiting and passing by (The data is stored in the flash.), Supports real-time uploading and uploading by statistic cycle, Supports generating daily, weekly, monthly or annually reports, Supports dynamic deduplication based on face picture comparison, and can filter out the target with the same custom face pictures, same attributes, or filter out repeated invalid targets within the set time interval, Supports face feature deduplication, Supports people flow data replenishment</p>
<p>Queue Management</p>	<p>Supports up to 8 detection regions, and independent arming schedule and linkage method Supports 2 detection modes: regional people queuing-up, waiting time detection Generates reports to compare the efficiency of different queuing-ups and display the changing status of one queue Supports raw data export for further analysis Supports real-time data uploading and scheduled data uploading Regional people queuing-up: supports 4 alarm trigger conditions, including greater than threshold, less than threshold, equal to threshold, not equal to threshold Waiting time detection: supports 1 alarm trigger condition, including greater than threshold</p>
<p>Heat Map</p>	<p>A graphic description of visits (by calculating amount of people or amount of dwell time) in a configured area., Two report types are available, space heat map and time heat map line chart.</p>
<p>Hard Hat Detection</p>	<p>Detects up to 30 human targets simultaneously Supports up to 4 shield regions</p>
<p>Perimeter Protection</p>	<p>Line crossing, intrusion, region entrance, region exiting Support alarm triggering by specified target types (human and vehicle) Support combined event alarm triggering</p>
<p>Metadata</p>	<p>Intrusion detection,line crossing detection,region entrance detection,region exiting detection,face capture,multi-target-type detection</p>

Handwritten signatures and initials in blue ink, including a large signature on the left, a signature in the center, and initials 'H' and 'J' at the bottom.

Regional People Counting	<p>Supports up to 8 detection regions, and independent arming schedule and linkage method</p> <p>Supports 3 detection modes: people density detection, number of people exception detection, waiting time exception detection</p> <p>Supports parameter settings: alarm times per exception, alarm interval, first alarm delay</p> <p>Supports searching real-time number of people</p> <p>People density detection: supports scheduled uploading, number of people change uploading, congestion level uploading</p> <p>Number of people exception detection: supports 6 alarm trigger conditions, including greater than threshold A, less than threshold A, equal to threshold A, not equal to threshold A, greater than threshold A and less than threshold B, less than threshold A or greater than threshold B (threshold A should be less than threshold B)</p> <p>Waiting time exception detection: supports 3 alarm trigger conditions, including greater than threshold A, less than threshold A, greater than threshold A and less than threshold B (threshold A should be less than threshold B)</p>
On/Off Duty Detection	<p>Supports up to 8 detection regions, and independent arming schedule and linkage method</p> <p>Supports 2 detection modes: absence detection, on/off duty detection</p> <p>Supports parameter settings: person on duty, absence duration</p>
General	
Power	<p>Three-core terminal block, 12 VDC \pm 20%, 1.90 A, max. 22.7 W, 24 VAC \pm 20%, 1.39 A, max. 22.3 W, PoE: IEEE 802.3at, Type 2, Class 4, 42.5 V to 57 V, 0.59 A to 0.44 A, max. 24.7 W</p>
Material	Aluminum alloy body
Dimension	\varnothing 140 mm \times 378.4 mm (\varnothing 5.5" \times 14.9")
Package Dimension	425 mm \times 190 mm \times 180 mm (16.7" \times 7.5" \times 7.1")
Weight	Approx. 2280 g (5.0 lb.)
With Package Weight	Approx. 3370 g (7.4 lb.)
Storage Conditions	-40 °C to 60 °C (-40 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-40 °C to 60 °C (-40 °F to 140 °F). Humidity 95% or less (non-condensing)
Language	33 languages: English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian
General Function	Heartbeat, anti-banding, one-key reset, mirror, password protection, flash log
Heater	Yes
Demist	Yes
Device Management	Supports adding alarm box (DS-FM2466) in the LAN to expand 6 additional input and 6 output alarm interfaces

Approval	
EMC	FCC: 47 CFR Part 15, Subpart B, CE-EMC: EN 55032: 2015, EN 61000-3-2:2019, EN 61000-3-3: 2013+A1:2019, EN 50130-4: 2011 +A1: 2014, RCM: AS/NZS CISPR 32: 2015, IC: ICES-003: Issue 7, KC: KN32: 2015, KN35: 2015
Safety	UL: UL 62368-1, CB: IEC 62368-1: 2014+A11, CE-LVD: EN 62368-1: 2014/A11: 2017, BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005, LOA: IEC/EN 60950-1
Environment	CE-RoHS: 2011/65/EU, WEEE: 2012/19/EU, Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013, IK10: IEC 62262:2002
Anti-Corrosion Protection	-Y: NEMA 4X (NEMA 250-2018)
Automotive and Railway	EN50121-4
Other	PVC FREE

▪ Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

With -Y model: This model has MODERATE PROTECTION.

Without -Y model: This model has NO SPECIFIC PROTECTION.

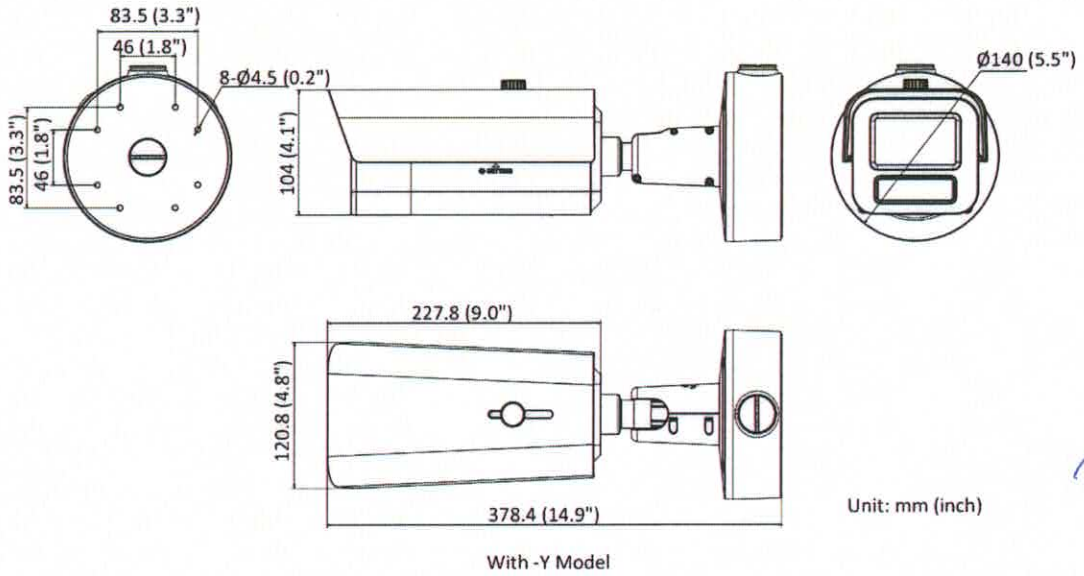
Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Available Model

iDS-2CD7A47G0-XZHSY(C)(2.8-12mm)

iDS-2CD7A47G0-XZHS(C) (2.8-12mm)

▪ Dimension



▪ Accessory

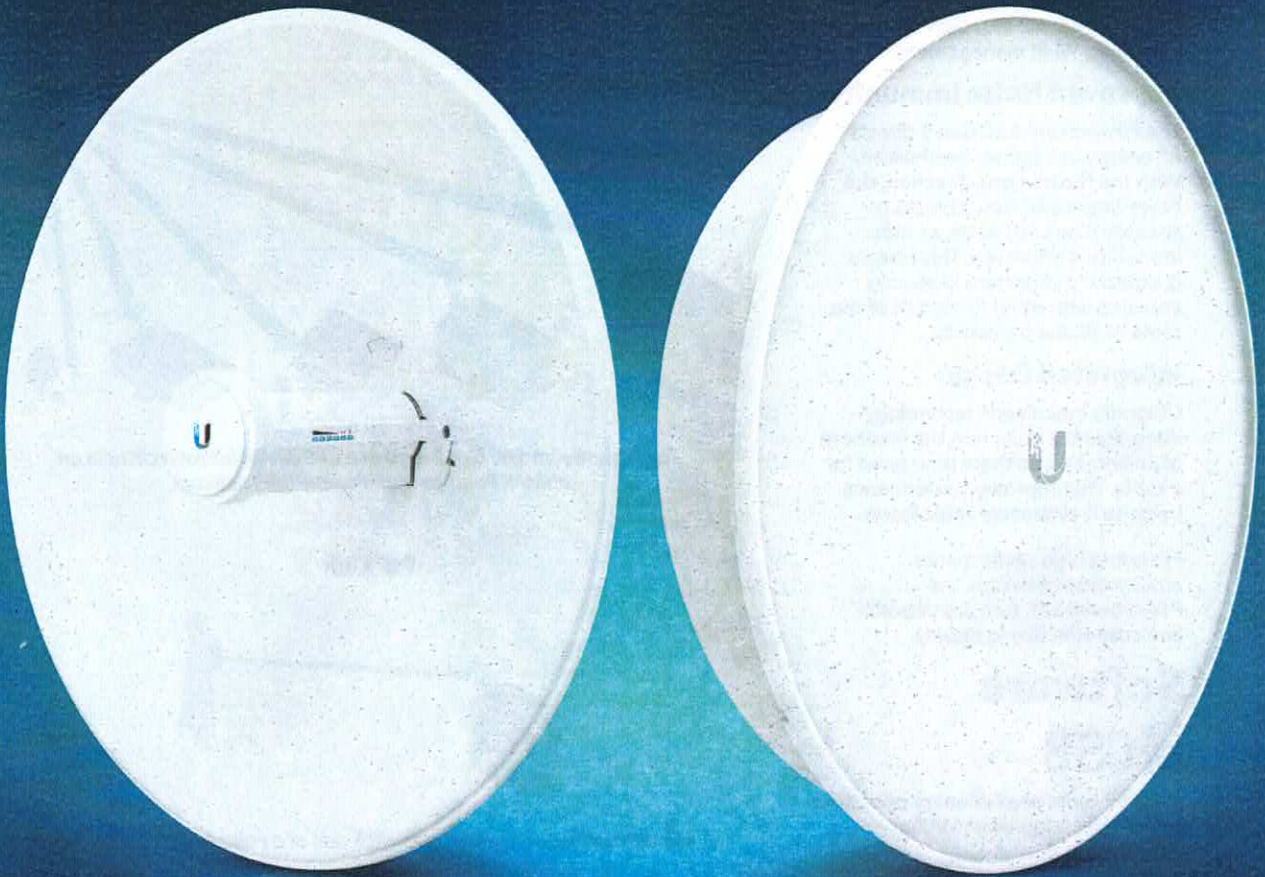
▪ Optional

DS-1475ZJ-SUS Vertical pole mount	DS-1476ZJ-SUS Corner mount	DS-1275ZJ-S-SUS Vertical pole mount	DS-1475ZJ-Y Vertical pole mount	DS-1476ZJ-Y Corner mount

Headquarters
 No.555 Qianma Road, Binjiang District,
 Hangzhou 310051, China
 T +86-571-8807-5998
 www.hikvision.com

Follow us on social media to get the latest product and solution information.





PowerBeam® AC GEN2

5 GHz High Performance airMAX® ac Bridge

Models: PBE-5AC-Gen2, PBE-5AC-ISO-Gen2

Highly Efficient Antenna Beam Performance

Up to 450+ Mbps Throughput

Dedicated Wi-Fi Radio for Management



Advanced RF Analytics

airMAX ac devices feature a multi-radio architecture to power a revolutionary RF analytics engine.

An independent processor on the PCBA powers a second, dedicated radio, which persistently analyzes the full 5 GHz spectrum and every received symbol to provide you with the most advanced RF analytics in the industry.

Real-Time Reporting

airOS 8 displays the following RF information:

- Persistent RF Error Vector Magnitude (EVM) constellation diagrams
- Signal, Noise, and Interference (SNI) diagrams
- Carrier to Interference-plus-Noise Ratio (CINR) histograms

Spectral Analysis

airView allows you to identify noise signatures and plan your networks to minimize noise interference. airView performs the following functions:

- Constantly monitors environmental noise
- Collects energy data points in real-time spectral views
- Helps optimize channel selection, network design, and wireless performance

In airView, there are three spectral views, each of which represents different data: waveform, waterfall, and ambient noise level.

airView provides powerful spectrum analyzer functionality, eliminating the need to rent or purchase additional equipment for conducting site surveys.

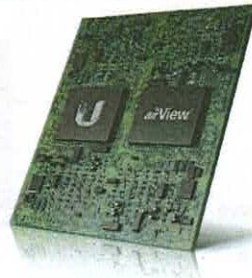
UNMS App

The PowerBeam 5AC Gen 2 integrates a separate Wi-Fi radio for fast and easy setup using your mobile device.

Accessing airOS via Wi-Fi

The UNMS™ app provides instant accessibility to the airOS configuration interface and can be downloaded from the App Store® (iOS) or Google Play™ (Android). UNMS allows you to set up, configure, and manage the PowerBeam 5AC Gen 2 and offers various configuration options once you're connected or logged in.

Multi-Radio Architecture



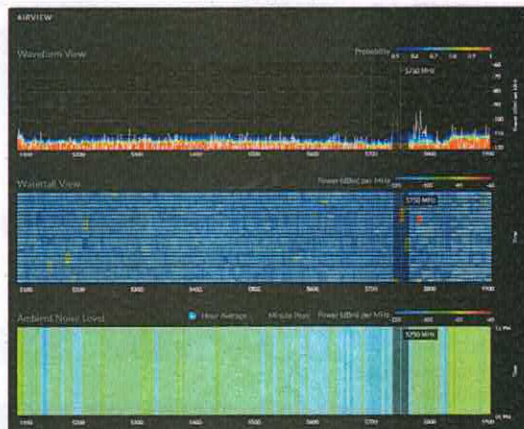
Constellation Diagrams



SNI Diagram and CINR Histogram



Dedicated Spectral Analysis



UNMS Configuration Screen



Handwritten blue ink signatures and scribbles.

Technology

airMAX ac

Unlike standard Wi-Fi protocol, Ubiquiti's Time Division Multiple Access (TDMA) airMAX protocol allows each client to send and receive data using pre-designated time slots scheduled by an intelligent AP controller.

This time slot method eliminates hidden node collisions and maximizes airtime efficiency, so airMAX technology provides performance improvements in latency, noise immunity, scalability, and throughput compared to other outdoor systems in its class.

Intelligent QoS Priority assigned to voice/video for seamless streaming.

Scalability High capacity and scalability.

Long Distance Capable of high-speed, carrier-class links.

Superior Performance

The next-generation airMAX ac technology boosts the advantages of our proprietary TDMA protocol.

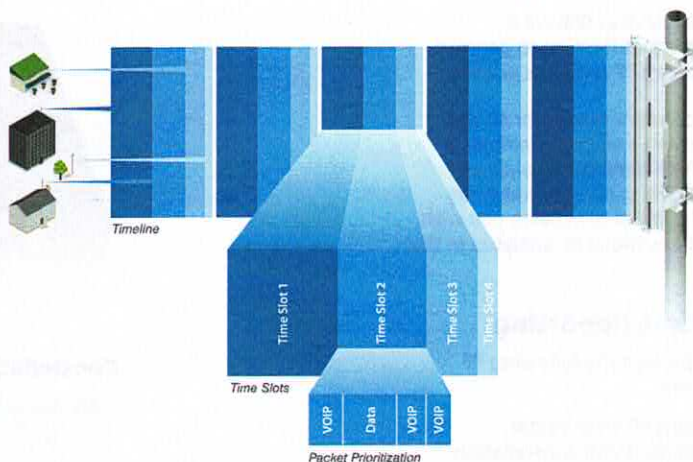
Ubiquiti's airMAX engine with custom IC dramatically improves TDMA latency and network scalability. The custom silicon provides hardware acceleration capabilities to the airMAX scheduler, to support the high data rates and dense modulation used in airMAX ac technology.

Throughput Breakthrough

airMAX ac supports high data rates, which require dense modulation: 256QAM – a significant increase from 64QAM, which is used in airMAX.

With their use of proprietary airMAX ac technology, airMAX ac products supports up to 450+ Mbps real TCP/IP throughput – up to triple the throughput of standard airMAX products.

airMAX ac TDMA Technology

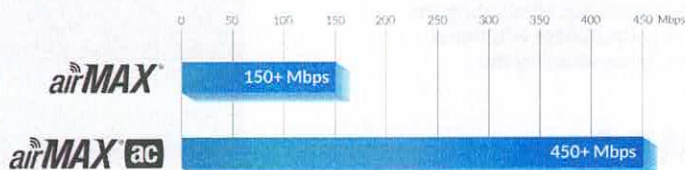


Up to 100 airMAX ac stations can be connected to an airMAX ac Sector; four airMAX ac stations are shown to illustrate the general concept.

airMAX Network Scalability



Superior Throughput Performance



Hardware Overview

The PowerBeam 5AC Gen 2 supports up to 450+ Mbps real TCP/IP throughput and features improved surge protection.

Innovative Mechanical Design

- **Built-in mechanical tilt** Mounting bracket conveniently offers elevation adjustments: $\pm 20^\circ$ tilt.
- **Quick assembly** Minimal fasteners simplify installation.
- **Easy removal** The antenna feed can be detached with the push of a button.

Industrial-Strength Construction

- **Fasteners** GEOMET-coated for improved corrosion resistance when compared with zinc-plated fasteners.
- **Dish and brackets** Made of galvanized steel that is powder-coated for superior corrosion resistance. The hardware also prevents paint from being removed from the metal brackets for improved corrosion resistance.
- **Optional support** In high-wind environments, you can enhance support with additional hardware (not included).

PBE-5AC-Gen2

The dish reflector design of the PBE-5AC-Gen2 makes it an ideal CPE for deployments requiring maximum performance. A protective radome is available as an optional accessory for the PBE-5AC-Gen2.

PowerBeam® 400 mm Radome

Model	Frequency	PBE-5AC-Gen2	Dish Reflector
PBE-RAD-400	5 GHz	✓	400 mm



PBE-5AC-ISO-Gen2

The PBE-5AC-ISO-Gen2 offers a rear housing with a metal-plated interior, designed to enhance RF shielding. Additionally, an included protective radome shields the PowerBeam 5AC ISO Gen 2 from nature's harshest elements.

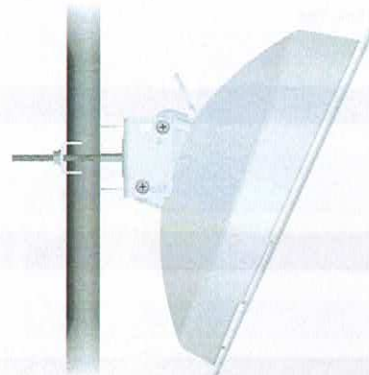
Breakthrough RF Isolation

The integrated isolator design spatially filters out interference, so the PBE-5AC-ISO-Gen2 delivers improved noise immunity in co-location deployments.

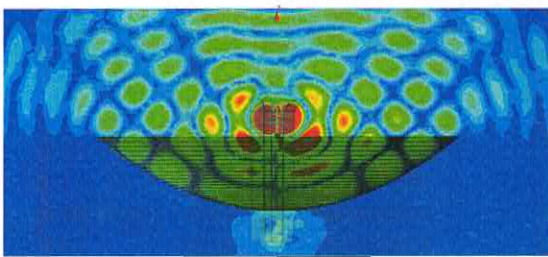
Compare the two near-field plots below, and note the superior performance of the integrated RF isolator.

Both near-field plots are displayed in watts and use a linear scale. The strength of the electromagnetic field is color-coded:

- **Red:** Highest strength
- **Green:** Medium strength
- **Indigo:** Lowest strength



Without Integrated RF Isolator



With Integrated RF Isolator



028
Specifications

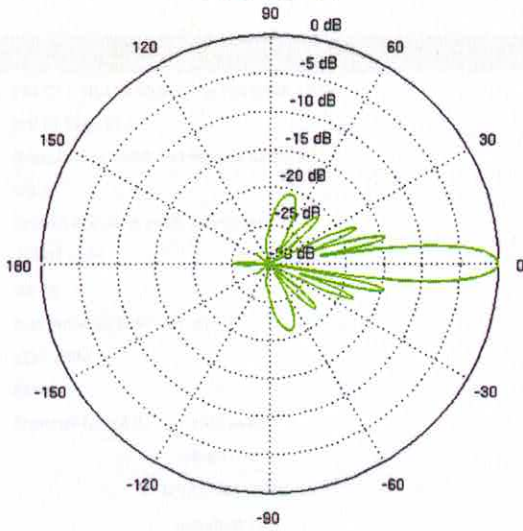
PBE-5AC-Gen2		
Dimensions	420 x 420 x 230 mm (16.54 x 16.54 x 9.06")	
Weight	2.22 kg (4.89 lbs)	
Power Supply	24V, 0.5A Gigabit PoE Adapter (Included)	
Max. Power Consumption	8.5W	
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)	
Supported Voltage Range	20 to 26VDC	
Gain	25 dBi	
Networking Interface	(1) 10/100/1000 Ethernet Port	
Processor Specs	MIPS 74Kc	
Memory	64 MB	
LEDs	Power, Ethernet, (4) Signal Strength	
Channel Sizes	PtP Mode	PtMP Mode
	10/20/30/40/50/60/80 MHz	10/20/30/40 MHz
Enclosure Characteristics	Antenna Feed	Dish Reflector
	Outdoor UV Stabilized Plastic	Powder-Coated SPCC
Mounting	Pole-Mounting Kit (Included)	
Wind Loading	380 N @ 200 km/h (85.4 lbf @ 125 mph)	
Wind Survivability	200 km/h (125 mph)	
ESD/EMP Protection	Air: ± 24 kV, Contact: ± 24 kV	
Operating Temperature	-40 to 70° C (-40 to 158° F)	
Operating Humidity	5 to 95% Noncondensing	
RoHS Compliance	Yes	
Salt Fog Test	IEC 68-2-11 (ASTM B117), Equivalent: MIL-STD-810 G Method 509.5	
Vibration Test	IEC 68-2-6	
Temperature Shock Test	IEC 68-2-14	
UV Test	IEC 68-2-5 at 40° C (104° F), Equivalent: ETS 300 019-1-4	
Wind-Driven Rain Test	ETS 300 019-1-4, Equivalent: MIL-STD-810 G Method 506.5	
Certifications	CE, FCC, IC	

Operating Frequency (MHz)				
Worldwide	5150 - 5875			
USA	U-NII-1: 5150 - 5250	U-NII-2A: 5250 - 5350 MHz	U-NII-2C: 5470 - 5725 MHz	U-NII-3: 5725 - 5850

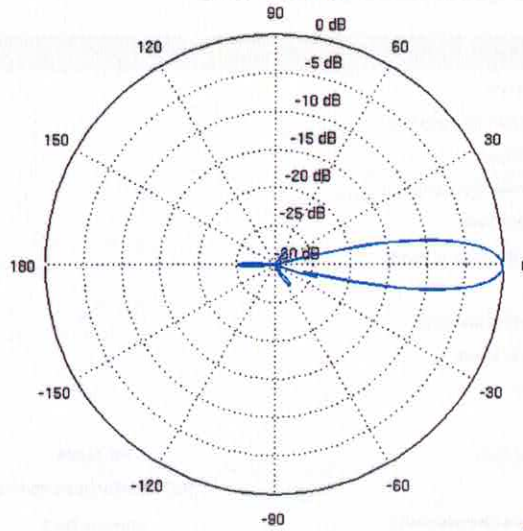
Management Radio (MHz)	
Worldwide	2412 - 2472
USA	2412 - 2462

PBE-5AC-Gen2 Output Power: 24 dBm							
TX Power Specifications				RX Power Specifications			
Modulation	Data Rate	Avg. TX	Tolerance	Modulation	Data Rate	Sensitivity	Tolerance
airMAX ac	1x BPSK (½)	24 dBm	± 2 dB	airMAX ac	1x BPSK (½)	-96 dBm Min.	± 2 dB
	2x QPSK (½)	24 dBm	± 2 dB		2x QPSK (½)	-95 dBm	± 2 dB
	2x QPSK (¾)	24 dBm	± 2 dB		2x QPSK (¾)	-92 dBm	± 2 dB
	4x 16QAM (½)	24 dBm	± 2 dB		4x 16QAM (½)	-90 dBm	± 2 dB
	4x 16QAM (¾)	24 dBm	± 2 dB		4x 16QAM (¾)	-86 dBm	± 2 dB
	6x 64QAM (¾)	22 dBm	± 2 dB		6x 64QAM (¾)	-83 dBm	± 2 dB
	6x 64QAM (¾)	21 dBm	± 2 dB		6x 64QAM (¾)	-77 dBm	± 2 dB
	6x 64QAM (¾)	21 dBm	± 2 dB		6x 64QAM (¾)	-74 dBm	± 2 dB
	8x 256QAM (¾)	20 dBm	± 2 dB		8x 256QAM (¾)	-69 dBm	± 2 dB
	8x 256QAM (¾)	20 dBm	± 2 dB		8x 256QAM (¾)	-65 dBm	± 2 dB

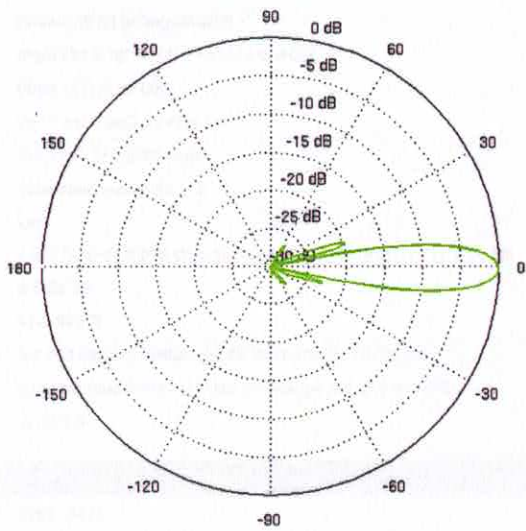
Vertical Azimuth



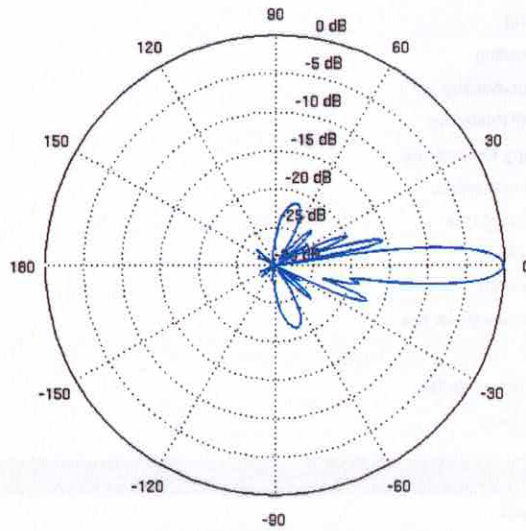
Vertical Elevation



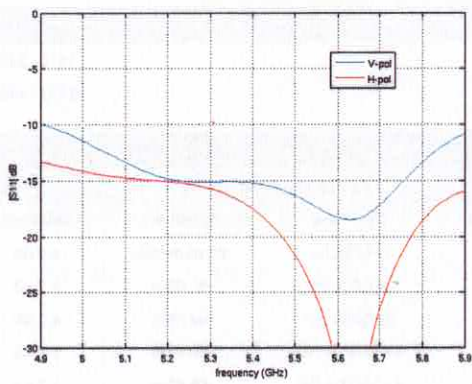
Horizontal Azimuth



Horizontal Elevation



Return Loss



Specifications

030

PBE-5AC-ISO-Gen2		
Dimensions	459 x 459 x 261 mm (18.07 x 18.07 x 10.28")	
Weight (Mount Included)	3.22 kg (7.10 lbs)	
Power Supply	24V, 0.5A Gigabit PoE Adapter (Included)	
Max. Power Consumption	8.5W	
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)	
Supported Voltage Range	20 to 26VDC	
Gain	25 dBi	
Networking Interface	(1) 10/100/1000 Ethernet Port	
Processor Specs	MIPS 74Kc	
Memory	64 MB	
LEDs	Power, Ethernet, (4) Signal Strength	
Channel Sizes	PtP Mode	PtMP Mode
	10/20/30/40/50/60/80 MHz	10/20/30/40 MHz
Enclosure Characteristics	Antenna Feed	Dish Reflector
	Outdoor UV Stabilized Plastic	Powder-Coated SPCC
Mounting	Pole-Mounting Kit (Included)	
Wind Loading	559 N @ 200 km/h (125.7 lbf @ 125 mph)	
Wind Survivability	200 km/h (125 mph)	
ESD/EMP Protection	Air: ± 24 kV, Contact: ± 24 kV	
Operating Temperature	-40 to 70° C (-40 to 158° F)	
Operating Humidity	5 to 95% Noncondensing	
RoHS Compliance	Yes	
Salt Fog Test	IEC 68-2-11 (ASTM B117), Equivalent: MIL-STD-810 G Method 509.5	
Vibration Test	IEC 68-2-6	
Temperature Shock Test	IEC 68-2-14	
UV Test	IEC 68-2-5 at 40° C (104° F), Equivalent: ETS 300 019-1-4	
Wind-Driven Rain Test	ETS 300 019-1-4, Equivalent: MIL-STD-810 G Method 506.5	
Certifications	CE, FCC, IC	

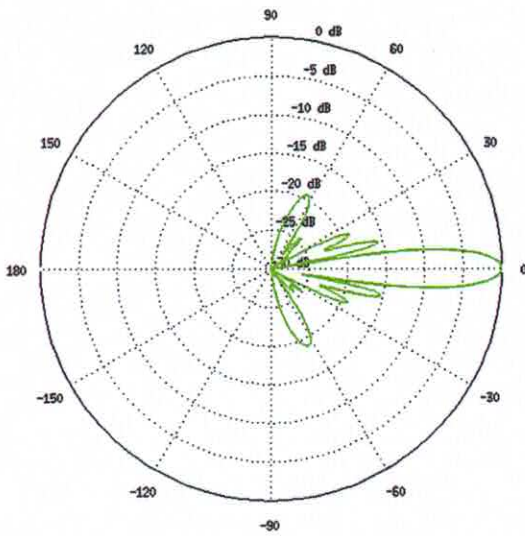
Operating Frequency (MHz)				
Worldwide	5150 - 5875			
USA	U-NII-1: 5150 - 5250	U-NII-2A: 5250 - 5350 MHz	U-NII-2C: 5470 - 5725 MHz	U-NII-3: 5725 - 5850

Management Radio (MHz)	
Worldwide	2412 - 2472
USA	2412 - 2462

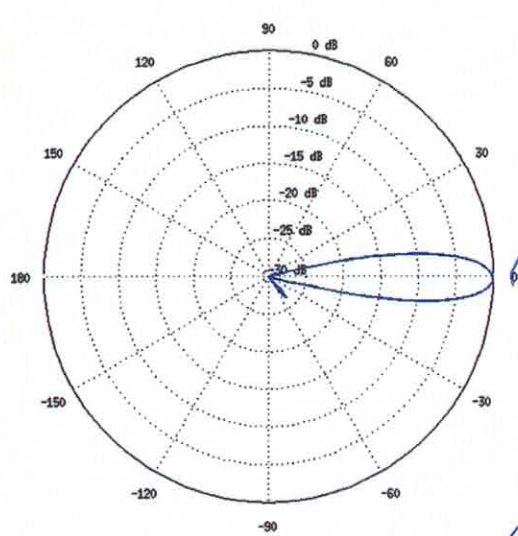
PBE-5AC-ISO-Gen2 Output Power: 24 dBm							
TX Power Specifications				RX Power Specifications			
Modulation	Data Rate	Avg. TX	Tolerance	Modulation	Data Rate	Sensitivity	Tolerance
airMAX ac	1x BPSK (1/2)	24 dBm	± 2 dB	airMAX ac	1x BPSK (1/2)	-96 dBm Min.	± 2 dB
	2x QPSK (1/2)	24 dBm	± 2 dB		2x QPSK (1/2)	-95 dBm	± 2 dB
	2x QPSK (3/4)	24 dBm	± 2 dB		2x QPSK (3/4)	-92 dBm	± 2 dB
	4x 16QAM (1/2)	24 dBm	± 2 dB		4x 16QAM (1/2)	-90 dBm	± 2 dB
	4x 16QAM (3/4)	24 dBm	± 2 dB		4x 16QAM (3/4)	-86 dBm	± 2 dB
	6x 64QAM (2/3)	23 dBm	± 2 dB		6x 64QAM (2/3)	-83 dBm	± 2 dB
	6x 64QAM (3/4)	23 dBm	± 2 dB		6x 64QAM (3/4)	-77 dBm	± 2 dB
	6x 64QAM (5/6)	22 dBm	± 2 dB		6x 64QAM (5/6)	-74 dBm	± 2 dB
	8x 256QAM (3/4)	20 dBm	± 2 dB		8x 256QAM (3/4)	-69 dBm	± 2 dB
	8x 256QAM (5/6)	20 dBm	± 2 dB		8x 256QAM (5/6)	-65 dBm	± 2 dB

[Handwritten signatures and scribbles]

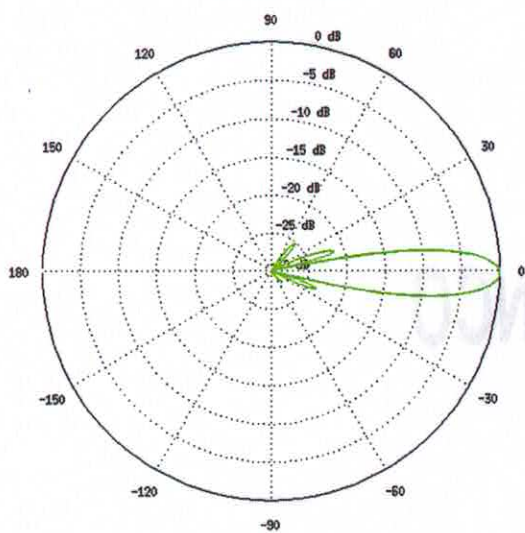
Vertical Azimuth



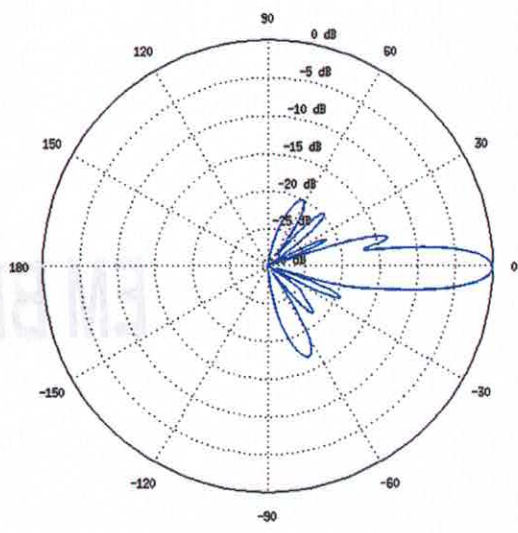
Vertical Elevation



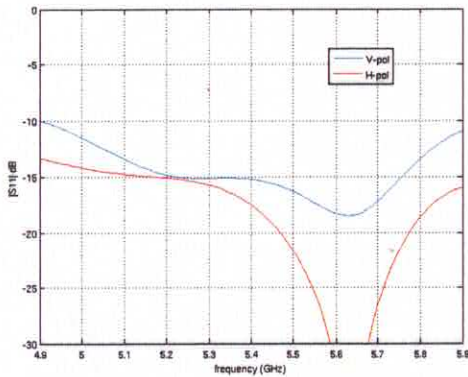
Horizontal Azimuth



Horizontal Elevation



Return Loss



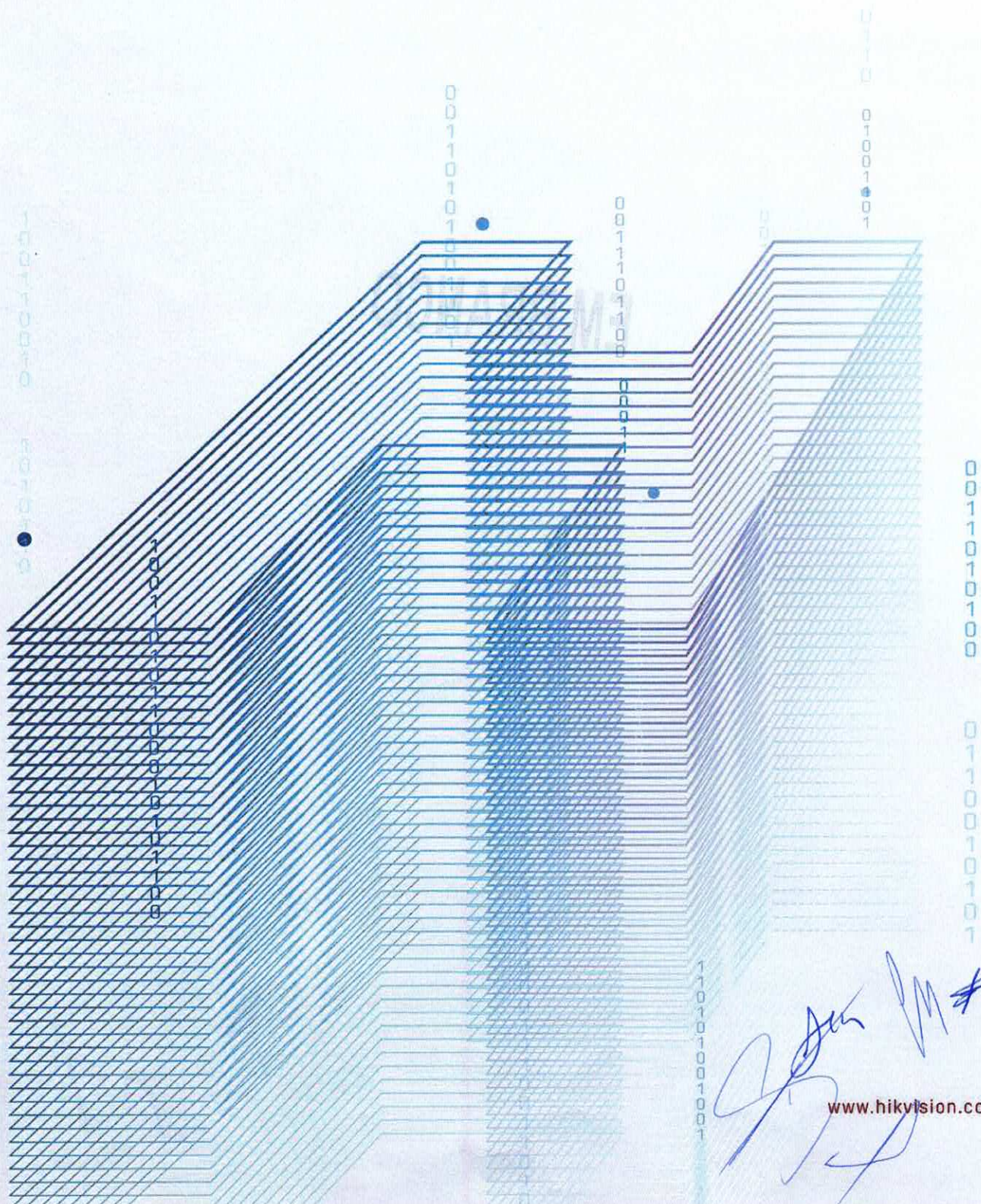
Specifications are subject to change. Ubiquiti products are sold with a limited warranty described at: www.ubnt.com/support/warranty
 ©2016-2019 Ubiquiti Networks, Inc. All rights reserved. Ubiquiti, Ubiquiti Networks, the Ubiquiti U logo, the Ubiquiti beam logo, airMagic, airMAX, airOS, airView, InnerFeed, PowerBeam, and UNMS are trademarks or registered trademarks of Ubiquiti Networks, Inc. in the United States and in other countries. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc., registered in the U.S. and other countries. Android, Google, Google Play, the Google Play logo and other marks are trademarks of Google Inc. All other trademarks are the property of their respective owners.



Handwritten signatures and initials in blue ink at the bottom of the page.



HIKVISION Cybersecurity White Paper



Handwritten signatures and initials in blue ink.

About this Documentation

Offering an overview of our current practice on product cybersecurity, Hikvision Cybersecurity White Paper provides users with the company's cybersecurity capabilities in an open and transparent manner.

Hikvision reserves rights to update this Documentation. Please kindly find the latest version on the company website (<http://www.hikvision.com/en/>).

Copyright Disclaimer

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. ALL RIGHTS RESERVED.

This Documentation shall not be reproduced, translated, modified, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks Acknowledgement

海康威视, HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer


TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CONTENT DESCRIBED IN THIS DOCUMENTATION IS PROVIDED "AS IS", AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, FITNESS FOR COMMERCIAL USE OR A PARTICULAR PURPOSE.

HIKVISION PROVIDES NO WARRANTY ON THE ACCURACY OF THIS DOCUMENTATION CONTENT, AND RESERVES RIGHTS TO CORRECT OR MODIFY THE CONTENT WITHOUT FURTHER NOTICE. ANY DECISIONS RELIED ON OR BY THE USE OF THIS DOCUMENTATION TOGETHER WITH ANY CONSEQUENCES THAT IT MAY CAUSE SHALL BE UNDER YOUR OWN RESPONSIBILITY.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Revision Record

First published in January 2018 and revised in September 2023.



Company Introduction

Founded in 2001, Hikvision is a technology company focusing on technological innovation.

We adhere to the business philosophy of "Professionalism, Reliability, and Integrity," and fulfill the company's core values: dedicated to customers' continual success, adding value to companies and communities, acting with honesty and integrity, pursuing excellence in every endeavor. Hikvision is committed to serving various industries through its cutting-edge technologies of machine perception, artificial intelligence, and big data, leading the future of AIoT:

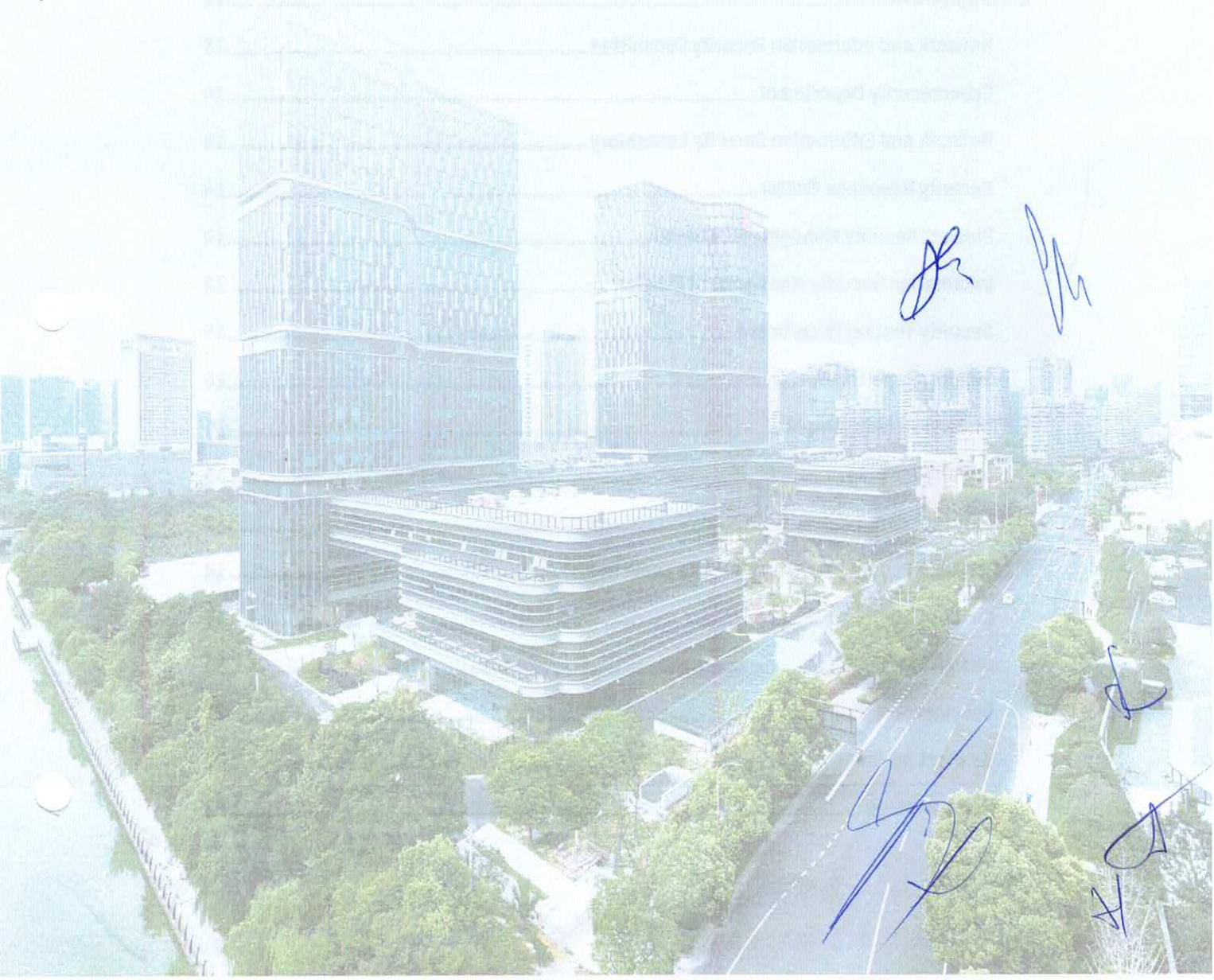
- Through comprehensive machine perception technologies, we aim to help people better connect with the world around them.
- With a wealth of intelligent products, we strive to identify diverse demands by delivering intelligence at your fingertips.
- Through innovative AIoT applications, we are dedicated to empowering every individual to enjoy a better future by building an intelligent world that is more convenient, efficient, and secure.

More than 20 years ago, Hikvision began with video technology and has continued to expand and deploy visible light, millimeter wave, infrared, X-ray, sound wave, and other technologies, creating a comprehensive and multi-dimensional IoT perception technology platform. Beyond IoT perception equipment, Hikvision has five categories of software and hardware products including AIoT products that fully integrate with artificial intelligence and big data technologies, basic IT products, platform service products, data service products, and application service products. Hikvision has also expanded into integrated security to smart homes, digital enterprises, smart industries, and smart cities.

Hikvision currently has 58,284 employees (as of the end of 2022), including more than 27,951 R&D personnel and technical service personnel. R&D investment accounts for 11.80% of the annual operating income (2022), making the Company a leader in the industry. The company has R&D centers worldwide, including in Montreal, London, and Dubai, and various Chinese

cities. Hikvision has a global presence with 72 overseas subsidiaries and branch offices, serving clients in more than 150 countries and regions (2022).

Hikvision went public in May 2010, and is listed on the SME Board at Shenzhen Stock Exchange, stock code: 002415.



CONTENTS

About this Documentation	I
Company Introduction	II
1. A letter from the President	1
2. Preface.....	3
3. Security Threats in the Internet of Things.....	5
Perception-layer threats	5
Transport-layer threats.....	6
Application-layer threats.....	7
4. Network and Information Security in the Security Industry.....	9
5. Hikvision Security Research and Development Maturity Model HSDMM.....	12
6. Security Governance.....	13
6.1 Organization.....	13
Network and Information Security Committee	13
Cybersecurity Department	14
Network and Information Security Laboratory	14
Security Response Center.....	14
Product Security Management Division.....	14
Information Security Management Division	15
Security Testing Department	15
Support Departments	15
6.2 Personnel Management	15
6.3 Security Training.....	16
7. Security Process	18
7.1 Hikvision Security Development Life Cycle HSDLCL	18
Concept Stage.....	18
Design Stage	19
Development Stage	21
Verification Stage	21
Release Stage	22

Maintenance Stage.....	22
7.2 Data Life Cycle Security Management.....	26
8. Security Technology	29
8.1 Configuration Management	29
8.2 Security Certification.....	33
Supply Chain Security.....	34
Common Criteria / ISO 15408.....	35
ISO/IEC 27001	36
ISO/IEC 27701	36
ISO/IEC 29151	36
CMMI5 Software Maturity Certification.....	37
Information Security Level Protection Certification	37
CSA STAR Certification	37
GDPR.....	38
8.3 Product Security Research and Collaboration	38
Security Engine	40
Security Situational Awareness.....	41
Vulnerability Assessment.....	42
Security Visualization	42
Honeypot	43
Digital Watermark	44
Exchange and Collaborations	45
9. Security Commitment.....	47

HIKVISION

Handwritten signatures and initials in blue ink, including a large signature, a checkmark, and various initials like 'v', 'P', and '4'.

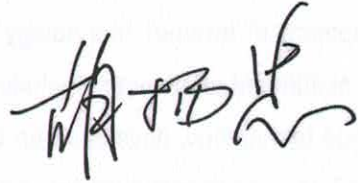
1. A letter from the President

The "Internet of Everything" is being translated from dreams to reality. As a forerunner to the "Internet of Everything", video security technology has developed rapidly over the past 10 years. Evolving from analog, to digital, to the network era, it is now entering the intelligent era. Improvements in technology advance human society, but also present new challenges. The development of Internet technology has greatly benefited human society, but it has also posed significant challenges, including those related to cybersecurity. Similarly, the Internet of Things technology, developed on the foundation of the internet, will enhance human life while introducing new challenges, with cybersecurity being one of them.

Compared to the IT industry, the security industry has not been in the digital era for as long, with relatively less know-how of cybersecurity industrywide. In 2014, following international practice, the company established the "Hikvision Security Response Center" (HSRC), to form a centralized platform for addressing cybersecurity issues. In 2015, Hikvision established the "Network and Information Security Laboratory", greatly enhancing the corporate cybersecurity efforts. The lab, together with the subsequent Network and Information Security Committee and the Cybersecurity Department, facilitated the company's efforts to improve the cybersecurity system centered around organization and processes. Cybersecurity design stood out as a special enabler to the overall cybersecurity integrity of the company's products and systems. We understand that cybersecurity is not solely the responsibility of product manufacturers. Every stakeholder in a project, including users, integrators, operators, engineering designers, other service providers, and government entities, bears the responsibility throughout the project's entire lifecycle. All parties involved are confronted with the challenges of cybersecurity, the successful handling of which could be attributed to 30% of technological competence and 70% of managerial expertise. Collective efforts are needed from all vested parties and never should anyone take cybersecurity for granted.

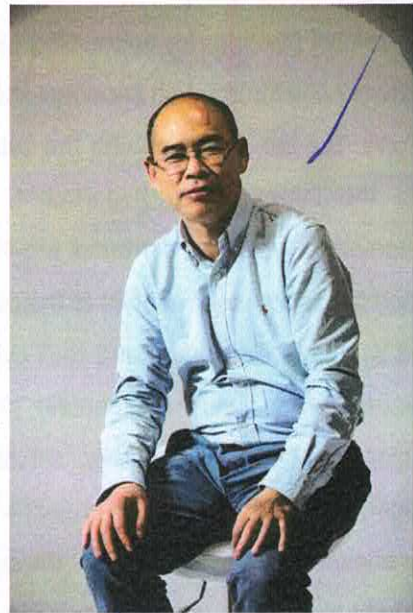
Confronted with the urgent need for collective efforts to address the common challenges, we are fully aware of the keen public and media attention and concerns over the security of the Internet of Things (IoT), which further underscore the responsibility and mission we carry. Always committed to the corporate values of "being dedicated to customers' continual success, adding value to companies and communities, acting with honesty and integrity, pursuing excellence in every endeavor", we pledge to prioritize the network and business security of our customers over the company's interests.

The challenges of cybersecurity will persist, and we are committed to continuing our efforts for the best solutions.



Hu Yangzhong, President

Hangzhou Hikvision Digital Technology Co., Ltd.



2. Preface

The past several years have witnessed the progression of digitalization and the rapid development in the security industry. In these years, we have seen how the intelligent security industry explores the dream of the Internet of Things and we are happy to see that the industry is at the forefront of developing, exploring and implementing IoT technology.

Without a doubt, the development of the intelligent security industry must follow the trends of digitalization, networking, and intelligence. However, cybersecurity is a completely new field for the security industry and the openness of networks has interconnected security systems which were once independent and completely isolated, promoting data flow and sharing in ways that have drastically benefited society. This has brought about more innovative opportunities, enabled the Internet of Things industry to grow, and pushed the human progress to new heights.

During the industry's transformation from "analog", "isolated", and "data acquisition", to "digital", "networked", and "image intelligence", we have seen the benefits that the digital and networking revolution brings. However, we have also witnessed the spread of various types of malicious cybersecurity attacks from the Internet to the security industry. Furthermore, since the current security systems are based on "seamless" switching from original ones, some of the industry's inherent features may develop into possible security defects when placed in the cyberspace.

As a global company, Hikvision operates in more than 150 countries and regions. As a company of such a scale, Hikvision is actively responding to these challenges. Hikvision deeply understands, from a technological perspective, how intelligent security systems operate safely and effectively, and how technology fundamentally supports and promotes the health, prosperity, and security of the global citizens.

Cybersecurity is not just a problem for certain countries or companies. All stakeholders, governments, and industries must understand that cybersecurity is a problem that everyone in the world faces, and that meeting these challenges requires international cooperation in employing the risk-oriented methods and best practices. To effectively handle security issues, various stakeholders must form mechanisms of trust and cooperation.

Hikvision makes the following commitments: We will support and adhere to internationally recognized cybersecurity standards and the best practices; we will support research efforts

000

to increase network defense capabilities; we will continue to improve and use open and transparent methods so that users can assess Hikvision's cybersecurity capabilities.

Finally, just as we did in the past, we encourage our clients to help us improve the procedures, technology, and cybersecurity techniques to create even more benefits to them and their customers.

A collection of handwritten signatures and initials in blue ink, including a large signature at the top, a smaller signature below it, and several initials at the bottom right.

3. Security Threats in the Internet of Things

The Internet of Things (IoT) connects "smart devices" from all over the world through the Internet and allows for the interaction between people and things on a global scale. The interconnection of a massive number of devices has made networks more open, complex and diversified. However, the advent of IoT also brings incredible security challenges.



Figure 3-1 Characteristics of IoT

In addition to the traditional cybersecurity threats, there are still some special security issues in the IoT, because it is composed of a large number of unattended devices or perceptive nodes without effective monitoring, exacerbated by large numbers and huge concentrations. Based on the IoT framework, security threats in the IoT can be categorized as perception-layer threats, transport-layer threats, and application-layer threats.

Perception-layer threats

➤ Physical attack

IoT assets that are deployed remotely without physical protection are susceptible to theft or damage.

Outdoor devices are sometimes easily accessible, and not well managed, leading to physical attacks, tampering, and counterfeiting.

➤ Data leakage

Sensitive information leakage is caused by the lack of encryption or access control during data collection and processing by IoT devices.

➤ Unauthorized access

Lack of authentication requirements, weak passwords, or easily bypassed authentication mechanism leave some IoT devices susceptible to potential attacks and compromises.

Some IoT devices leave a debug interface, which could allow an attacker to obtain device operation information.

➤ Unauthorized update

Some IoT devices do not use a robust update verification mechanism, which could allow unofficial firmware packages that may contain vulnerabilities or malware to be installed into the devices.

➤ Expired components

IoT devices come with built-in components with known vulnerabilities or expired components.

➤ Malicious software

Malicious software may contain malicious code or viruses, which can be used to obtain device information and system files, or affect the normal operation of the device.

Transport-layer threats

➤ Cyberattack

Exploiting protocol vulnerabilities, such as lack of effective authentication, may lead to leaks on the access side.

➤ Man-in-the-Middle Attacks

Attackers intercept communication between IoT devices and manipulate data or commands exchanged, leading to unauthorized access or control over these devices.

➤ Denial-of-Service Attacks

Floods of data requests or commands can overwhelm IoT devices, rendering them unresponsive or causing malfunctions, disrupting regular operations.

➤ Data leakage

During communication between IoT devices, cloud hosting servers, and mobile devices, attackers can access sensitive data by monitoring the transmission channel.

➤ Data tampering

When a device communicates over a network, commands and data may be intercepted and altered by attackers if the transmission data is not checked for integrity.

Application-layer threats

➤ Device management

There are challenges in managing the update process and the security of the numerous devices managed by the Application-layer.

➤ Unauthorized access

Imperfect authorization (rights) management at the application layer may lead to unauthorized access and the risk of data leakage.

➤ Insecure APIs and Interfaces

Weaknesses in application programming interfaces (APIs) and communication interfaces can be exploited to manipulate device functionalities or steal data.

➤ System vulnerabilities

IoT device application software or operating system software has logical defects or errors in design, which can be exploited by attackers to control the entire device through network implantation of Trojan horses, viruses, and other methods, resulting in abnormal device operation.

➤ Data leakage

The application layer manages a large volume of data, which is prone to leakage if not encrypted or access control not properly managed.

➤ Outdated components

The application layer uses components with known vulnerabilities or expired components. If the components are not updated in a timely manner, the inherent vulnerabilities of the components can be easily exploited.

➤ Configuration vulnerabilities

In the security configuration for applications, frameworks, containers and operating systems, security vulnerabilities caused by unreasonable or improper configuration, such as using versions with security flaws, granting excessive permissions to certain accounts, and failing to control access to sensitive resources may allow attackers to access certain system data or use system functions without authorization.

After investigating the numerous hidden security risks in the IoT environment, as well as the complexities of computational capabilities and the complex hardware and software environment, Hikvision developed the video-centric IoT security solutions that promise to create a brand new security architecture, establish a multi-dimensional security system, and guarantee terminal security, data security, application security, network security, personal data protection, and security compliance.

4. Network and Information Security in the Security Industry

The development of the security industry has gone through an initial analog phase followed by a digital phase. During the analog era, security systems operated within private networks, so the industry focused more on product cost, performance, and ease of use. Due to the characteristics of systems at that time, security was not a primary concern. However, with the rapid adoption of network connectivity, the security industry transitioned directly from analog to IP digital technology. During this transition, security issues didn't get much attention. Consequently, user-friendly designs that were advantageous in the analog era didn't keep up with best practices in information security in the digital era. Security manufacturers often default to enabling all supported protocols to facilitate users in integrating devices from multiple manufacturers with a single click. The server automatically connects using whichever protocol that is supported. Although such a design is very easy to use for customers, it compromises best practices in information security.

It is precisely due to this evolution of the security industry that certain information security issues have arisen in recent years. However, the emergence of these issues does not necessarily mean that the entire industry is as vulnerable as some portray it to be. Hikvision has recognized both existing and potential security risks. Substantial and effective efforts have already been undertaken to address these challenges.

Objectively speaking, cybersecurity issues are not exclusive to the security industry. They represent a challenge faced collectively by human society today. Given the entire IT landscape, cybersecurity challenges are present in all domains, and several fundamental consensuses exist:

➤ The Common Occurrence of Security Vulnerabilities

There is no such thing as an IT system or product with no security vulnerabilities. In fact, security vulnerabilities are very common. There are millions of lines of code in each product, and if only one parameter is incorrectly set, or if the positioning of two lines of code is incorrect, this may lead to a high-risk vulnerability in a system. Currently, automated or manual techniques cannot be used to detect all potential cybersecurity issues. Therefore, product security issues are common across all manufacturers.

➤ Security for the Entire System

The security of any system cannot be guaranteed solely by a single point; it must encompass the entire system. To ensure the security of a video security system, collaboration and supplementation among various components are necessary. This includes front-end and back-end devices, platform systems, network equipment, security devices, and more. By establishing a multi-layered defense system, or "defense in depth", the overall system's security can be ensured. Any problems in any part of the system can potentially lead to a system breach but if implemented correctly, attackers must get past the many layers of security to achieve their goal.

➤ Security of Third-Party Open Source Software

Currently, various third-party open-source software is widely utilized in different systems. These software solutions come with attributes like openness, sharing, and freedom, and they play an increasingly crucial role in software development. They are also a significant part of the software supply chain. While businesses benefit from the convenience provided by open-source software, they also assume substantial security risks. In recent years, open-source software has frequently revealed high-risk vulnerabilities, such as Struts2 and OpenSSL. Many of these components are deeply integrated into the underlying infrastructure of information systems and are used extensively. As a result, the security risks posed by these vulnerabilities are far-reaching, often evolving into "generic" vulnerabilities that can potentially impact entire industry sectors or a company's product lines.

➤ Security in Dynamic Balance

There is no such thing as "absolute" security; security is always relative. The perpetual game of offense and defense is a dynamic balance, where gains made on one side can be countered by advancements on the other. Mechanisms and methods deemed secure today might be vulnerable tomorrow. Likewise, products considered "secure" today might be compromised tomorrow. As a result, security is an ongoing process with no definitive endpoint. Throughout the lifecycle of any product, information security challenges and risks persist. The uncertainty lies in whether these risks will materialize and when they might arise, making it difficult to predict in advance.

➤ Product Security Management

The most important element in system security is security management. Even with systems that are more secure, if the user cannot manage or operate them properly then system security cannot be maintained. Currently, some security issues within the security industry are caused by "inappropriate" usage of users and ineffective security management. Some cybersecurity devices still have "weak" passwords and some security systems do not have firewalls or other security equipment installed. Users also need to develop good security habits, take regular note of security announcements from manufacturers, update firmware to the latest version and install patches as soon as possible.

[Handwritten signature]

[Handwritten signature]

[Large handwritten signature]

[Handwritten mark]

[Handwritten mark]

[Handwritten mark]

5. Hikvision Security Development Maturity Model

With our extensive research and development efforts, and drawing on industry best security practices such as OpenSAMM, BSIMM, CSDL, MSDL, and customer feedback, we have established the Hikvision Security Development Maturity Model (HSDMM). Quantifying the security activities in product security development, this model integrates a comprehensive organizational structure, well-defined security development management processes, and robust technical measures to ensure the effective implementation of security activities. This, in turn, enhances product confidentiality, integrity, and availability, while strengthening personal data protection, ultimately providing customers with safer products and solutions. In subsequent section of the paper, we will walk you through the HSDMM across security governance, security processes, and security technologies.

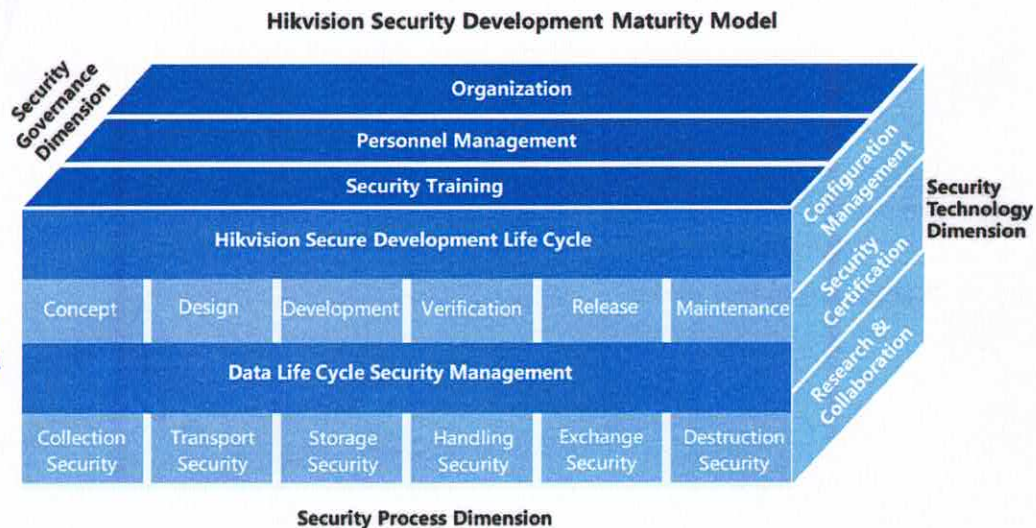


Figure 5-1 Hikvision Security Development Maturity Model

6. Security Governance

6.1 Organization

To ensure that product security is incorporated into every aspect of Hikvision product the development, supply chain, marketing and sales, delivery, technical service and other processes, we first need to establish an organizational structure that can guarantee its implementation and assign clear responsibilities to each group. The security administrative structure of Hikvision is as follows:

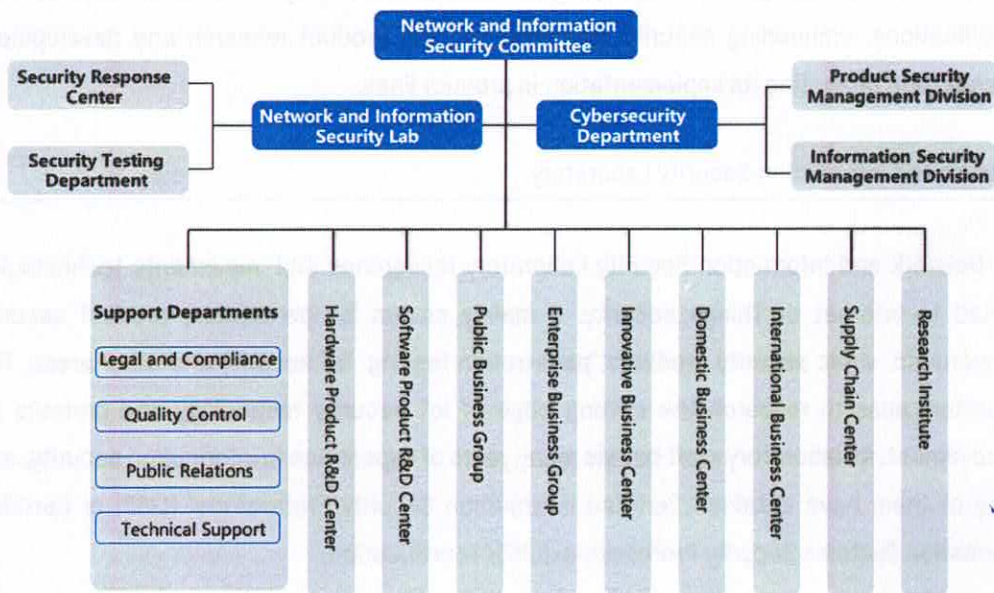


Figure 6-1 Hikvision Security Organization Structure

Network and Information Security Committee

Hikvision's Network and Information Security Committee is responsible for strategic planning and policy making for network and information security. If any conflict or serious issue arises, the committee has the authority to make decisions and make necessary adjustments to services. Hikvision President, Mr. Hu Yangzhong, acts as the head of the committee, which has set up a specialized Cybersecurity Department to formulate network and information security strategies, policies, procedures, and standards, and to manage resource allocation on a daily basis.

Cybersecurity Department

As a standing body of the Network and Information Security Committee, the Cybersecurity Department is responsible for implementing the product security strategies, establishing the product security baselines, and conducting product security assessments. The Department also promotes external collaborations related to product security, conducts research into product security technical standards of the industry, advances product security research and development, participates in major project reviews of product security, and provides recommendations for leadership decisions. It is also responsible for aligning the company's product security strategy with industry requirements, establishing research and development specifications, embedding security elements into the product research and development process, and promoting its implementation in product lines.

Network and Information Security Laboratory

The Network and Information Security Laboratory researches and implements technologies related to Internet of Things security. It mainly covers IoT perception, product security components, video security products, penetration testing, IoT security and other areas. The laboratory aims to research the cutting-edge of IoT security technology and promote its improvement. All laboratory staff boasts many years of experience in information security, and many of them have obtained Certified Information Security Professional (CISP) or Certified Information Systems Security Professional (CISSP) certification.

Security Response Center

The Hikvision Security Response Center is responsible for receiving, addressing, and disclosing Hikvision product and solution security vulnerabilities. Hikvision is a member of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the Security Emergency Service Support Organization of the Industrial Information Security Industry Development Alliance. It shares best practices and experience in security emergencies with other excellent members worldwide, enhances reliable communication and cooperation, and enhances the effectiveness and timeliness of the company's response to security incidents.

Product Security Management Division

Each Hikvision product line has a product security division, which works with the Cybersecurity Department to establish product security baselines and related product technical standards

and is responsible for the implementation of processes such as product planning, R&D, and testing on the product line, and is responsible for the security of the product line.

Information Security Management Division

The Information Security Management division is responsible for assisting the Cybersecurity Department in implementing information security policies, procedures, standards, and processes within the company. They also assist in conducting information security monitoring, auditing, training, and awareness activities. Additionally, they are responsible for handling internal security incidents.

Security Testing Department

The Security Testing Department is a third-party body independent of the product lines and is responsible for the product security testing for all of Hikvision's product lines. This department inspects the company's product security policies, and assesses the implementation of security baselines in products. It is also responsible for ensuring that the released products are secure, and for preventing various types of security issues that may arise during the research and development process.

Support Departments

The Support Departments are responsible for providing related internal control, laws and regulations, brand promotion, auditing, and PR support for matters related to product security.

6.2 Personnel Management

In terms of cybersecurity awareness education for all employees, Hikvision intends to build a company-wide security awareness education and cultural atmosphere. In order to achieve this, Hikvision provides cybersecurity training for all new employees, organizes continuous cybersecurity awareness popularization and education activities, and carries out training and learning of cybersecurity knowledge and skills based on their respective business needs and other awareness. Educational activities will also feature education and learning of cybersecurity cases based on the characteristics of their own business fields. The company regularly promotes cybersecurity periodicals on the internal platform for all employees; at the same time, it also promotes cybersecurity awareness to all employees through posters, information security promotional posters, videos/micro movies, startup reminders, etc.

Hikvision has identified the key positions of cybersecurity in various business fields, and the key positions of product security. For employees in key product safety positions, we have put forward the following requirements:

- Employees must pass background checks before taking up their jobs to ensure that people with backgrounds and experience that meet customer requirements are assigned to the correct positions. The "Safety-Critical Positions Confidentiality Agreement" will be signed to clarify the confidentiality obligations of employees.
- Employees should follow the qualification standards to enhance their awareness and improve their related skills. We conduct regular security reviews. Personnel in key positions will be subject to on-the-job investigations for possible violations.
- We instruct human resources and security specialists to regulate or modify the authority account for resigned employees, and their assets when necessary. Resignation review includes internal transfer and resignation.

We require every employee to be responsible for what they do and the results they produce, not only for technology, but also for legal responsibilities. Our employees know that once a cybersecurity issue occurs, it may have a great impact on customers, companies and individuals. Therefore, regardless of whether it is intentional or unintentional, Hikvision will continue to take action to ensure accountability and cybersecurity of its systems and products.

6.3 Security Training

Drawing on the best practices of the industry, Hikvision established a comprehensive cybersecurity training system. Various forms of training are incorporated into stages such as employee onboarding, job placement, and promotions, enhancing employees' security capabilities. Coupled with the company's well-developed security research and development management processes, the training system ensures our provision of secure and compliant products and services to customers.

Cybersecurity capability certification for product R&D positions: A cybersecurity competency certification is required for employees at software research and development (R&D) positions such as technical planning, demand design, solution development, code implementation, and verification testing, in order to enhance employees' awareness of cybersecurity, improve their cybersecurity capabilities, and elevate the security quality of our products. Employees must complete the competency certification before being eligible for job placement or applying for promotions.

Cybersecurity capability training camp: The Cybersecurity Department regularly organizes cybersecurity competency camps to provide concentrated training for the core security personnel. The training encompasses areas such as cybersecurity standards, certification, product security design, practical threat modeling, and product security management. This continuous effort enhances the security capabilities of core personnel and empowers them to better support their respective teams, ultimately elevating the security competence of all employees.

Special cybersecurity activities: Hikvision has carried out various practice-oriented special capacity-enhancing activities to enhance the knowledge and skills of employees in key positions in cybersecurity, such as: Cybersecurity Promotion Week, expert lectures, cybersecurity forums, and a case library.

Handwritten signature

Large handwritten signature
Handwritten initials: BZ, H, and a signature

7. Security Process

7.1 Hikvision Security Development Life Cycle

Product security and personal data protection relies on processes and systems for protection. Hikvision Security Development Life Cycle (HSDL) is developed by Hikvision, which deeply integrates product security requirements with the company's research and development process, and has formulated clear security requirements from concept, design, development, verification, release, and maintenance stages to ensure the safety and quality of our products.

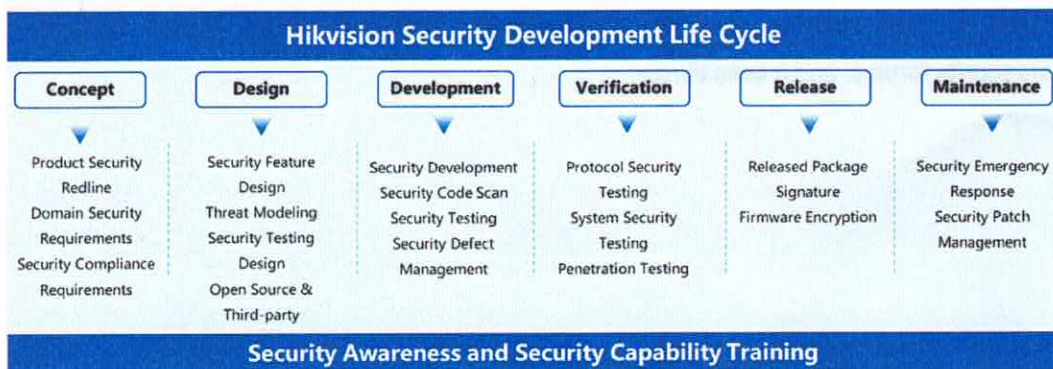


Figure 7-1 Hikvision Security Development Life Cycle

Concept Stage

During the concept stage, there are three important points in product security requirement analysis:

1. The product security redlines are mandated in the requirement list. Redlines represent the fundamental requirements that ensure the security objectives or minimize risks to acceptable levels. These requirements stem from laws, regulations, government mandates, client admissions, industry standards, and more. They aim to ensure product security compliance, safeguard sensitive user data, enhance system access control, and bolster the system's resistance to attacks.

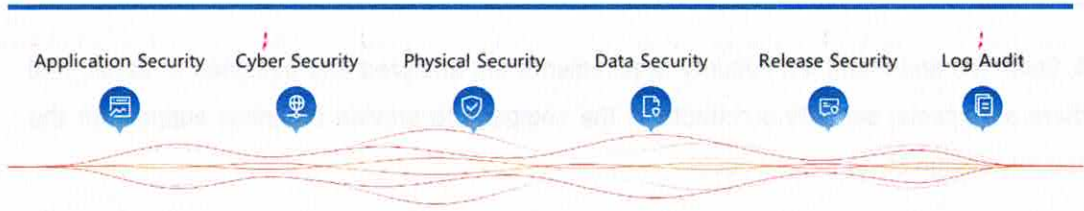


Figure 7-2 Product Security Redline

2. If the product involves personal data, a list of personal data involved in the product will be identified during the conceptual stage.
3. A threat analysis for the future usage scenarios of the product is conducted, aimed at identifying targeted security requirements. The analysis involves identifying all potential threat sources, types, and attack vectors specific to the product's usage scenarios. This helps us assess risks and ensures that relevant response and preventive measures are incorporated into the product requirement list.

Design Stage

Threat modeling is crucial in the product design phase. It's a structured approach that uses abstract methods to aid in risk assessment, aiming to identify, quantify, and address security risks associated with the product. The purpose of threat modeling is to identify potential threats to the system during the design phase, identify risks, and establish appropriate response measures. Threat modeling can identify security issues during the design phase, sort out security requirements, and avoid security risks during the coding phase, which helps to effectively control product security risks and reduce the cost of fixing security issues.

Hikvision requires that all baseline versions of new projects undergo threat modeling, and the Cybersecurity Department will review the threat modeling files through auditing:

1. Based on the logical architecture of the product, threat modeling methods are used to model the architecture level threats to the product, identify potential security threats to the product from the architecture level, and develop corresponding mitigation measures.
2. Security design and functional design are integrated together. When conducting functional design, we also establish threat modeling on a functional level to timely recognize security threats in the design and make mitigation measures accordingly.

[Handwritten signatures and marks in blue ink]

3. Collected and identified security requirements are analyzed and designed in detail, and there are special security architects in the company to provide technical support for the security design of various products.

4. For residual high risks in threat modeling, attack path analysis will be provided.

5. In the design stage, analysis on attack surface minimization will be conducted for all products, to reduce the overall product security risk.

Hikvision follows the HSDL safety research and development process to ensure that product functional design and safety design are synchronized, which can better balance safety and functional efficiency. Based on industry-wide design principles and combined with the company's main products, Hikvision has summarized six key principles: attack surface minimization, minimal privilege, default distrust, open design, default security and defense in depth.

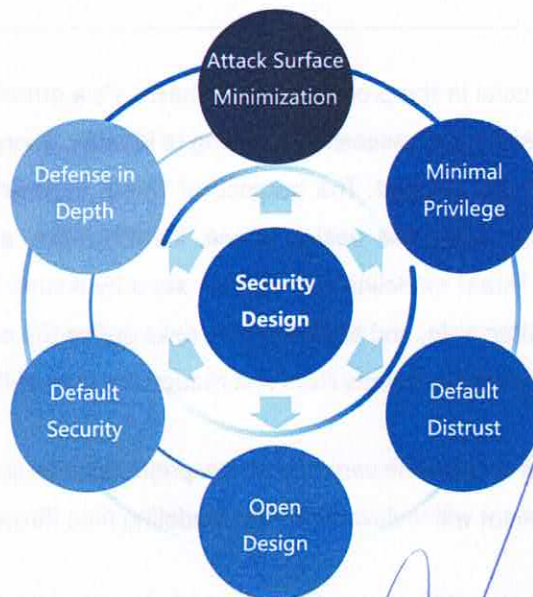


Figure 7-3 Security Design Principles

Development Stage

Hikvision requires R&D personnel to follow secure coding standards and conduct cross reviews during the development process. Through self-developed source code scanning platforms, code defects can be checked to quickly and accurately identify dangerous functions and defect issues in high complexity codes, reduce code security defect rates, and identify areas that require further inspection. Through self-developed code defect analysis and scanning tools for company business scenarios, known defects can be identified through code features, and R&D personnel can be informed of the existence of defects in various branches. The synchronization of defects is evaluated to ensure they are in place, and interception is carried out during continuous construction activities to control known code problems in the source code stage, greatly reducing repair costs.

Verification Stage

In order to ensure the security of Hikvision products and prevent various security issues that may occur during the development process, we conduct relevant security tests at stage of product development to ensure product security:

- Strengthen protocol security testing in product security testing, conduct network protocol security, robustness and reliability analysis on all products.
- Introducing vulnerability scanning tools in system security testing and timely tracking of CVE vulnerability library information can comprehensively identify various vulnerability issues in the product, including security vulnerabilities, security configuration issues, and application system security vulnerabilities.
- Introduce dynamic application security testing tools in application security testing to discover web application vulnerabilities.
- Conduct App security compliance testing to meet various security, personal data, and compliance requirements.
- Use multiple mainstream antivirus software to detect known viruses, Trojan horses, and other malicious code before product release.
- Hikvision's Interactive Application Security Testing (IAST) utilizes a proxy server to capture and simulate the request traffic that can monitor all instructions executed on the server

side in real-time by loading the monitoring program's jar package through configuring JVM parameters. It can transparently track the flow of the testing script in memory, and has the advantages of high efficiency, low false positives, and clear alerts (including call stacks, final executed commands, and other information) compared to traditional black-box testing tools, greatly facilitating developers to locate and fix security issues.

- The company will conduct penetration tests on products regularly to minimize business risks and keep security risks within controllable range.
- The company's product security management team analyzes security issues discovered during product testing on a quarterly basis, compiles a list of typical common security issues, and then delivers them to each product line for self-inspection to prevent similar problems from happening again.

Release Stage

Before the product release, Hikvision needs to develop a security test plan and strategy according to the product demand stage to complete the test. The test methods include functional security test, adversarial security test, fuzzing, penetration test, static source code review, and virus scanning through the company's self-developed security testing platform. The Cybersecurity Department and the Testing Department conduct a comprehensive security assessment.

The product release packages of Hikvision are digitally signed by the product development management to ensure the source and integrity of the software release packages are verified, effectively avoiding illegal software packages.

Maintenance Stage

1. Technical Support

The technical support team provides services to customers. With customer authorization, they may need access to some sensitive customer information. Therefore, providing them with essential training in network and information security is of utmost importance, which empowers them to assist in safeguarding customer interests and preventing errors in access control, communication security, and personal data protection. For employee management, the company has established the "Hikvision Technical Support On-Site Service Standards",

encompassing guidelines for behavior, personal safety, information security, and other aspects.

Hikvision strictly manages employees who can access customer networks and signs commitment letters with these employees, detailing their roles, responsibilities, and potential legal responsibilities. They are required to learn cybersecurity knowledge and take relevant exams.

2. Emergency Response

Hikvision established the Hikvision Security Response Center (HSRC), which is responsible for receiving, addressing, disclosing, and resolving security-related vulnerability issues with Hikvision's products and solutions. Responsibilities include:

- Responding to and handling customer-submitted security incidents.
- Responding to and handling security matters reported by industrial associations.
- Formulating the company's information security incident management strategy and procedures for handling security incidents.
- Analyzing the vulnerabilities and patches announced and released by system software providers and professional security companies.

The company also specifies each department's responsibilities and the procedures for product security incident management to ensure the quality and efficiency of security incident management. The scope of the Security Response Center's management responsibility covers product security during the pre-sales, sales, and after-sales processes, and includes customers' security related interactions, cooperation with security organizations, emergency response management, security information announcement, information security compliance, and the process and implementation of legal compliance.

Hikvision is a member of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the Security Emergency Service Support Organization of the Industrial Information Security Industry Development Alliance. It shares best practices and experience in security emergencies with other excellent members worldwide, enhances reliable communication and cooperation, and enhances the effectiveness and timeliness of the company's response to security incidents.

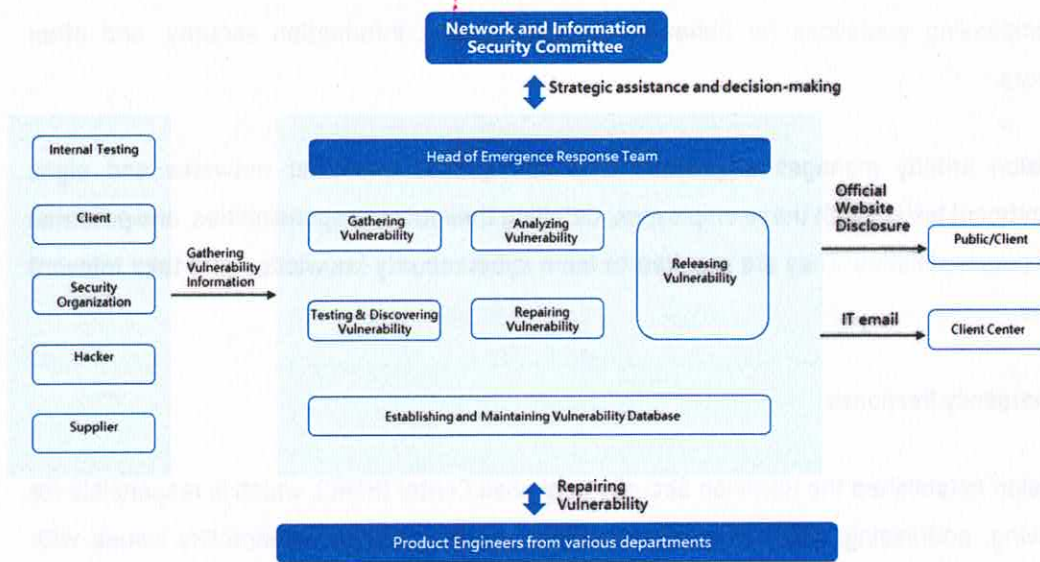


Figure 7-4 Security Emergency Response

3. Vulnerability Management

Hikvision has established a product security vulnerability handling and warning disclosure process based on the "Regulations on the Management of Network Product Security Vulnerabilities", ISO/IEC 30111, ISO/IEC 29147, etc., which includes five stages:

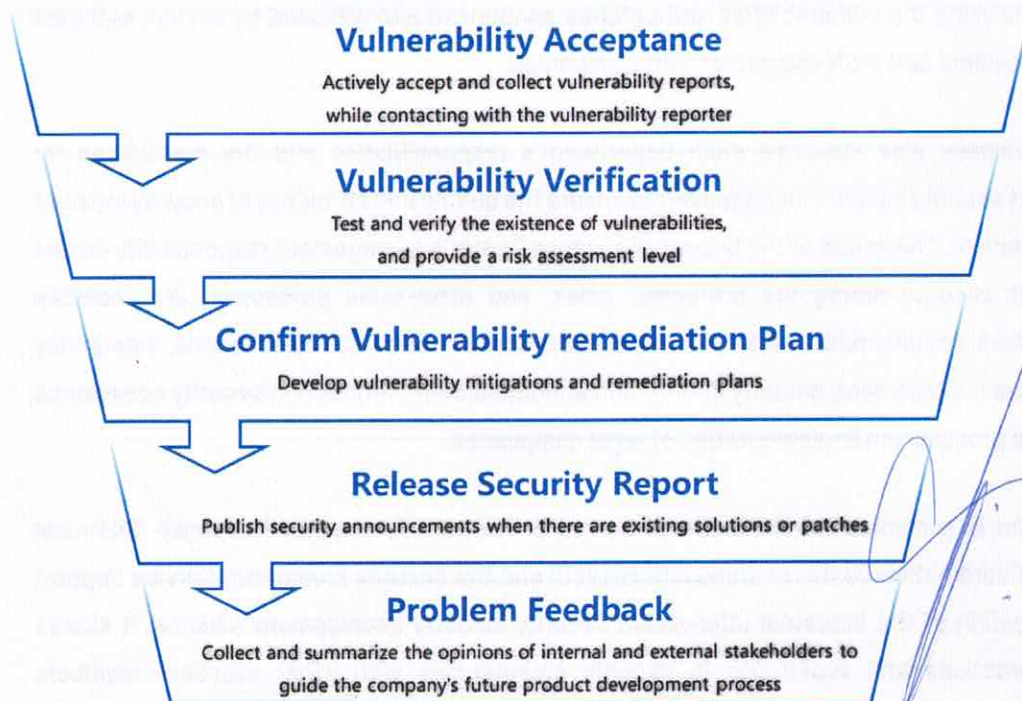


Figure 7-5 Vulnerability Handling Process

- **Vulnerability research and collection:** We obtain vulnerability information through customers, external CERTs, security researchers or related security websites. At the same time, we continue to discover potential security threats through our internal team. Hikvision supports responsible vulnerability disclosure and handling process, and respects the research results of every security researcher. External vulnerability discoverers should give manufacturers a reasonable period of time to process and solve problems before public disclosure.
- **Vulnerability assessment, analysis and verification:** Whether it is a suspected vulnerability or a confirmed one, the HSRC team will work with the personnel responsible for the product to quickly complete the assessment of the authenticity of the vulnerability and related risks.
- **Tracking and resolution:** Once the vulnerability is confirmed, HSRC team will immediately pass the information to the vulnerability submitter, and then actively track and feedback about the progress of the solution, and will also investigate the vulnerability to ensure that the problem is resolved in all product versions and product models. The HSRC process is closely integrated with the R&D core process to ensure a timely response to vulnerabilities.

At all stages of the process, protecting the confidentiality of customer and vulnerability information is critical to Hikvision. If vulnerability information falls into the hands of malicious people before patches or mitigation information is publicly released, it could allow threat actors to exploit vulnerabilities on unpatched systems. All parties must protect their confidentiality throughout the vulnerability disclosure process.

The Hikvision security response team actively participates in industry and public activities, and establishes long-term relationships with CERTs, vulnerability disclosure platforms, customer SRCs, other suppliers, researchers, and third-party coordinating agencies. Hikvision is a member of the internationally renowned vulnerability information database Common Vulnerability & Exposures (CVE) as a CVE Partner. The company is also a member of the China National Vulnerability Database of Information Security (CNNVD), China National Vulnerability Database (CNVD), China National Cyber Security Vulnerability Database (CICSVD). With these memberships, Hikvision can obtain security vulnerabilities discovered by external organizations without delay, improve security emergency response speed, and provide customers with more secure products and solutions.

7.2 Data Life Cycle Security Management

The company's product or service team consider the protection of personal data during the requirements analysis and design phase, and use appropriate technical and management measures to ensure the security of personal data according to specific business use scenarios. A Product Personal Data Statement is included in the product interface, if the company is involved in the processing of personal information. The Statement describes the type, purpose, processing method, retention period, risks or recommendations of all personal data generated in the product.

Data subjects have the right to be informed, the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to restrict processing, the right to data portability, the right to object, and the right to not be subject to automated decisions. To comply with regulations and better protect the data security, functions that support data subjects in exercising the above rights are included in the design and implementation of products and services.

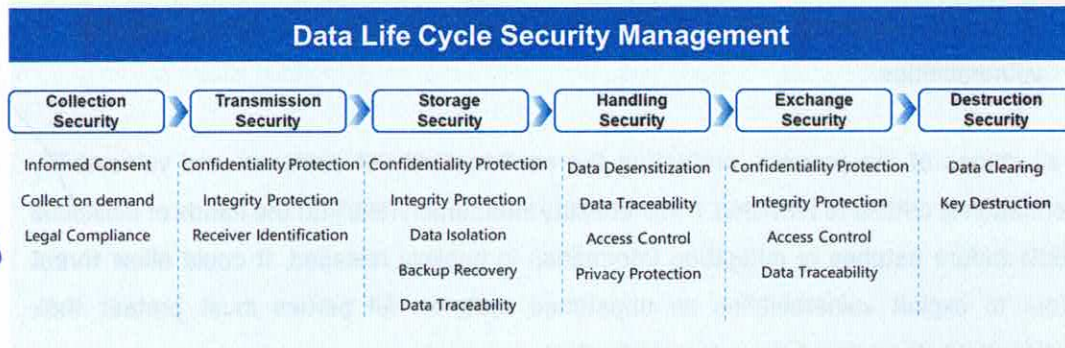


Figure 7-6 Data Life Cycle Security Management

1. Data Collection Security

Compliance with the applicable laws and regulations is a must for data collection. Users must be informed, and principles such as user consent and data minimization should be followed. Data should only be collected as needed, and the scope of collection and purposes of use should be clearly outlined in the personal data policy. When users engage with services or products that involve personal data, such as using Hikvision cloud services or IoT devices, Hikvision will inform users of the scope and purposes of data collection in accordance with applicable laws and regulations. Personal data will be collected only upon obtaining user consent.

2. Data Transmission Security

When transmitting collected data, it's crucial to authenticate the identities of both communication parties to ensure that the entity receiving or sending data is a legitimate user. This is primarily achieved through cryptographic techniques like message digests and digital signatures. During transmission, it's essential to prevent data leakage and to detect any tampering with the data. This involves ensuring the confidentiality and integrity of the transmitted data, which can be achieved using encryption, hashing, and digital signatures, among other traditional cryptographic algorithms. Hikvision product transmission security is ensured by utilizing the SSL/TLS protocol to guarantee the confidentiality and integrity of the data.

3. Data Storage Security

When storing data, data can be segregated and stored based on different levels of sensitivity. This can be achieved through various techniques such as physical isolation, logical isolation, or virtualization to create separation between areas containing data of different security levels.

Data storage media can potentially experience malfunctions or data loss. To ensure the availability of stored data, redundancy mechanisms are employed to back up the data. When the data storage media becomes available again, data recovery and restoration are carried out to bring the data back to its original state.

After data is stored, it's important to establish data traceability mechanisms. This ensures that if data is illicitly leaked, it can still be traced, allowing identification of the source of the leak and enabling relevant audits. Digital watermarking technologies can be employed to achieve data traceability in such cases.

When storing data, it's also essential to ensure data confidentiality and integrity. This means that even if attackers manage to access the data, they should not be able to retrieve meaningful information, and any unauthorized modifications should be detectable. To achieve this, traditional cryptographic techniques such as encryption, hashing, and digital signatures can be used. These techniques play a vital role in safeguarding data from unauthorized access and tampering.

Data storage security is ensured by employing standard cryptographic algorithms to ensure data confidentiality and integrity. The cryptographic algorithm calculation module provided by

the vendor utilizes cryptographic cards that comply with commercial cryptography specifications.

4. Data Processing Security

When processing and computing data, it is essential to ensure that users have the corresponding permissions. When data is used, sensitive information should be anonymized based on business relevance and the principle of least privilege. In data calculations, it is crucial to prevent the extraction of additional personal information from intermediate results. Privacy-preserving technologies such as secure multi-party computation, homomorphic encryption, and differential privacy computing can be employed to protect personal information during the data usage process. Hikvision employs techniques such as data anonymization, encryption, and privacy-preserving computing to safeguard personal information during the data processing.

5. Data Exchange Security

Security control on data exchange channels is necessary for data transmission and sharing, with measures such as mandatory identity authentication and strict access control. Data watermarking and other methods are used for traceability in the process of data exchange. Hikvision adopts password technology to ensure data confidentiality, integrity and access control in interacting with data, and employs digital watermarking technology for data traceability.

6. Data Destruction Security

Logical deletion and physical destruction are to be employed for data destruction to prevent the data from being recovered or retrieved after erasure, especially sensitive data such as passwords and keys.

8. Security Technology

8.1 Configuration Management

Configuration Management plays a vital role to guarantee a product's integrity, consistency, and traceability. It contains many processes, including strategy and planning, configuration item identification, configuration item change management, configuration status tracking, configuration activity reporting, configuration auditing, build management, release management, third-party software and open-source component management, and repository management, etc. Configuration management underlines the integrity of Hikvision's product delivery, including third-party software and open-source components within the product. Hikvision's configuration management process constitutes an inseparable part of the IPD process. The aforementioned configuration management steps are conducted at each stage in the Integrated Product Development (IPD) process to promote the implementation of product traceability. They are a key part of security.

Build Management Specifications

Build management specifications include build resource management, build process management, and build process optimization. The segregation of duties is an important part of configuration management. The activities, roles, and responsibilities must be clearly defined in the specifications during the build process. The various stages of product development should be integrated, and the life cycle be clearly incorporated into the IPD process.

Compiling and Build Center

To ensure the repeatability and consistency of the construction process, Hikvision established a compiling and build center. In addition to meeting the management requirements of compilation, the center also enforces strict admission standards control for all hardware, compilation tools, third-party software, data sources, and operating systems. As a comprehensive solution for product compilation and build, the center offers compilation and build cloud services, supporting software building within the IPD process.

Standardization of the Build Process: unified tool management, standardized build scripts, one-click building, and automated installation of the build environment realize automation throughout the entire product building process, including environment setup, code downloading, one-click compilation, packaging, static checks, and automated unit testing,

up to system testing. This ensures replicability, reproducibility, and traceability of the product building process.

The center also features two additional functionalities: a Virus Scanning Center and a Digital Signature Center. The former operates multiple antivirus software tools simultaneously for scanning, integrated into the testing process. For security purposes, the Digital Signature Center employs key pairs stored in a key database to digitally sign the compiled code. Hikvision authorizes and records signature activities to ensure traceability throughout the entire process.

Software and Component Version Management

With its self-developed SWMS software management platform, Hikvision enjoys a structured and standardized software version organizational structure. Focusing on the entire software development process, the platform aligns with the software lifecycle management approach spanning requirements, design, development, integration, testing, and release. It facilitates the intuitive display of software development processes and process data, ultimately achieving artifact management and realizing the goal of effective software management.

Furthermore, Hikvision utilizes a component-based development approach for its products, focusing on managing the lifecycle of these components. This entails component version, build, delivery, and data management. After completing the version development of a component, it undergoes component version validation. Once validation is successful, the component is submitted to the component repository within Hikvision's proprietary SWMS software management platform. The component repository identifies information about each component package, including its name, group, version, target platform, source code, static analysis results, whether it includes third-party software, and security status. Hikvision employs a methodology similar to Maven to manage embedded components such as C/C++ components. Each component is integrated using a component configurator that aligns logically with the Project Object Model (POM), gradually assembling them into a finalized software product. Based on the integrated information, a unified version information structure and Software Bill of Material (SBOM) repository are established to track component version application. In case a security issue arises with a specific component version, it allows for quick identification of software versions utilizing that component version, aiding in maintenance and updates. Additionally, the ability to disable problematic component versions and provide replacement versions is offered to prevent issues from spreading unnoticed.



Third-party Component Management

Hikvision procures many third-party and open-source components from around the world and uses them in our products. That is why Hikvision takes the following issues seriously:

- Reliability of the source code or component source
- Compliance with the company's security risk assessment requirements
- Elimination of any known vulnerabilities
- Management of license compliance
- Strategies to address newly discovered vulnerabilities
- Life cycles of third-party components
- Incorporation of third-party components into Hikvision's product life cycle

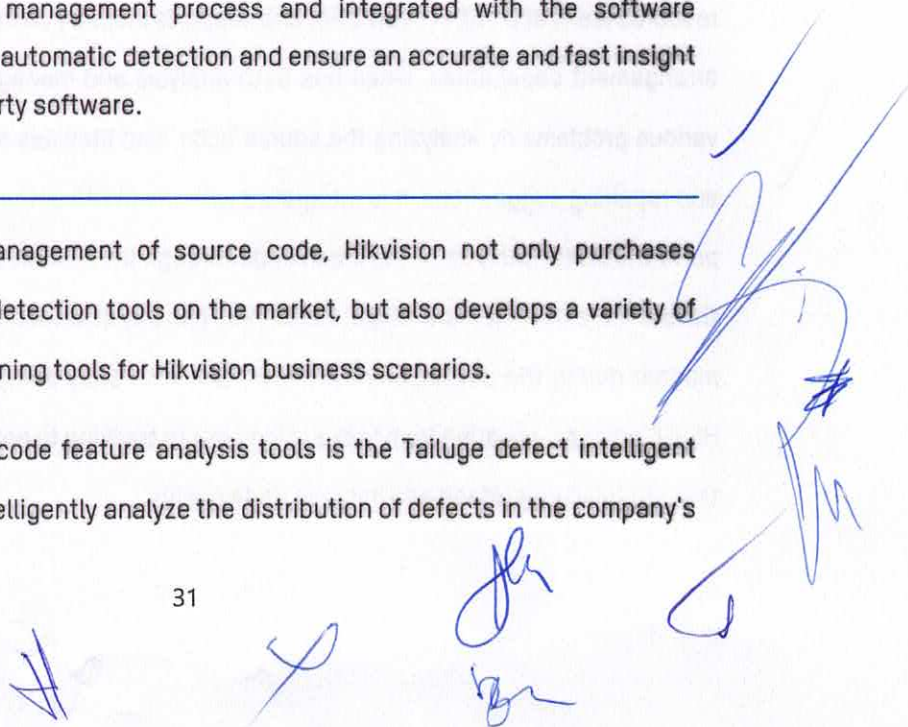
Hikvision not only needs to assure the security of third-party components, we also need to ensure that the related components required by all compiled source code or third-party components are managed properly. Hikvision has formulated the "Third-party Component and Source Code Management Specifications" to ensure that third-party components comply with our requirements and can be effectively managed.

Hikvision places great emphasis on the compliant, reasonable and secure use of the third-party software. Various binary and source code analysis software, such as FOSSID, Cybellum, etc., are introduced into the management process and integrated with the software management platform to realize automatic detection and ensure an accurate and fast insight into the components of third-party software.

Code Static Analysis

In the quality and security management of source code, Hikvision not only purchases mainstream commercial static detection tools on the market, but also develops a variety of known defect analysis and scanning tools for Hikvision business scenarios.

One of the key self-developed code feature analysis tools is the Tailuge defect intelligent analysis platform, which can intelligently analyze the distribution of defects in the company's



code warehouse, software version warehouse, order system and other systems based on the characteristics of defect codes. The system will inform R&D personnel of the existence of defects in each branch, the risk situation of each version, and even the impact of orders, so as to ensure that R&D can systematically evaluate defects and work synchronously. We have a complete set of mechanisms to ensure that the defects identified by Tailuge analysis form closed-loops: Before new code branches are generated, we will scan the source code for Tailuge defects. When there are known defects, we will remind relevant personnel to repair in time and support online one-click repair. If there is a specified type of high-risk defect, we will automatically disable the branch, requiring that the defect be repaired first. During the code development process, if there are known defects in the code, we will give an early warning in the IDE used by the developer and push related pending repairs. When the code development is completed to trigger the CI build, Tailuge's defect scanning function will be triggered first to detect whether the current branch version contains Tailuge's known defects. The scan results will inform the builders immediately. If there are specified types of high-risk and high-risk defects, we will directly stop the build and require that the defects be repaired first. In addition, we have also added problem version status management, aligned with PLM to realize software disabling, and also aligned with the production order system, and realized immediate interception of high-risk defect orders.

Another key code feature is the iScan code static scanning platform developed by Hikvision, which supports the detection of serious vulnerabilities such as null pointer references, resource leaks and buffer overflows, and supports industry coding standard detection and rule arrangement capabilities. iScan has both analysis and management functions, it identifies various problems by analyzing the source code, and provides efficient problem management and repairing suggestions. It is integrated with the SWMS software management platform and performs static analysis of the iScan code through the continuous integration pipeline during the software development stage. Developers can pay attention to safety and quality in a timely manner during the development process, and efficiently manage and solve problems in the HSDLC process, covering from task assignment to tracking to problem closure, helping the R&D team to fully understand and improve code quality.

8.2 Security Certification

The global legal environment is complicated and is constantly evolving, and industry supervision requirements are becoming increasingly complex. Particularly in the field of cybersecurity laws, many countries and regions have issued laws and regulations in recent years, such as the Cybersecurity Law of China, and the General Data Protection Regulation (GDPR) of the EU. Security compliance has become a major challenge for Internet of Things service providers. Hikvision strives to establish effective internal control security systems that follow and comply with the requirements of different industries, fields, and countries, while also completing its own compliance foundation in its system processes and control activities. To meet the needs of global business expansion, help the company better comply with global regulations and laws, and promote the normalization of operations in countries and regions, Hikvision established the Compliance Department in December 2018 to improve its global compliance system.

Hikvision has a professional team of lawyers for the investigation, identification, and tracking of laws and regulations that are applicable to the company around the world. Hikvision has also established a long-term cooperation with experienced and prestigious law firms domestically and internationally. We have a dedicated group to integrate the applicable laws and regulations into Hikvision's operations, and to identify and control the legal risks involved in the product development, manufacturing, delivery, and service processes and also to provide compliance advice and support. We continue to conduct special compliance training for new employees, mid and high-level managers, and employees in key cybersecurity posts as new laws and regulations are issued to improve compliance awareness.

Hikvision strives to improve the security integrity of our video products. In addition to abiding by the applicable security regulations in the countries and regions where we operate, and referencing the best practices within the industry, the company has also established a complete, sustainable, and reliable security system that involves company policy, organization, process, technology, and specifications.

Hikvision supports mainstream international standards, and contributes actively to the formulation of these standards. Hikvision has participated in the formulation of industrial security standards which further open key security technologies to work with other industry experts and national standards organizations to perfect security standards related to Internet of Things.

Hikvision also cooperates with independent third-party assessment organizations and staff for fair security assessments and certification.

Supply Chain Security

Diverse participating entities, numerous process steps, and cross-regional product transfers of supply chain systems render it susceptible to both internal adversities and external threats, such as unauthorized production, tampering, theft, malicious software and hardware implantation, as well as poor manufacturing and development practices within the supply chain. Vulnerabilities in supply chain systems may remain latent for years before being discovered, and in many instances, it's difficult to ascertain whether security events are a direct result of supply chain vulnerabilities. Security issues within the supply chain could exert sustained negative impacts on organizations.

In order to reduce security risks and ensure hardware and software integrity, Hikvision uses anti-tampering, anti-implantation, anti-replacement and other security management measures during key stages of product manufacturing, such as software provision, chip burning/calibration, software loading, and production testing. This helps prevent unauthorized hardware replacement, software implantation and tampering, virus infection and other risks. The product data management system takes the software required by the devices and downloads them onto a secure distribution system. Before software is embedded into devices, multiple integrity checks are conducted.

The network used in the supply chain for software burning, software loading, assembly, and testing should be isolated from the company's office IT system and from the Internet.

Automated testing is implemented for Hikvision products. Hikvision uses automated testing to reduce the risk and security threat brought about by human errors.

Besides by technical means, Hikvision also guarantees its supply chain security by management system. ISO 28000 supply chain security management system is aimed at comprehensively improving supply chain security, and helping organizations and departments deal with potential security risks in supply chain by auditing security risks and implementing control and mitigation measures. ISO 28000 is compatible with ISO 9001 quality management system and ISO 14001 environmental management system, and can be integrated with them in the organization.

After specifying the operating environment of supply chain, identifying threats from various links and conducting risk assessment and response, Hikvision established a supply chain security management system that fully complies with ISO 28000, and has realized continuous update and improvement of the system with the management method of PDCA (plan-do-check-act).

Hikvision has implemented a secure and strict maintenance process to ensure the integrity of products during the process. Information from the entire process is recorded in Hikvision's manufacturing and barcode systems. A detailed executive record and log is kept for the research and development, procurement, manufacturing (chip burning, software loading, assembly, testing, etc.), warehousing, and logistics processes to ensure traceability.

Common Criteria / ISO 15408

CC (Common Criteria) certification is one of the most widely recognized international certifications in the field of information technology security. It is endorsed by the United States National Information Assurance Partnership (NIAP), which operates under the oversight of the National Institute of Standards and Technology (NIST). It is also recognized by countries such as the United Kingdom, Canada, and other Western nations. Currently, security certification organizations from 31 countries around the world have joined the CC Recognition Arrangement (CCRA). Since CCRA members are either government agencies or third-party authoritative organizations in their respective countries, CC certification has high acceptance and credibility on a global scale. It has become an important foundation for security assessments.

CC certification is primarily used to evaluate the security, reliability, and privacy protection of information technology products or solutions. The certification is divided into seven levels based on the Evaluation Assurance Levels (EAL), ranging from EAL1 to EAL7, with increasing levels of verification requirements.

In September 2018, two series of Hikvision cameras were certified with EAL2⁺¹, and another three series of cameras with EAL3+ in June 2022. Hikvision is committed to making all products up to the EAL3+ standards, thus improving the company's security practices to new heights and setting a great example within the industry.

¹ CC certificate query: <https://www.commoncriteriaportal.org/>

ISO/IEC 27001

ISO/IEC 27001 Information Security Management System (ISMS) is the most authoritative, rigorous, widely accepted, and applied certification standard in the field of information security internationally. Acquiring this certification suggests that a company has established a scientifically effective ISMS to align its business development strategy with information security management. This ensures appropriate control and responses to information security risks. Hikvision first established its ISMS in 2012 and, after a decade of innovation and improvement, officially launched Hikvision Information Security Management System 3.0 (HISMS3.0) in 2021. Covering management requirements for cybersecurity, information security, and privacy protection, this system follows the PDCA (Plan-Do-Check-Act) continuous improvement approach, providing reliable support and assurance for Hikvision's operations. In January 2023, Hikvision successfully obtained certification from the British Standards Institution (BSI), an internationally renowned audit organization. It marked Hikvision as one of the first companies worldwide to receive the ISO/IEC 27001:2022 certification, showcasing Hikvision's information security management capabilities as a global leader on the international stage.

ISO/IEC 27701

As the privacy extension of ISO/IEC 27001 of the Information Security Management System (ISMS), ISO/IEC 27701 is designed to assist organizations in effectively protecting and compliantly handling personal information. As the most authoritative privacy protection standard globally, it serves as an internationally recognized guide for best practices in privacy protection. The standard also offers guidance for the appropriate technical and organizational measures stipulated in the General Data Protection Regulation (GDPR), making it an important reference and major support for privacy-related legal compliance.

Hikvision obtained the ISO/IEC 27701:2019 certification awarded by BSI in December 2021.

ISO/IEC 29151

The British Standards Institution (BSI) ISO/IEC 29151 standard addresses security concerns related to personal information in the rapidly advancing IT sector. With the protection of personal information at its core, it regulates various data operations throughout the stages of personal information collection, storage, processing, usage, and disclosure. The standard aims to strengthen the identification of risks associated with personally identifiable information, conduct accurate assessments, and implement effective control measures. ISO/IEC 29151 further enhances the security and reliability of business processes, reduces the

risks associated with personally identifiable information in IT operations, and maximizes the protection of users' legal rights and societal interests.

Hikvision obtained the ISO/IEC 29151:2017 certification awarded by BSI in December 2021.

CMMI5 Software Maturity Certification

Capability Maturity Model Integration (CMMI) is an enterprise-level process management framework and a best practice used by the world's top companies. It is recognized by the industry as the authoritative standard for measuring an enterprise's product and service capabilities. It is also a method for improving processes that can help companies achieve commercial goals, ensure quality, guarantee deliveries and improve customer satisfaction levels. There are five maturity levels which companies are assigned in the Software CMMI specifications. Level 5 is the highest level.

Hikvision successfully passed CMMI5 certification in April 2016.

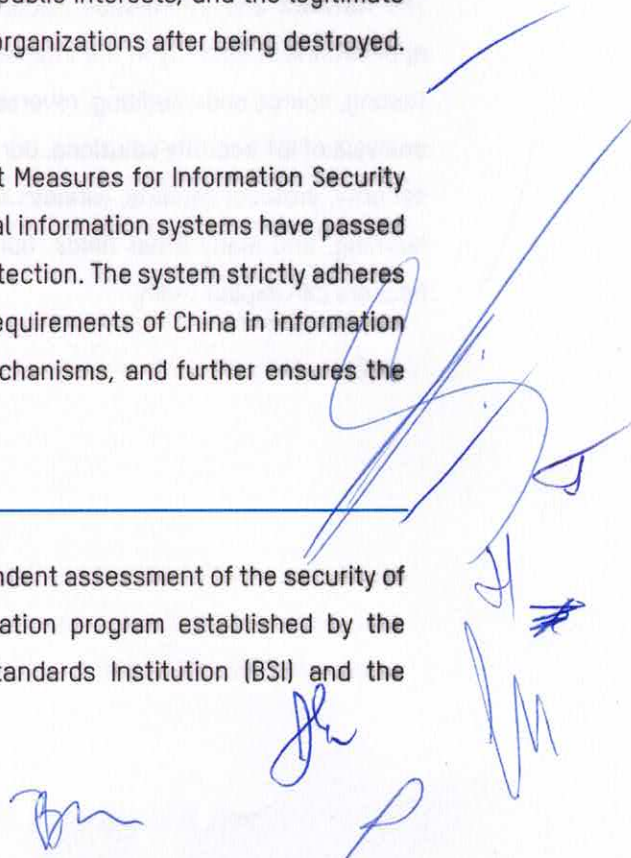
Information Security Level Protection Certification

The Information Security Level Protection is a fundamental system in China's information security guarantee, which aims to protect the development of information technology and maintain the fundamental guarantee of national information security. The security protection level of information systems is divided into five levels based on factors such as the importance of the information system in national security, economic development, and social life, as well as the degree of harm to national security, social order, public interests, and the legitimate rights and interests of citizens, legal persons, and other organizations after being destroyed. The fifth level is the highest system level.

According to the relevant provisions of the "Management Measures for Information Security Level Protection", both EZVIZ Cloud and Hikvision's internal information systems have passed the third-level evaluation of information security level protection. The system strictly adheres to the technical guarantees and security management requirements of China in information system security construction, establishes long-term mechanisms, and further ensures the continuous implementation of security protection work.

CSA STAR Certification

The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. It is an international certification program established by the founders of global standards, including the British Standards Institution (BSI) and the



international Cloud Security Alliance (CSA), which are the world's leading organizations dedicated to defining best practices that help ensure secure cloud computing environments.

Based on ISO/IEC 27001 certification, combined with the requirements of cloud security control matrix CCM, and using the maturity model and evaluation method provided by BSI, CSA STAR conducts a comprehensive assessment of the cloud security management and technical capabilities of the organization who provides and uses cloud computing, and finally produces an independent third-party audit result.

In December 2021, Hikvision achieved CSA-STAR certification.

GDPR

Hikvision is always committed to protecting personal data and will fully support the implementation of the GDPR. Hikvision has been taking a number of initiatives to protect personal data, including data collection through authorization, minimization of data collection, data anonymization, communication and storage encryption, data security audit, etc.

To ensure the security of products and services, Hikvision has put forward a series of data protection policies and established a data protection working group, integrating GDPR requirements into the business operation.

8.3 Product Security Research and Collaboration

The Network and Information Security Laboratory is dedicated to research and practical applications of security in the Internet of Things. Our work includes penetration testing, fuzz testing, source code auditing, reverse analysis, vulnerability research, tool development, and analysis of IoT security solutions. Our team's main research areas cover web security, mobile security, protocol security, wireless security, firmware security, threat intelligence, machine learning, and many other fields. Our goal is to discover and solve security issues before hackers can exploit them.

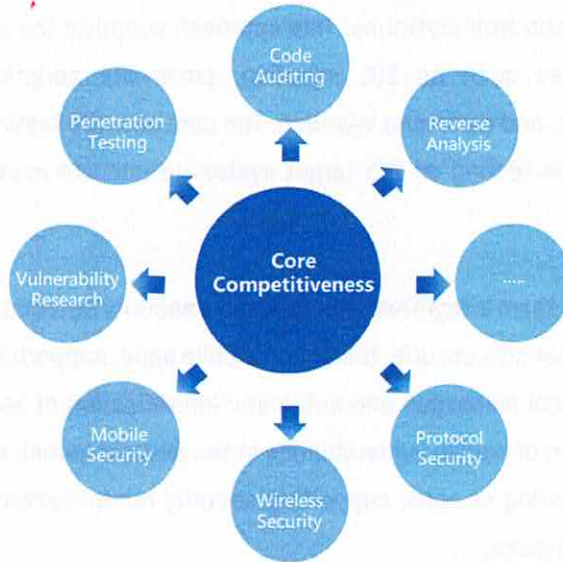


Figure 8-1 Research on core competitiveness of product security

Core Competitiveness:

- **Embedded Device Vulnerability Mining:** Benefiting from experience in embedded device security, Hikvision employs firmware reverse, firmware emulation, serial debugging, static analysis, symbolic execution, and other means for vulnerability mining.
- **Protocol Vulnerability Mining:** Integrating commercial tools and self-developed fuzzing testing tools to automatically mine high-risk vulnerabilities in mainstream IoT device protocols, hundreds of which have been discovered to date.
- **Wireless Security Research:** The team has a variety of security hardware testing environments, including RFID, wireless radio frequency, and Bluetooth modules, which can achieve wireless data packet eavesdropping, wireless signal replay attacks, wireless signal deception attacks, wireless signal hijacking attacks, RFID cracking attacks, and NFC cloning attacks.
- **White-box Audit:** Integrating commercial tools to track and detect known vulnerabilities of all open-source components used internally and provide threat warnings; the internal team will conduct white-box auditing of target source code during penetration testing to comprehensively improve vulnerability mining efficiency.
- **Web Security:** Commercial tools and proprietary web testing utilities are integrated with crawler-based reconnaissance techniques and passive proxy technology to conduct

[Handwritten signatures and scribbles in blue ink]

penetration testing on web platforms. This approach supports the detection of various web security issues such as SQL injection, cross-site scripting (XSS), sensitive information leakage, and command injection. The core security testing team will perform in-depth penetration testing on the target system to uncover more potential security vulnerabilities.

- **Mobile Security:** The team integrates internal mobile security detection and analysis tools to conduct comprehensive security testing on mobile apps, supporting real-time capture of interaction protocol messages and automatic identification of sensitive information; supporting detection of known vulnerabilities in the Android kernel; supporting personal data compliance testing of apps; supporting security reinforcement of mobile apps to prevent malicious attacks.
- **Threat Intelligence:** The team builds various types of distributed high/low interaction honeypots, which can sense all kinds of malicious IoT attacks and capture attack samples in real-time and conduct real-time correlation analysis and warning.
- **Machine Learning:** The team uses machine learning algorithms to conduct security analysis of IoT device logs, providing various security attack detection models, which can quickly detect potential or known malicious attack behaviors from massive logs and conduct real-time threat warnings.

Security Engine

1. IoT Security Protection Engine

In order to continuously improve the detection and defense capabilities of IoT devices against cyber threats, the Network and Information Security Laboratory team has independently developed intrusion defense and protocol firewalls for security detection and protection engines that can be applied to IoT devices. This achieves a comprehensive monitoring of the status of IoT devices, full perception of risks, and real-time blocking of attacks for security protection capabilities. The engine supports non-destructive upgrades through hot updates to cope with new types of network attacks, providing reliable and stable operation of IoT devices.

2. Intrusion Prevention Engine

The intrusion prevention engine is specifically designed and developed for the IoT devices of a company. The IoT devices are equipped with built-in intrusion defense engine modules at

the factory. After booting up, the engine monitors and analyzes the real-time status and operational behavior of the device's files, networks, processes, and other aspects. It blocks the startup and operation of malicious processes through a process whitelist. It also monitors and detects malicious file creation, deletion, modification, and other operations, and intercepts them. Moreover, the engine monitors and blocks abnormal device external network behavior in real-time, preventing the possibility of IoT devices being controlled as zombie network bots.

3. Protocol Firewall Engine

Due to resource constraints, IoT devices are unable to cope with large-scale malicious scans and cyber-attacks, and conventional security software cannot be deployed for use. In order to effectively defend against common cyber-attacks on device security and stability, the company's security team, through accumulated knowledge of security attack and defense techniques and a deep understanding of embedded devices, collaborated with the R&D team to customize and develop a lightweight IoT protocol firewall engine module. The engine directly obtains the raw request message content from the business module and conducts cyber-attack behavior detection before the message enters the business processing logic. When an attack is detected, the engine notifies the business module to promptly discard the message and decides whether to automatically block the attack target based on the interception strategy. By deeply integrating with the business module, this solution overcomes the pain point of traditional security protection products' inability to detect encrypted messages and can comprehensively detect and analyze various IoT protocols, effectively resisting various common cyber-attacks and enhancing the security and stability of IoT devices.

Security Situational Awareness

The enormous Internet of Things system, formed by devices, network, platforms and applications, requires multi-layer protection and End-Cloud Collaboration with smart, big data security analysis capabilities. The implementation of smart security situational awareness, visualization, and security for entire networks will be an emerging trend for the Internet of Things.

Security situational awareness refers to the acquisition, understanding, display, and prediction of important security elements that can cause changes in the system state within large-scale system environments.

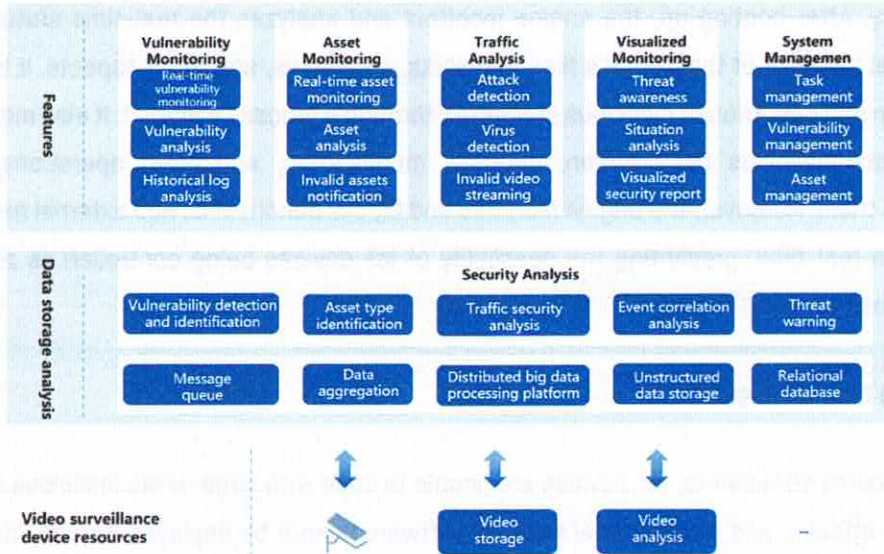


Figure 8-2 Security Situation Awareness

Vulnerability Assessment

Vulnerability assessment is key to determining the effectiveness of a security situational awareness system in detecting security vulnerabilities. The Hikvision security situational awareness system integrates mainstream vulnerability databases to conduct checks on existing vulnerabilities. In addition, Hikvision has a professional vulnerability research team that continually tracks security announcements released by other well-known security organizations and vendors. The team also continuously analyzes, explores, and verifies various new vulnerabilities. With the continuous investment of Hikvision’s professional vulnerability research team and the continuous upgrading of the vulnerability database, users can be promptly alerted to potential security risks and take preventive measures.

Furthermore, the Hikvision video security situational awareness system can perform correlation analysis on discovered security threats and asset information. By establishing a big data analysis model and dynamically analyzing real-time and historical data, the system can accurately and efficiently perceive the security status and development trends of the entire network. This enables users to make reasonable security reinforcements for video security networks and ensure the security of video security systems.

Security Visualization

Security visualization can present data characteristics intuitively and be easily accepted and understood by readers. Therefore, big data analysis (such as deep packet inspection and full

[Handwritten signatures and scribbles in blue ink at the bottom of the page]

traffic analysis) results require visualization.

When a system is under attack, it is necessary to quickly identify the source of the attack, the attack path, and respond to the attack quickly. Effective measures should be implemented before the attack causes greater damage in order to reduce losses. After the attack, it is necessary to quickly prevent such attacks from happening again.

Honeypot

Honeypot technology is essentially a deceptive technique used against attackers. By deploying some hosts, network services, or information as bait, attackers are lured into attacking them, allowing for the capture and analysis of the attack behavior, understanding the tools and methods used by the attacker, and inferring the attack intent and motivation.

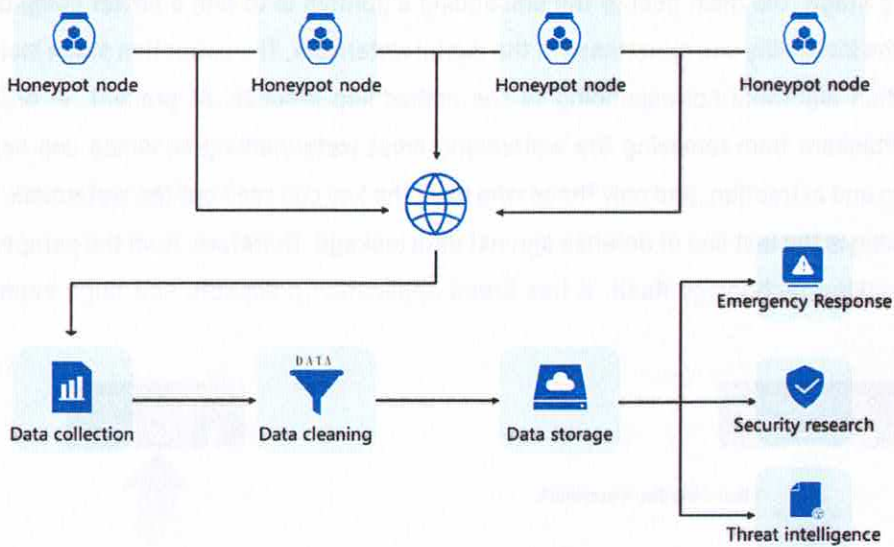


Figure 8-3 Honeypot system

Benefiting from the rise and development of technologies such as data storage, retrieval, mining, and threat intelligence, the value of honeypot technology can be more fully realized. Hikvision has deployed honeypot nodes worldwide based on self-developed and modified honeypots as data collectors, and has established a honeypot data pipeline for collecting, processing, storing, and retrieving honeypot data, providing data support for security research, emergency response, attack tracing, and situational awareness.

Hikvision's honeypot system is based on a rule engine that monitors attacks on IoT devices in real time and issues alerts for unknown threats. The analysis engine of the honeypot system can focus on monitoring and correlating analysis of malicious attackers based on historical data from the honeypot system, and predict threat trends.

As an important component of Hikvision's threat intelligence platform, the honeypot system will continue to monitor security threats from around the world to ensure the secure and stable operation of user devices.

Digital Watermark

Data watermarking refers to the embedding or implicit marking of display in data files (such as videos, audios, images, documents, databases, models, etc.) based on information security, information hiding, data encryption and other technologies, in order to cope with traceability and copyright declaration after data leakage.

The digital watermarking system mainly includes two stages: embedding and extraction. In the embedding stage, the main goal of the embedding algorithm is to find a better compromise between the invisibility and robustness of the digital watermark. The extraction stage includes an extraction algorithm corresponding to the embedding process. At present, in order to prevent attackers from removing the watermark, most watermarking schemes use keys in embedding and extraction, and only those who have the key can read out the watermark. Data watermarking is the last line of defense against data leakage. Therefore, from the perspective of watermarking technology itself, it has broad application prospects and huge economic value.

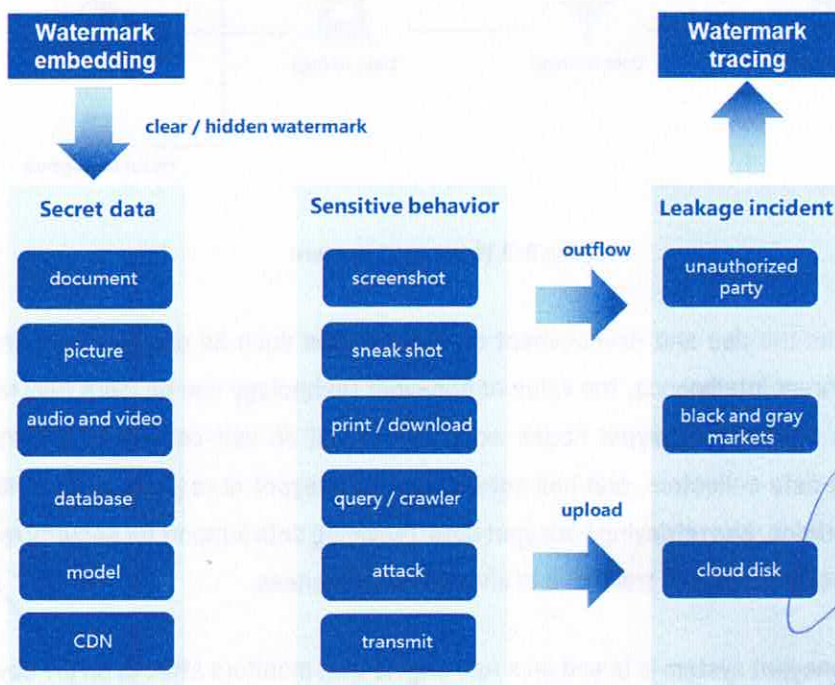


Figure 8-4 Digital watermark

Exchange and Collaborations

- Invite well-known domestic and foreign security assessment institutions to benchmark and construct the company's R&D security management system, ensuring that Hikvision's R&D security system is in line with international first-class companies.
- Strengthen communication and cooperation with domestic and foreign security vendors to enhance the security of the company's products.
- Invite well-known domestic and foreign security testing teams to conduct penetration testing on the company's products, minimizing business risks to maintain security risks within a controllable range.
- Invite well-known domestic and foreign security experts to the company to teach R&D personnel, improving their competencies of security.
- The company communicates with customers several times a year on product security topics, emergency response mechanisms, and security requirements, and timely pushes security progress to customers to understand their needs.
- The "Security White Hat Rewards Program" launched by the company to reward domestic and foreign white hats who pay attention to Hikvision's information security, and to collaborate with excellent security technology researchers who promote the continuous improvement of Hikvision's product security.



Figure 8-5 Exchange and Collaborations

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

Hikvision through external exchange and collaboration, accepts feedback from stakeholders, absorbs advanced security technology and management experience in the field, systematically transforms them into future improvement goals, and continuously improves the company's information security capabilities.



Handwritten signatures and initials in blue ink, including a large signature at the top, several smaller initials below it, and a checkmark on the right side.

9. Security Commitment

Hikvision is committed to using leading security and personal data protection technologies to help customers protect their personal information and to adopting a comprehensive approach to protect user data.

Hikvision uses a unified integrated security infrastructure throughout the entire video IoT application ecosystem. Hikvision has a professional security team responsible for supporting all Hikvision products. This team provides security audits and testing for products released or under development. The security team also provides security training and actively monitors reports of newly discovered security issues and threats. To learn more about how to report issues to Hikvision, please contact us here:

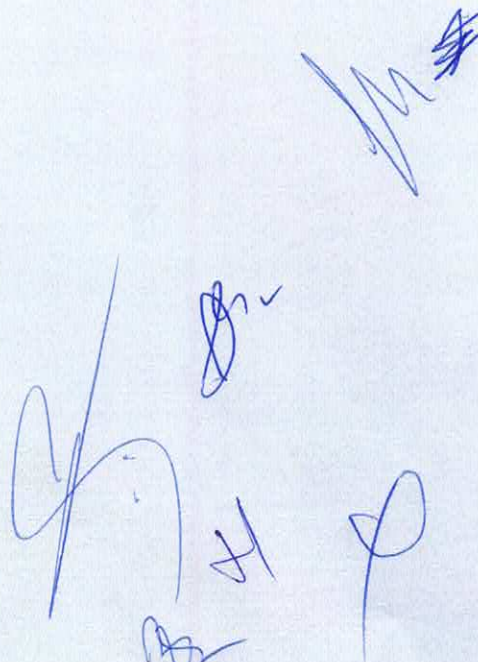
<https://www.hikvision.com/en/support/cybersecurity/>

Hikvision Cybersecurity White Paper

See Far, Go Further

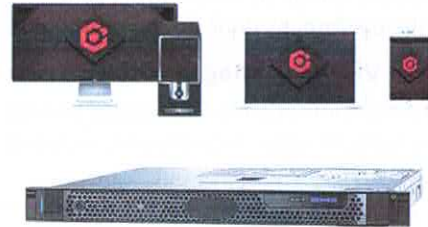
HIKVISION

Hangzhou Hikvision Digital Technology Co., Ltd.
No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China

A collection of approximately seven handwritten signatures in blue ink, scattered in the lower right quadrant of the page. The signatures vary in style, with some being highly stylized and others more legible. One signature at the top right appears to be a name, possibly 'M. #'. Other signatures are more abstract scribbles.

HikCentral Professional

HikCentral Professional is an integrated security software designed to meet versatile security challenges in one intuitive platform: from managing individual systems such as video security, access control, intrusion alarm, etc., to collaborating multiple systems under a unified architecture. While protecting people and property, it makes daily operations more efficient, and helps various kinds of users make smarter decisions.



Key Feature

Home Page

- Providing three predefined Home page modes on Web Client, including system installation and management mode, security control and management mode, and attendance management mode
- Supports customizing Home page mode on Web Client
- Supports customizing control panel on Control Client
- Supports switching Home page mode for visualization and non-visualization management
- Providing different report dashboards for resource status, intelligent analysis results, access records, vacant parking spaces, alarms, etc., on the Home page of Web Client

Wizard

- Providing wizards for video management, access control, vehicle management, alarm detection, and digital signage management on Web Client

Live View and Playback

- Up to 256 channels live view simultaneously
- Custom window division configurable
- Viewing maps and real-time events during live view and playback
- Stream type self-adaptive, transcoded playback, and frame- extracting playback
- Fisheye dewarping of multi-channel
- Controlling PTZ in visualization way
- Supports decoding stream from cameras with high-definition, such as PanoVu series camera

Visual Tracking

Recording and Storage

- Recording schedule for continuous recording, event recording and command recording
- Storing videos on encoding devices, Hybrid SANs, cloud storage servers, pStors
- Providing main storage and auxiliary storage
- Providing video copy-back
- Storing alarm pictures on NVRs, Hybrid SANs, cloud storage servers, pStors, or HikCentral server
- Supports search of VCA event related videos, video footages, and event triggered video footages.

Event and Alarm Management

- Camera linkage, alarm pop-up window and multiple linkage actions
- Multiple events for video security, access control, resource group, resource maintenance, etc.
- Supports adding combined alarms in a visualization way



Access Control, Elevator Control, and Video Intercom

- Setting schedules for free access status and access forbidden status of doors or floors
- Supports multiple access modes for both card reader authentication and person authentication
- Supports assigning an access level to persons, assigning access levels to persons, assigning access levels to person groups, and assigning access levels to an access group
- Supports advanced functions such as multi-factor authentication, anti-passback, and multi-door interlocking
- Controlling door or floor status in real-time
- Calling indoor station by the Control Client
- Calling the platform by door station and indoor station, and answering the call by the Control Client

Person and Visitor Management

- Getting person information from added devices
- Provides multiple types of credentials, including card number, face, and fingerprint, for composite authentications
- Visitor registration and check-out

Security Control

- Real-time alarm management for added security control panels
- Adding zone as hot spot on E-map and viewing the video of the linked camera
- Event and alarm linkage with added cameras, including pop-up live view, captured picture
- Subscribing the events that the Control Client can display in real-time
- Acknowledging the received alarm on the Control Client

Time and Attendance

- Setting different attendance rules for various scenarios, such as normal shift and man-hour shift
- Customizing overtime levels and setting corresponding work hour rate
- Supports assigning shift schedule to person group or person(s), or adding temporary schedule
- Supports multiple types of reports according to different needs and sending reports to specified emails regularly

Entrance and Exit Control

- Managing parking lot, entrances and exits, and lanes.
- Supports linking a LED screen with lane for information display
- Setting entry & exit rules for vehicles in the vehicle lists as well as vehicles not in any vehicle lists
- Entrance and exit control based on license plate recognition, card, or video intercom
- Viewing real-time and history vehicle information and controlling barrier gate manually on the Control Client

Temperature Screening

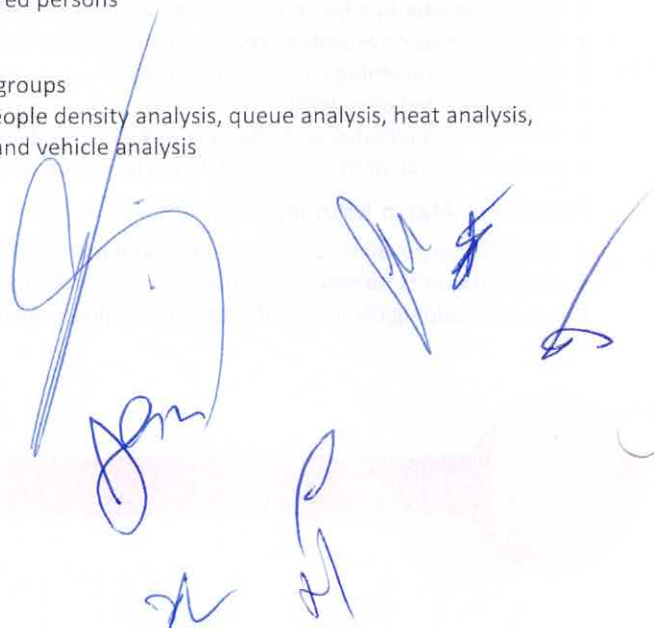
- Displaying the skin-temperature and whether wearing a mask or not about the recognized persons in real time
- Triggering events and alarms when detects abnormal temperature and no mask worn
- Viewing reports about skin-surface temperature and mask-wearing

Face and Body Recognition

- Displaying the information of the recognized persons in real-time
- Searching history records of recognized persons, including searching in captured pictures, searching matched persons, searching by features of persons, and searching frequently appeared persons

Intelligent Analysis

- Supports setting resource groups and analyzing data by different groups
- Supports intelligent analysis reports including people counting, people density analysis, queue analysis, heat analysis, pathway analysis, person feature analysis, temperature analysis, and vehicle analysis
- Displaying the number of people in specified regions in real-time



Digital Signage

- Supports static materials, including picture, video, audio, TXT file, document, static web page, Android APP, etc.
- Supports dynamic materials, including Streaming Server, network camera, URL, etc.
- Supports uploading up to 10,000 material file. Each file size cannot exceed 4 GB
- Creating normal program, attendance program, and people counting & temperature screening program
- Managing up to 2,000 programs. Program's resolution cannot exceed 4K
- Supports creating a loop schedule, customizing a schedule, or creating schedule by day, by week, or by default
- Managing up to 1,000 schedules
- Supports cut-in program, and cut-in message

Third-Party Integration

- Sending the original attendance data to a third-party database (Microsoft® SQL Server, MySQL, PostgreSQL, or Oracle), thus the client can access third-party T&A and payment system

Network Management

- Managing network transmission devices such as switches, displaying the network connection and hierarchical relationship of the managed resources by a topology
- Viewing the network details between the device nodes in the topology, such as downstream and upstream rate, port information, etc. and checking the connection path
- Exporting the topology and abnormal data to check the device connection status and health status

PM 4
Jm

l

9
i

2m

H

Software Specification

The following table shows the maximum performance of the HikCentral Professional server. For other detailed data and performance, refer to *Software Requirements & Hardware Performance*.

	Features	Maximum Performance
Devices and Resources	Cameras	General Performance: 3,000 ^① High Performance: 10,000 ^② High Performance (RSM): 100,000 ^②
	Managed Device IP Addresses <i>*Including Encoding Devices, Access Control Devices, Elevator Control Devices, Security Control Devices, Digital Signage Terminals, and Remote Sites</i>	General Performance: 1,024 ^① High Performance: 2,048 ^②
	Video Intercom Devices	2,048
	Alarm Inputs (Including Zones of Security Control Devices)	3,000
	Alarm Outputs	3,000
	Dock Stations	1,500
	Security Radars and Radar PTZ Cameras	30
	Alarm Inputs of Security Control Devices	2,048
	DS-5600 Series Face Recognition Terminals When Applied with Hikvision Turnstiles	32
	Recording Servers	64
	Streaming Servers	64
	Security Audit Server	8
	DeepinMind Server	64
	ANPR Cameras	3,000
	People Counting Cameras	Recommended: 300
	Heat Map Cameras	Recommended: 70
	Thermal Cameras	Recommended: 20 ^③
	Queue Management Cameras	Recommended: 300
	Digital Signage Terminals	1,024
	Areas	3,000
	Cameras per Area	256
	Alarm Inputs per Area	256
Alarm Outputs per Area	256	
Recording	Recording Schedule	General Performance: 3,000 ^① High Performance: 10,000 ^②
	Recording Schedule Template	200
Event & Alarm	Event and Alarm Rules	General Performance: 3,000 ^① High Performance: 10,000 ^②
	Storage of Events or Alarms without Pictures	General Performance: 100/s ^① High Performance: 1,000/s ^②
	Events or Alarms Sent to Clients <i>*The clients include Control Clients and Mobile Clients.</i>	120/s 100 Clients/s
Picture	Picture Storage <i>*Including event/alarm pictures, face pictures, and vehicle pictures.</i>	20/s (Stored in SYS Server) 80/s (Stored in Recording Server)
Reports	Regular Report Rules	100
	Event or Alarm Rules in One Event/Alarm Report Rule	32
	Records in One Sent Report	10,000 or 10 MB
	Resources Selected in One Report <i>*With this limitation, you can generate a neat and clear report via the Control Client and it costs less time.</i>	20
Data Storage	Data Retention Period	Stored for 3 Years
	People Counting	5 million

	Heat Map	0.25 million
	ANPR	60 million
	Events	60 million
	Alarms	60 million
	Access Records	1.4 billion
	Attendance Records	55 million
	Visitor Records	10 million
	Operation Logs	5 million
	Service Information Logs	5 million
	Service Error Logs	5 million
	Recording Tags	60 million
Users and Roles	Concurrent Accesses via Web Clients, Control Clients, and OpenAPI Clients	100
	Concurrent Accesses via Mobile Clients and OpenAPI Clients	100
	Users	3,000
	Roles	3,000
Vehicle (ANPR)	Vehicle Lists	100
	Vehicles per Vehicle List	5,000
	Under Vehicle Surveillance Systems	4
	Vehicle Undercarriage Pictures	3,000
Entrance & Exit	Lanes	8
	Cards Linked with Vehicles	250,000
	Vehicle Passing Frequency in Each Lane	1 Vehicle/s
Face Comparison	Persons with Profiles for Face Comparison	1,000,000
	Face Comparison Groups	64
	Persons in One Face Comparison Group	1,000,000
Person	Person Group	3,000
	Person Group Hierarchies	10
Access Control	Persons with Credentials for Access Control	50,000
	Visitors	10,000
	Total Credentials (Card + Fingerprint)	250,000
	Cards	250,000
	Fingerprints	200,000
	Profiles	50,000
	Access Points (Doors + Floors)	1,024
	Access Levels	512
Time and Attendance	Persons for Time and Attendance	10,000
	Shift Schedules	128
	Major Leave Types	64
	Minor Leave Types of One Major Type	128
Smart Wall	Decoding Devices	32
	Smart Walls	32
	Views	1,000
	View Groups	100
	Views in One View Group	10
	Cameras in One View	150
	Views Auto-Switched Simultaneously	32
Intelligent Recognition	Resource Groups for Intelligent Recognition	1,000
	Resources in One Group	64
Digital Signage	Materials	10,000
	Programs	2,000
	Schedules	1,000
	Release Records	1,000

Handwritten signatures and initials in blue ink at the bottom of the page.

Streaming Server's Maximum Performance

Video Input Bandwidth per Streaming Server	300 × 2 Mbps
Video Output Bandwidth per Streaming Server	300 × 2 Mbps

- ①: The general performance requires Intel® Xeon® E3-1220 or higher.
②: The high performance requires Intel® Xeon® E5-2620 or higher.
③: This recommended value refers to the number of thermal cameras connected to the system directly. It depends on the maximum performance (data processing and storage) in the situation when the managed thermal cameras uploading temperature data to the system. For thermal cameras connected to the system via NVR, there is no such limitation.

[Handwritten signatures and marks in blue ink]

Hardware Specification



Processor	Intel® Xeon® E-2124	
Memory	16G DDR4 DIMM slots, Supports UDIMM, up to 2666 MT/s, 64GB Max. Supports registered ECC	
Storage Controllers	Internal Controllers: SAS_H330 Software RAID: PERC S140 External HBAs: 12Gbps SAS HBA (non-RAID) Boot Optimized Storage Subsystem: 2x M.2 240GB (RAID 1 or No RAID), 1x M.2 240GB (No RAID Only)	
Drive Bays	1T 7.2K SATA×2	
Power Supplies	Single 250W (Bronze) power supply	
Dimensions	Form Factor: Rack (1U) Chassis Width: 434.00mm (17.08 in) Chassis Depth: 595.63mm (23.45 in) (3.5"HHD) Note: These dimensions do not include: bezel, redundant PSU	
Dimensions with Package (W × D × H)	750 mm × 614 mm × 259 mm (29.53" × 24.17" × 10.2")	
Net Weight	12.2 kg	
Weight with Package	18.5 kg	
Embedded NIC	2 x 1GbE LOM Network Interface Controller (NIC) ports	
Device Access	Front Ports: 1x USB 2.0, 1 x iDRAC micro USB 2.0 management port Rear Ports: 2 x USB 3.0, VGA, serial connector	
Embedded Management	iDRAC9 with Lifecycle Controller iDRAC Direct DRAC RESTful API with Redfish	
Integrations and Connections	Integrations: Microsoft® System Center VMware® vCenter™ BMC Truesight (available from BMC) Red Hat Ansible	Connections: Nagios Core & Nagios XI Micro Focus Operations Manager i (OMi) IBM Tivoli Netcool/OMNibus
Operating Systems	Certify XenServer Citrix® XenServer® Microsoft Windows Server® with Hyper-V Red Hat® Enterprise Linux Ubuntu Server This model is installed with Microsoft Windows Server® 2016 multilingual operating system.	SUSE® Linux Enterprise Server VMware® ESXi

Handwritten signatures and scribbles in blue ink are present at the bottom right of the page, overlapping the bottom of the table and extending into the margin.

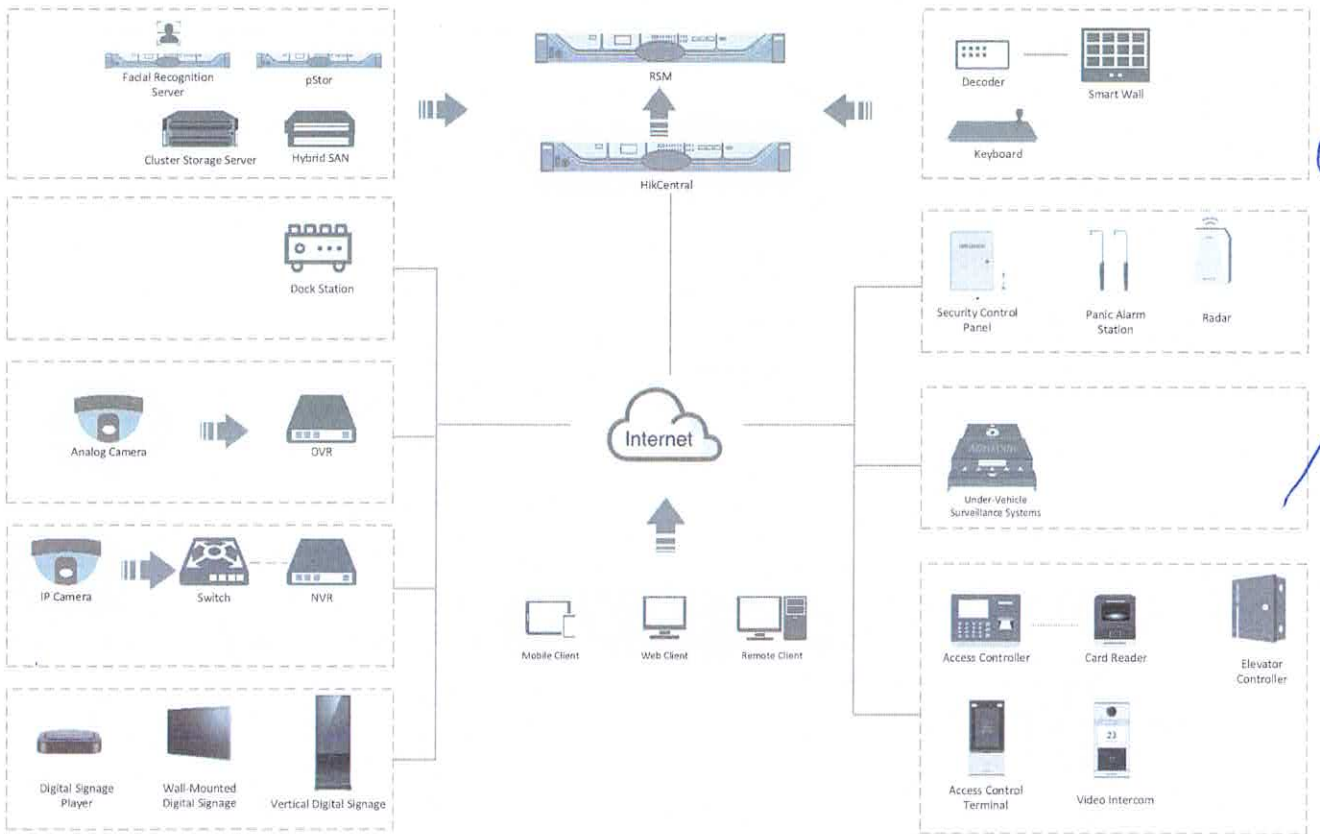
System Requirement

* For high stability and good performance, the following system requirements must be met.

Feature	Description
OS for HikCentral Professional Server	Microsoft® Windows 7 SP1 (64-bit) Microsoft® Windows 8.1 (64-bit) Microsoft® Windows 10 (64-bit) Microsoft® Windows Server 2008 R2 SP1 (64-bit) Microsoft® Windows Server 2012 (64-bit) Microsoft® Windows Server 2012 R2 (64-bit) Microsoft® Windows Server 2016 (64-bit) Microsoft® Windows Server 2019 (64-bit) <i>*For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) updated in April, 2014.</i>
OS for Control Client	Microsoft® Windows 7 SP1 (32/64-bit) Microsoft® Windows 8.1 (32/64-bit) Microsoft® Windows 10 (64-bit) Microsoft® Windows Server 2008 R2 SP1 (64-bit) Microsoft® Windows Server 2012 (64-bit) Microsoft® Windows Server 2012 R2 (64-bit) Microsoft® Windows Server 2016 (64-bit) Microsoft® Windows Server 2019 (64-bit) <i>*For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) updated in April, 2014.</i>
OS for Visitor Terminal	Android 7.1 and later
Browser Version	Internet Explorer 11 and above Chrome 61 and above Firefox 57 and above Safari 11 and above (running on Mac OS X 10.3/10.4)
Database	PostgreSQL V11.8
OS for Smartphone	iOS 10.0 and later Android phone OS version 5.0 or later, and dual-core CPU with 1.5 GHz or above, and at least 2G RAM
OS for Tablet	iOS 10.0 and later Android tablet with Android OS version 5.0 and later
Virtual Machine	VMware® ESXi™ 6.x Microsoft® Hyper-V with Windows Server 2012/2012 R2/2016 (64-bit) <i>*The Streaming Server and Control Client cannot run on the virtual machine.</i> <i>*Virtual server migration is not supported.</i>

Handwritten blue ink signatures and scribbles are present at the bottom of the page, including a large signature on the left and several smaller ones on the right.

Typical Application



[Handwritten signatures and scribbles in blue ink]

Distributed by

HIKVISION

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

Hikvision USA
T +1-909-895-0400
sales.usa@hikvision.com

Hikvision Australia
T +61-2-8599-4233
salesau@hikvision.com

Hikvision India
T +91-22-28469000
sales@pramahikvision.com

Hikvision Canada
T +1-866-200-6690
sales.canada@hikvision.com

Hikvision Thailand
T +662-275-9949
sales.thailand@hikvision.com

Hikvision Europe
T +31-23-5542770
sales.eu@hikvision.com

Hikvision Italy
T +39-0438-6902
info.it@hikvision.com

Hikvision Brazil
T +55 11 3318-0050
Latam.support@hikvision.com

Hikvision Turkey
T +90 (216)521 7070- 7074
sales.tr@hikvision.com

Hikvision Malaysia
T +601-7652-2413
sales.my@hikvision.com

Hikvision UK & Ireland
T +01628-902140
sales.uk@hikvision.com

Hikvision South Africa
Tel: +27 (0) 0351172
sate.africa@hikvision.com

Hikvision France
T +33(0)1-85-330-450
info.fr@hikvision.com

Hikvision Kazakhstan
T +7-727-9730667
nikia.panfilov@hikvision.ru

Hikvision Vietnam
T +84-974270888
sales.vi@hikvision.com

Hikvision UAE
T +971-4-4432090
salesme@hikvision.com

Hikvision Singapore
T +65-6684-4718
sg@hikvision.com

Hikvision Spain
T +34-91-737-16-55
info.es@hikvision.com

Hikvision Tashkent
T +99-67-1238-9438
uzb@hikvision.ru

Hikvision Hong Kong
T +852-2151-1761
info.hk@hikvision.com

Hikvision Russia
T +7-495-669-67-99
saleru@hikvision.com

Hikvision Korea
T +82-10131-731-8817
sales.korea@hikvision.com

Hikvision Poland
T +48-22-460-01-50
info.pl@hikvision.com

Hikvision Indonesia
T +62-21-2933759
Sales.Indonesia@hikvision.com

Hikvision Colombia
sales.colombia@hikvision.com

XNB 1440

Nobreak interativo monovolt



- » Ideal para eletrônicos simples
- » 1440 VA / 720 W
- » Monovolt: 120 V ou 220 V
- » 6 tomadas de saída
- » 2 baterias de 12 V 7 Ah
- » 6 níveis de proteção
- » Religamento automático

Especificações técnicas

Modelo	XNB 1440 VA 120V	XNB 1440 VA 220V
Potência nominal de pico	1440 VA / 720 W	1440 VA / 720 W
Topologia	Interativo	Interativo
Entrada		
Tensão nominal de entrada	120 V~	220 V~
Variação da tensão	90-145 V~	165-265 V~
Frequência	60 Hz	60 Hz
Disjuntor	15 A	10 A
Cabo de força	Cabo de 1,2 m com plugue tripolar de acordo com a norma NBR 14136	Cabo de 1,2 m com plugue tripolar de acordo com a norma NBR 14136
Saída		
Fator de potência	0,5	0,5
Tensão nominal de saída*	120 V~	220 V~
Regulação da tensão	Modo Rede: 120V~ ±10% Modo Bateria: 120V~ ±5%	Modo Rede: 220V~ ±10% Modo Bateria: 220V~ ±5%
Tempo de transferência	<10 ms	<10 ms
Frequência no Modo Bateria	50 / 60 Hz ±1 Hz	50 / 60 Hz ±1 Hz
Forma de onda no modo Bateria	Semissenoidal (retangular)	Semissenoidal (retangular)
Tomada (NBR 14136)	6 tomadas de 10 A	6 tomadas de 10 A

Proteções

Proteção contra sub/sobretensão	Passa a operar no modo <i>Bateria</i>	Passa a operar no modo <i>Bateria</i>
Proteção contra descarga da(s) bateria(s)	Até 21 V	Até 21 V
Proteção contra sobrecarga na saída	Modo <i>Rede</i> : fusível rearmável Modo <i>Bateria</i> : limitador de corrente interno	Modo <i>Rede</i> : fusível rearmável Modo <i>Bateria</i> : limitador de corrente interno

Baterias

Bateria interna	Selada chumbo-ácido (VRLA)	Selada chumbo-ácido (VRLA)
Quantidade e capacidade	2 x 12 V 7 Ah	2 x 12 V 7 Ah
Conector para bateria(s) externa(s)	-	-
Expansão para bateria(s) externa(s)	-	-
Cabo conexão bateria(s) externa(s)	-	-
Barramento	24 V	24 V
Corrente de carga	1 A	1 A
Tempo de carga sem bateria externa	10 h	10 h

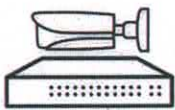
Físico

Dimensões (L x A x P)	149 x 162 x 353 mm	149 x 162 x 353 mm
Peso	8,67 kg	8,67 kg
Temperatura de operação	0-40 °C	0-40 °C
Umidade ambiente	0-90% (sem condensação)	0-90% (sem condensação)

*Utilize um multímetro com função True RMS para medir a tensão de saída do modo *Bateria*.

Atenção: o nobreak não deve ser utilizado para alimentar computadores dotados de fontes com função PFC ativo, equipamentos de sustentação à vida ou movidos a motor, como ventiladores, geladeiras, liquidificadores, micro-ondas, impressoras a laser, entre outros. Antes de utilizar os nobreaks Intelbras, leia o manual do usuário e as informações das etiquetas dos produtos e verifique se o modelo é adequado a sua aplicação.

Cenário de aplicação: ideal para eletrônicos simples.



Sistema de segurança CFTV



Computador desktop



Televisor e Monitor



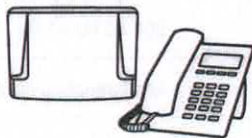
Roteador e Switch



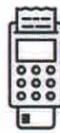
Controle de acesso



Impressora jato de tinta



Central Telefônica e Telefone



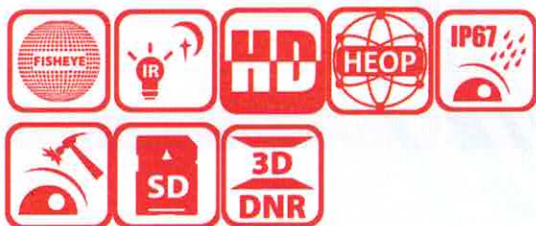
Caixa registradora e Máq. cartão (PDV)



Home theater

DS-2CD63C5G1-IVS(C)

12 MP DeepinView IR Network Fisheye Camera

DeepinView^{series}IMMERVISION
enables*

DS-2CD63C5G1-IVS (C) is a fisheye network camera capable of providing a 360-degree panoramic image of its scene. The progressive scan CMOS sensor provides high-resolution images of up to 4000 × 3000. Up to 20 live view display modes, designed for 3 mount types, meet various user preferences. Three independently controlled IR lights offer a range of 15 m and provide good vision in low or even zero-light environment.

- Heatmap: based on deep learning algorithms, the camera counts people and presents an intuitive map
- Multi dewarping modes: the image can be dewarped to normal image for viewing intuitively
- Built-in mic and speaker: the camera supports two-way audio for real-time audio security monitoring and communication
- Built-in IR light: an IR range of 15 meters provides good visibility in low or even zero-light environments
- High resolution 12 MP: capturing clear images even when dewarped into 4-image PTZ mode
- Each image is clear and detailed
- Panomorph lens RPL: 89VVT
- Water and dust resistant (IP67) and vandal resistant (IK10)

▪ Specification

Camera	
Image Sensor	1/1.7" Progressive Scan CMOS
Max. Resolution	4000 × 3000
Min. Illumination	Color: 0.01 Lux @ (F2.2, AGC ON), B/W: 0.006 Lux @ (F2.2, AGC ON), B/W: 0 Lux with IR
Shutter Time	1 s to 1/100,000 s
Day & Night	IR cut filter
Lens	
Lens Type	Fixed focal lens, 1.29 mm
Focal Length & FOV	1.29 mm, horizontal FOV 180°, vertical FOV 180°
Iris Type	Fixed
Aperture	F2.2
Depth of Field	0.2 m to ∞
DORI	
DORI	D: 27.9 m O: 11.1 m R: 5.6 m I: 2.8 m
Illuminator	
Supplement Light Type	IR
Supplement Light Range	Up to 15 m
Supplement Light Number	3
Smart Supplement Light	Yes
IR Wavelength	850 nm
HEOP	
Open Resources	Memory: 60 MB, Smart RAM: 800 MB, eMMC: 2 GB
Computing Power	2 TOPS
Open Capability	HEOP 2.0 OpendevSDK
Deep Learning Structure	Caffe, TensorFlow, PyTorch
Programming Language	C, C++

Handwritten signatures and initials in blue ink, including a large signature and the initials 'AM' and 'AI'.

Video	
Main Stream	50 Hz: 25 fps/60 Hz: 30 fps: Fisheye View: 3504 × 3504, 3024 × 3024, 2560 × 2560, 2048 × 2048 180 Panorama View: 3072 × 2304, 2048 × 1536 180 Dual Channel Panorama View: 3072 × 1152 Panorama View: 3072 × 2304, 2048 × 1536 4PTZ View: camera 01/camera 02/camera 03/camera 04: 1600 × 1200 Fisheye + 3PTZ View: camera 01: 2560 × 2560, 2048 × 2048, 1280 × 1280 camera 02/camera 03/camera 04: 1600 × 1200 4PTZ Fusion View: 3200 × 2400, 2048 × 1536
Sub-Stream	50 Hz: 25 fps/60 Hz: 30 fps: Fisheye View: 720 × 720, 480 × 480 180 Panorama View: 640 × 480, 320 × 240 180 Dual Channel Panorama View: 640 × 480, 320 × 240 Panorama View: 640 × 360, 320 × 240 4PTZ View: camera 01/camera 02/camera 03/camera 04: 640 × 480, 320 × 240 Fisheye + 3PTZ View: camera 01: 720 × 720 camera 02/camera 03/camera 04: 640 × 480, 320 × 240
Third Stream	50 Hz: 25 fps (1920 × 1080, 1280 × 720, 704 × 576, 640 × 480) 60 Hz: 30 fps (1920 × 1080, 1280 × 720, 704 × 480, 640 × 480)
Video Compression	Main stream: H.265+/H.265/H.264+/ H.264, Sub-stream: H.265/H.264/MJPEG, Third Stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 16 Mbps
H.264 Type	Baseline Profile, Main Profile, High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR, VBR
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	4 fixed regions for each stream
Fisheye Display	
Mount Type	Support wall/table/ceiling mounting
Decoding Mode	Support hardware decoding and software decoding

Handwritten signatures and scribbles in blue ink at the bottom right of the page.

Display Mode	20 display modes in total, Software decoding: fisheye view, 180 panorama view, 360 panorama view, 360 panorama + PTZ, 360 panorama + 3PTZ, 360 panorama + 6PTZ, 360 panorama + 8PTZ, 2PTZ, 4PTZ, fisheye + 3PTZ, fisheye + 8PTZ, hemisphere, AR hemisphere, cylinder, Hardware decoding: fisheye view, 180 panorama view, 180 dual channel panorama, panorama view, 4PTZ, fisheye + 3PTZ, 4PTZ fusion
Audio	
Audio Compression	G.711/G.722.1/G.726/MP2L2/PCM/MP3/AAC-LC
Audio Bit Rate	64 Kbps (G.711ulaw/G.711alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 192 Kbps (MP2L2)/8 to 320 Kbps (MP3)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	8 kHz/16 kHz/32 kHz/48 kHz
Environment Noise Filtering	Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, HTTPS, Filter IP, FTP, SFTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv4, IPv6, UDP, Bonjour, SSL/TLS, ISUP, ARP, WebSocket, WebSockets, SIP
Simultaneous Live View	Up to 20 channels
API	Open Network Video Interface (Profile S, Profile G, Profile T), ISAPI, SDK, ISUP, Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, peer to peer or integrated with SIP/PBX
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Security	Password protection, complicated password, HTTPS encryption, 802.1X authentication (EAP-TLS, EAP-LEAP, EAP-MD5), watermark, IP address filter, basic and digest authentication for HTTP/HTTPS, Protocol DDoS and Phishing, WSSE and digest authentication for Open Network Video Interface, RTP/RTSP over HTTPS, control timeout settings, security audit log, TLS 1.2, host authentication (MAC address)
Network Storage	NAS (NFS, SMB/CIFS), Auto Network Replenishment (ANR), Together with high-end Hikvision memory card, memory card encryption and health detection are supported.
Client	iVMS-4200, iVMS-4500, iVMS-5200, Hik-Connect
Web Browser	Plug-in required live view: IE 10, IE 11, Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Edge 89+, Safari 11+, Local service: Chrome 57.0+, Firefox 52.0+, Edge 89+
Image	
Image Parameters Switch	Yes
Image Settings	saturation, brightness, contrast, sharpness, white balance, AGC, adjustable by client software or web browser
Day/Night Switch	Day, Night, Auto, Schedule, Alarm Trigger
Wide Dynamic Range (WDR)	Digital WDR
Image Enhancement	BLC, HLC, 3D DNR, Distortion Correction, Defog
Privacy Mask	8 programmable polygon privacy masks
Picture Overlay	LOGO picture can be overlaid on video with 128 × 128 24 bit bmp format.
Interface	
Ethernet Interface	1 RJ45 10 M/100 M/1000 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 256 GB

Built-in Microphone	Yes, 4 built-in microphones
Built-in Speaker	Yes, 1 built-in speaker
Audio	1 input (line in), 3.5 mm connector, max. input amplitude: 3.3 Vpp, input impedance: 4.7 K Ω , interface type: non-equilibrium, 1 output (line out), 3.5 mm connector, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω , interface type: non-equilibrium
Alarm	2 inputs, 2 outputs (max. 24 VDC, 1 A)
RS-485	1 RS-485 (Half duplex, HIKVISION, Pelco-P, Pelco-D, self-adaptive)
Reset Key	1 Reset Key
Event	
Basic Event	Motion detection, video tampering alarm, alarm input and output, exception (network disconnected, IP address conflict, illegal login, HDD full, HDD error)
Smart Event	Line crossing detection, intrusion detection, region entrance detection, region exiting detection, scene change detection, audio exception detection, defocus detection, unattended baggage detection, object removal detection
Linkage	Upload to FTP/NAS/memory card, notify surveillance center, send email, trigger alarm output, trigger recording, trigger capture
Deep Learning Function	
People Counting	Counts people entering, exiting and passing by separately (The data is stored in the flash.) Supports real-time uploading and uploading by statistic cycle Sends email reports on daily, weekly, monthly or annually basis Supports up to 3 detection regions, and independent arming schedule and linkage method
Queue Management	Supports up to 8 detection regions, and independent arming schedule and linkage method Supports 2 detection modes: regional people queuing-up, waiting time detection Generates reports to compare the efficiency of different queuing-ups and display the changing status of one queue Supports raw data export for further analysis Supports real-time data uploading and scheduled data uploading Regional people queuing-up: supports 4 alarm trigger conditions, including greater than threshold, less than threshold, equal to threshold, not equal to threshold Waiting time detection: supports 1 alarm trigger condition, including greater than threshold
Heat Map	A graphic description of visits (by calculating amount of people or amount of dwell time) in a configured area., Two report types are available, space heat map and time heat map line chart.
Intersection Analysis	Detects and analyze flow in an intersection-like scene, and generate reports Support one intersection of up to 10 ways
General	
Power	12 VDC \pm 20%, 1 A, max. 11.5 W, two-core terminal block, PoE: IEEE 802.3af, Class 3, max. 12.5 W
Material	Metal
Dimension	\varnothing 140.3 mm \times 59.4 mm (\varnothing 5.5" \times 2.3")
Package Dimension	260 mm \times 230 mm \times 135 mm (10.2" \times 9.1" \times 5.3")

Weight	Approx. 715 g (1.58 lb.)
With Package Weight	Approx. 1206 g (2.66 lb.)
Storage Conditions	-40 °C to 60 °C (-40 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-40 °C to 60 °C (-40 °F to 140 °F). Humidity 95% or less (non-condensing)
Language	33 languages: English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian
General Function	Heartbeat, flash log, password reset via email, password protection, one-key reset, anti-banding
Heater	Yes
Cable Length	0.31 m (1.02 ft.)
Approval	
EMC	CE-EMC: EN 55032:2015+A1:2020, EN 50130-4:2011+A1:2014, EN IEC 61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:2019+A2:2021, EN 50121-4: 2016+A1:2019, RCM: AS/NZS CISPR 32: 2015, IC: ICES-003: Issue 7, KC: KN32: 2015, KN35: 2015
Safety	UL: UL 62368-1, CB: IEC 62368-1: 2014+A11, CE-LVD: EN 62368-1: 2014/A11: 2017, BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005
Environment	CE-RoHS: 2011/65/EU, WEEE: 2012/19/EU, Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013, IK10: IEC 62262:2002

▪ Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

This model has NO SPECIFIC PROTECTION.

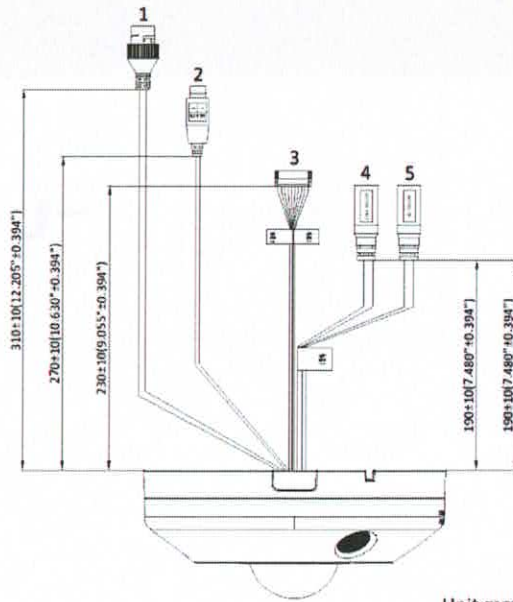
Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Physical Interface

No.	Interface Description
1	Network Interface
2	Power Interface
3	Alarm Interface, RS-485

[Handwritten signatures and marks]

4	Audio Output Interface
5	Audio Input Interface

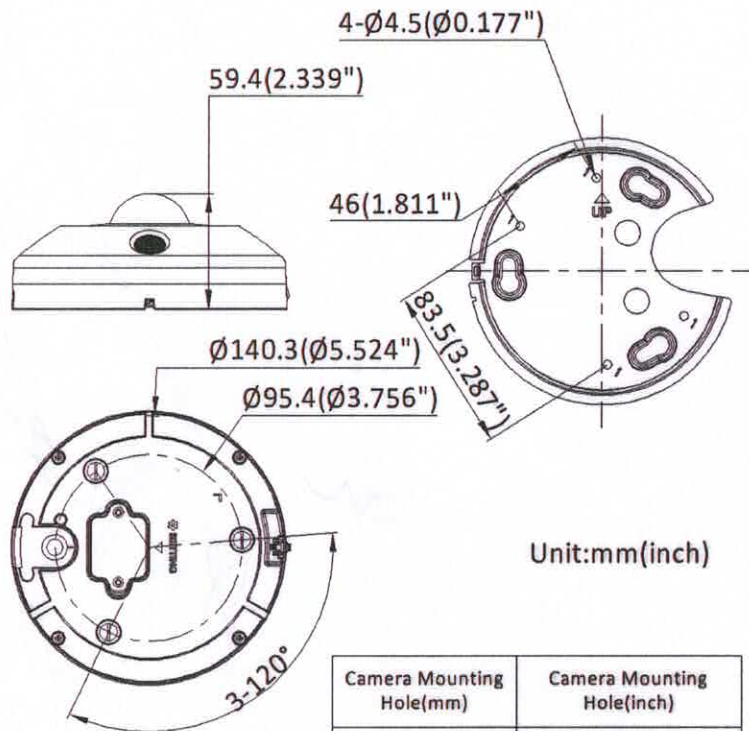


Unit:mm(inch)

▪ Available Model

DS-2CD63C5G1-IVS(C)(1.29mm)

▪ Dimension



Unit:mm(inch)

Camera Mounting Hole(mm)	Camera Mounting Hole(inch)
4xØ4.5	4xØ0.177"

Handwritten signatures and scribbles in blue ink.

▪ Accessory

▪ Optional

DS-1276ZJ-SUS Corner Mount	DS-2280ZJ-WA140 Junction Box	DS-1275ZJ-SUS Vertical Pole Mount	DS-1273ZJ-140B Wall Mount	DS-1273ZJ-140 Wall Mount
				
DS-1271ZJ-140 Pendant Mount				
				

*It is recommended to use DS-1276ZJ-SUS and DS-1275ZJ-SUS with DS-1273ZJ-140 or DS-1273ZJ-140B.

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq



Handwritten signatures and initials in blue ink.

DS-2CD1127G2-L(C)(UF) 2 MP ColorVu Fixed Dome Network Camera

ColorVu



Hikvision ColorVu technology provides 24/7 vivid colorful images with F1.0 advanced lenses and high performance sensors. F1.0 super-aperture collects more light to produce brighter images. Advanced sensor technology can vastly improve the utilization of available light.

- High quality imaging with 2 MP resolution, RAM memory 128MB
- 24/7 colorful imaging
- Support Human and Vehicle Detection
- Water and dust resistant (IP67) and vandal resistant (IK08)
- Efficient H.265+ compression technology
- Support on-board storage up to 256GB (SD card slot) (Optional)
- Built-in microphone for real-time audio security (Optional)

▪ Specification

Camera	
Image Sensor	1/2.7" Progressive Scan CMOS
Max. Resolution	1920 × 1080
Min. Illumination	Color: 0.001 Lux @ (F1.0, AGC ON), 0 Lux with light
Shutter Time	1/3 s to 1/100,000 s
Day & Night	24/7 color imaging
Angle Adjustment	Pan: 0° to 355°, tilt: 0° to 75°, rotate: 0° to 355°
Lens	
Lens Type	Fixed focal lens, 2.8 and 4 mm optional
Focal Length & FOV	2.8 mm, horizontal FOV: 111°, vertical FOV: 57°, diagonal FOV: 126° 4 mm, horizontal FOV: 83°, vertical FOV: 44°, diagonal FOV: 99°
Lens Mount	M12
Iris Type	Fixed
Aperture	F1.0
Depth of Field	2.8 mm: 1.5 m to ∞ 4 mm: 2.1 m to ∞
DORI	
DORI	2.8 mm, D: 44 m, O: 17 m, R: 8 m, I: 4 m 4 mm, D: 56 m, O: 22 m, R: 11 m, I: 5 m
Illuminator	
Supplement Light Type	White Light
Supplement Light Range	Up to 30 m
Smart Supplement Light	Yes
Video	
Main Stream	50 Hz: 25 fps (1920 × 1080, 1280 × 720) 60 Hz: 30 fps (1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (640 × 480, 640 × 360) 60 Hz: 30 fps (640 × 480, 640 × 360)
Video Compression	Main stream: H.265+/H.265/H.264+/H.264 Sub-stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 8 Mbps
H.264 Type	Baseline Profile, Main Profile, High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR, VBR
Region of Interest (ROI)	1 fixed region(s) for main stream
Audio	
Audio Type	-U: Mono sound
Audio Compression	-U: G.711ulaw/G.711alaw/G.722.1/G.726/MP2L2/PCM/AAC-LC
Audio Bit Rate	-U: 64 Kbps (G.711 ulaw)/64 Kbps (G.711 alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 160 Kbps (MP2L2)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	-U: 8 kHz/16 kHz
Environment Noise Filtering	-U: Yes

Network	
Security	Password protection, complicated password, watermark, basic and digest authentication for HTTP, WSSE and digest authentication for Open Network Video Interface, security audit log, host authentication (MAC address)
Simultaneous Live View	Up to 6 channels
API	Open Network Video Interface (Profile S, Profile T, Profile G (only -U model supports)), ISAPI, SDK
Protocols	TCP/IP, ICMP, DHCP, DNS, HTTP, RTP, RTSP, NTP, IGMP, IPv6, UDP, QoS, FTP, SMTP
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Client	iVMS-4200, Hik-Connect
Web Browser	Plug-in required live view: IE 10, IE 11 Local service: Chrome 57.0+, Firefox 52.0+
Image	
Wide Dynamic Range (WDR)	120 dB WDR
SNR	≥ 52 dB
Day/Night Switch	Day, Night, Auto, Schedule
Image Enhancement	BLC, HLC, 3D DNR
Image Settings	Rotate mode, saturation, brightness, contrast, sharpness, gain, white balance, adjustable by client software or web browser
Privacy Mask	4 programmable polygon privacy masks
Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 256 GB
Built-in Microphone	-U: Yes
Reset Key	-F: Yes
Event	
Basic Event	Motion detection (support alarm triggering by specified target types (human and vehicle)), video tampering alarm, exception
Linkage	Upload to FTP/memory card (-F), notify surveillance center, send email, trigger recording (-F), trigger capture
General	
Power	12 VDC ± 25%, 0.4 A, max. 5 W, Ø5.5 mm coaxial power plug PoE: 802.3af, Class 3, 36 V to 57 V, 0.2 A to 0.15 A, max. 6.5 W
Material	Base: aluminum alloy, cover: plastic
Dimension	Ø121.5 mm × 97.6 mm (Ø4.8" × 3.8")
Package Dimension	150 mm × 150 mm × 141 mm (5.9" × 5.9" × 5.6")
Weight	Approx. 500 g (1.1 lb.)
With Package Weight	Approx. 700 g (1.5 lb.)
Storage Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Language	English, Ukrainian
General Function	Heartbeat, anti-banding, mirror, password protection, password reset via email

Approval	
EMC	FCC: 47 CFR Part 15, Subpart B CE-EMC: EN 55032: 2015, EN 61000-3-2: 2019, EN 61000-3-3: 2013 + A1: 2019, EN 50130-4: 2011 + A1: 2014 RCM: AS/NZS CISPR 32: 2015 KC: KN32: 2015, KN35: 2015
Safety	UL: UL 62368-1 CB: IEC 62368-1: 2014 + A11 CE-LVD: EN 62368-1: 2014/A11: 2017 BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005
Environment	CE-RoHS: 2011/65/EU WEEE: 2012/19/EU Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013 IK08: IEC 62262:2002

▪ Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

This model has NO SPECIFIC PROTECTION.

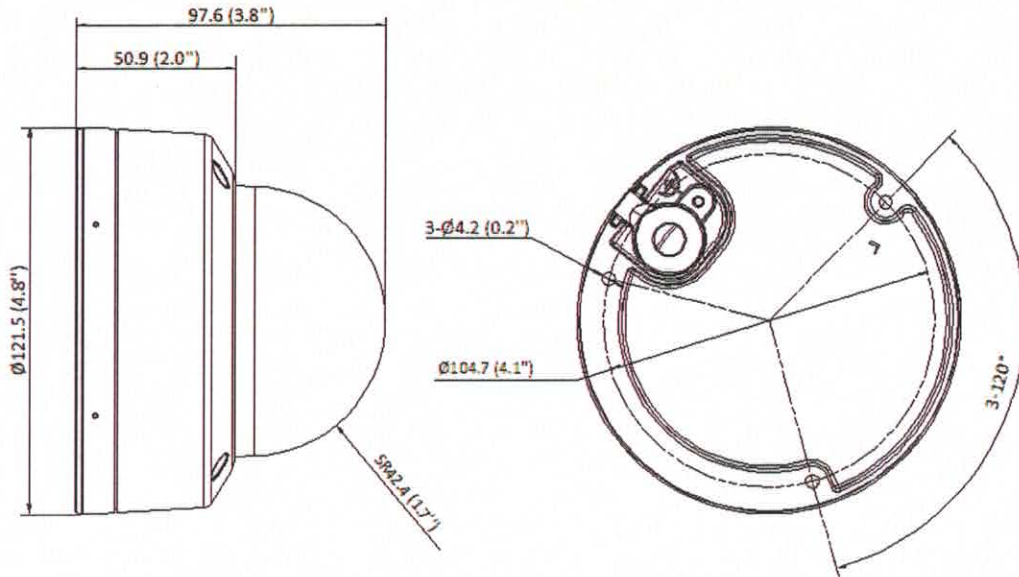
Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Available Model

DS-2CD1127G2-L (C)(2.8/4 mm)

DS-2CD1127G2-LUF(C) (2.8/4 mm)

▪ Dimension



Unit: mm (inch)

▪ Accessory

▪ Optional

DS-1272ZJ-120B Wall Mount	DS-1272ZJ-120 Wall Mount	DS-1253ZJ-M Rain Shade	DS-1275ZJ-SUS Vertical Pole Mount	DS-1271ZJ-120 Pendant Mount
DS-1280ZJ-DM46 Junction Box				

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq



DS-2CD1027G2-L(UF)(C)
2 MP ColorVu Fixed Bullet Network Camera

ColorVu



Hikvision ColorVu technology provides 24/7 vivid colorful images with F1.0 advanced lenses and high performance sensors. F1.0 super-aperture collects more light to produce brighter images. Advanced sensor technology can vastly improve the utilization of available light.

- High quality imaging with 2 MP resolution
- 24/7 colorful imaging
- Support Human and Vehicle Detection
- Water and dust resistant (IP67)
- Efficient H.265+ compression technology
- Support on-board storage up to 256GB (SD card slot) (Optional)
- Built-in microphone for real-time audio security (Optional)

Handwritten signatures and scribbles in blue ink.

▪ Specification

Camera	
Image Sensor	1/2.7" Progressive Scan CMOS
Max. Resolution	1920 × 1080
Min. Illumination	Color: 0.001 Lux @ (F1.0, AGC ON), 0 Lux with light
Shutter Time	1/3 s to 1/100,000 s
Day & Night	24/7 color imaging
Angle Adjustment	Pan: 0° to 360°, tilt: 0° to 90°, rotate: 0° to 360°
Lens	
Lens Type	Fixed focal lens, 2.8 and 4 mm optional
Focal Length & FOV	2.8 mm, horizontal FOV: 111°, vertical FOV: 57°, diagonal FOV: 126° 4 mm, horizontal FOV: 83°, vertical FOV: 44°, diagonal FOV: 99°
Lens Mount	M12
Iris Type	Fixed
Aperture	F1.0
Depth of Field	2.8 mm: 1.5 m to ∞ 4 mm: 2.1 m to ∞
DORI	
DORI	2.8 mm, D: 44 m, O: 17 m, R: 8 m, I: 4 m 4 mm, D: 56 m, O: 22 m, R: 11 m, I: 5 m
Illuminator	
Supplement Light Type	White Light
Supplement Light Range	Up to 30 m
Smart Supplement Light	Yes
Video	
Main Stream	50 Hz: 25 fps (1920 × 1080, 1280 × 720) 60 Hz: 30 fps (1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (640 × 480, 640 × 360) 60 Hz: 30 fps (640 × 480, 640 × 360)
Video Compression	Main stream: H.265+/H.265/H.264+/H.264, Sub-stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 8 Mbps
H.264 Type	Baseline Profile, Main Profile, High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR, VBR
Region of Interest (ROI)	1 fixed region(s) for main stream
Audio	
Audio Type	-U: Mono sound
Environment Noise Filtering	-U: Yes
Audio Sampling Rate	-U: 8 kHz/16 kHz
Audio Compression	-U: G.711ulaw/G.711alaw/G.722.1/G.726/MP2L2/PCM/AAC-LC
Audio Bit Rate	-U: 64 Kbps (G.711 ulaw)/64 Kbps (G.711 alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 160 Kbps (MP2L2)/16 to 64 Kbps (AAC-LC)
Network	
Protocols	TCP/IP, ICMP, DHCP, DNS, HTTP, RTP, RTSP, NTP, IGMP, IPv6, UDP, QoS, FTP, SMTP
Simultaneous Live View	Up to 6 channels

API	Open Network Video Interface (Profile S, Profile T, Profile G (only -U model supports)), ISAPI, SDK
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Security	Password protection, complicated password, watermark, basic and digest authentication for HTTP, Protocol DDoS and Phishing, WSSE and digest authentication for Open Network Video Interface, security audit log, host authentication (MAC address)
Client	iVMS-4200, Hik-Connect
Web Browser	Plug-in required live view: IE 10, IE 11 Local service: Chrome 57.0+, Firefox 52.0+
Image	
Wide Dynamic Range (WDR)	DWDR
SNR	≥ 52 dB
Day/Night Switch	Day, Night, Auto, Schedule
Image Enhancement	BLC, HLC, 3D DNR
Image Settings	Rotate mode, saturation, brightness, contrast, sharpness, gain, white balance, adjustable by client software or web browser
Privacy Mask	4 programmable polygon privacy masks
Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	-F: Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 256 GB
Built-in Microphone	-U: Yes
Reset Key	-F: Yes
Event	
Basic Event	Motion detection (support alarm triggering by specified target types (human and vehicle)), video tampering alarm, exception
Linkage	Upload to FTP/memory card (-F), notify surveillance center, send email, trigger recording (-F), trigger capture
General	
Power	12 VDC ± 25%, 0.4 A, max. 5 W, Ø5.5 mm coaxial power plug PoE: 802.3af, Class 3, 36 V to 57 V, 0.2 A to 0.15 A, max. 6.5 W
Material	Aluminum alloy body
Dimension	Ø76.6 mm × 164.4 mm (Ø3" × 6.5")
Package Dimension	234 mm × 120 mm × 117 mm (9.2" × 4.7" × 4.6")
Weight	-L: Approx. 405 g (0.9 lb.) -LUF: Approx. 425 g (0.9 lb.)
With Package Weight	-L: Approx. 630 g (1.4 lb.) -LUF: Approx. 650 g (1.4 lb.)
Storage Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Language	English, Ukrainian
General Function	Heartbeat, anti-banding, mirror, password protection, password reset via email

Approval	
EMC	FCC: 47 CFR Part 15, Subpart B CE-EMC: EN 55032: 2015, EN 61000-3-2: 2019, EN 61000-3-3: 2013 + A1: 2019, EN 50130-4: 2011 + A1: 2014 RCM: AS/NZS CISPR 32: 2015 KC: KN32: 2015, KN35: 2015
Safety	UL: UL 62368-1 CB: IEC 62368-1: 2014 + A11 CE-LVD: EN 62368-1: 2014/A11: 2017 BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005
Environment	CE-RoHS: 2011/65/EU WEEE: 2012/19/EU Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013

▪ **Typical Application**

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

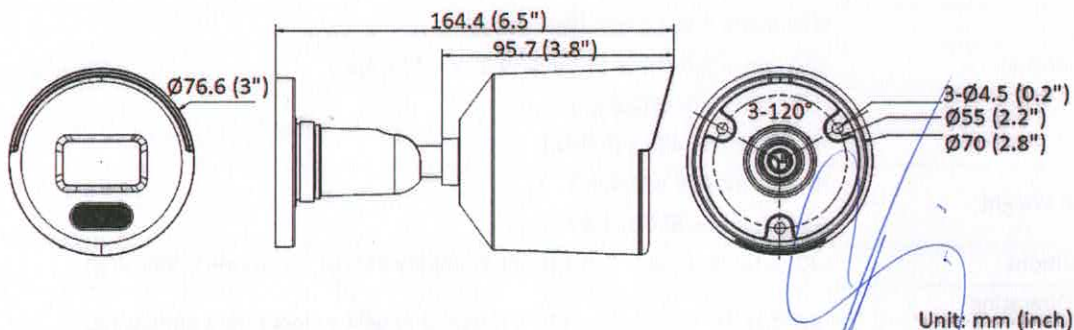
This model has NO SPECIFIC PROTECTION.

Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ **Available Model**

- DS-2CD1027G2-L(C)(2.8/4 mm)
- DS-2CD1027G2-LUF(C)(2.8/4 mm)

▪ **Dimension**



▪ Accessory

▪ Optional



EM BRANCO

Handwritten signature

Headquarters

No.555 Dianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.



Handwritten signature

iDS-7716NXI-M4/16P/X DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16-ch@4 MP decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 16-ch IP cameras can be connected, plug & play with .6 power-over-Ethernet (PoE) interfaces
- Intelligent analytics based on deep learning algorithm
- Up to 16-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 16-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability
- System Embedded Linux System

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 4 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm

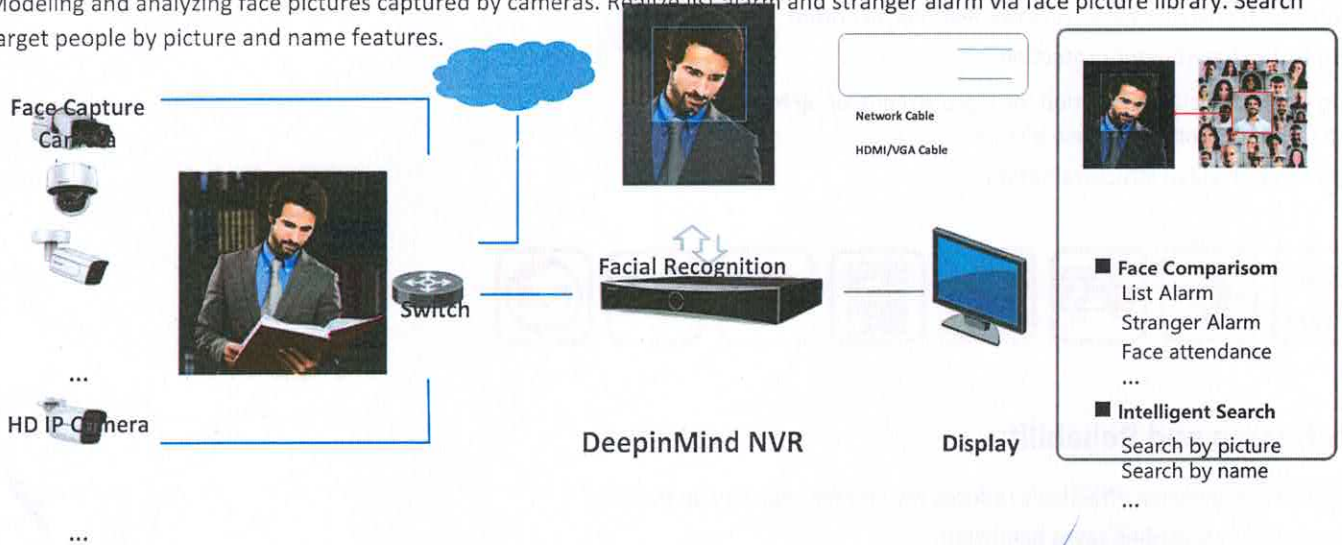
Network & Ethernet Access

- 1 self-adaptive 10M/100M/1000M Ethernet interface
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Support feature for searching cameras on the network

Typical Application

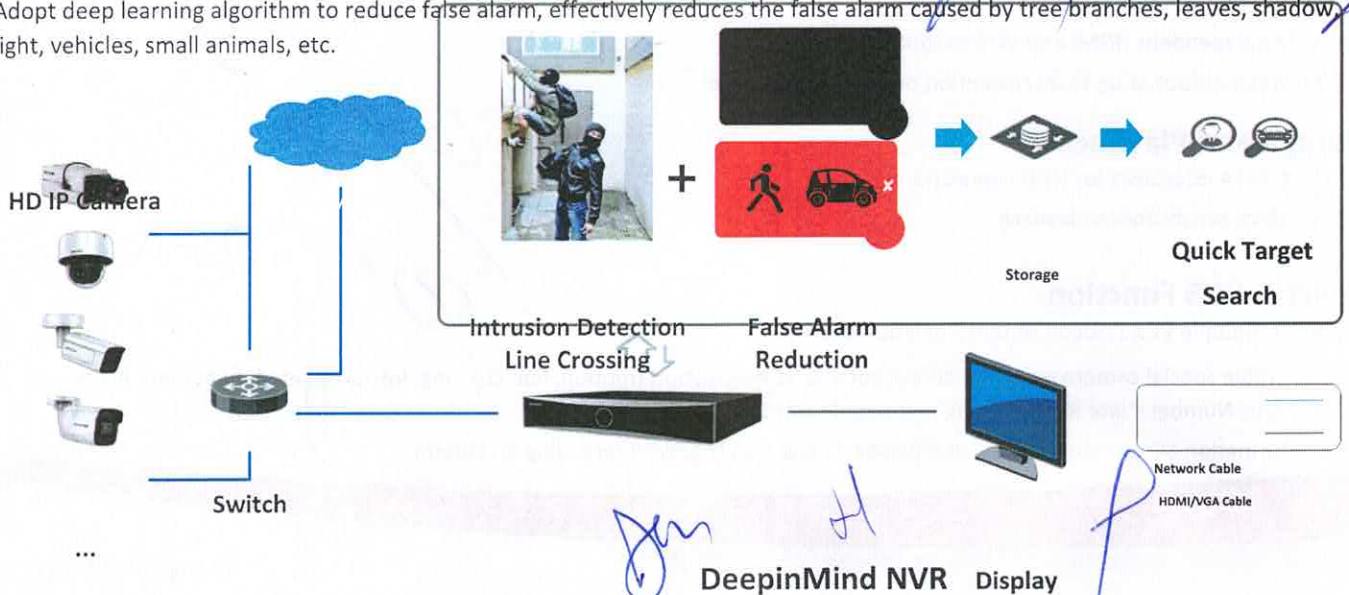
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



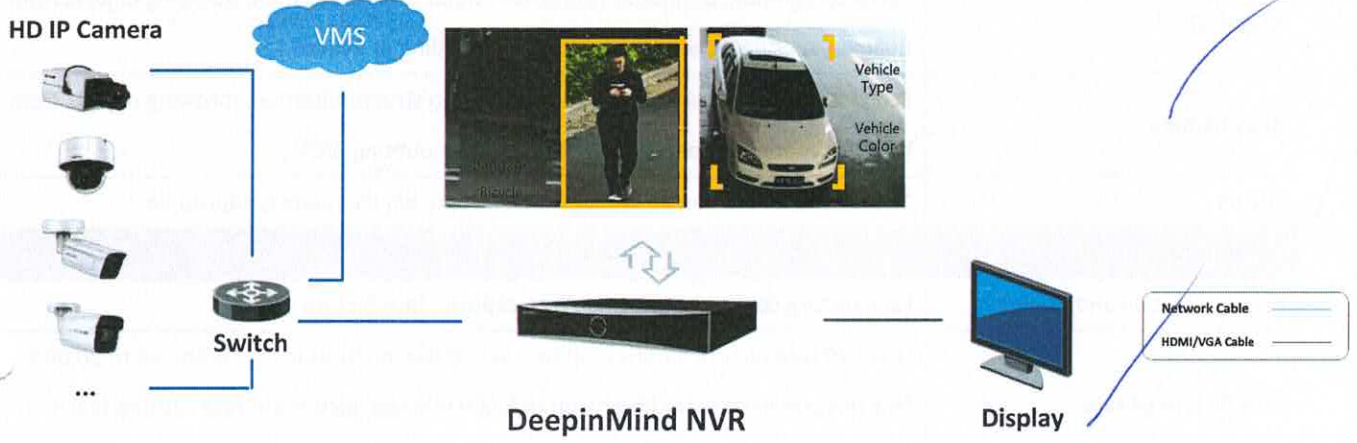
Perimeter Protection

Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.



Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles.



Handwritten signature

Handwritten signature

29th H

■ Specification

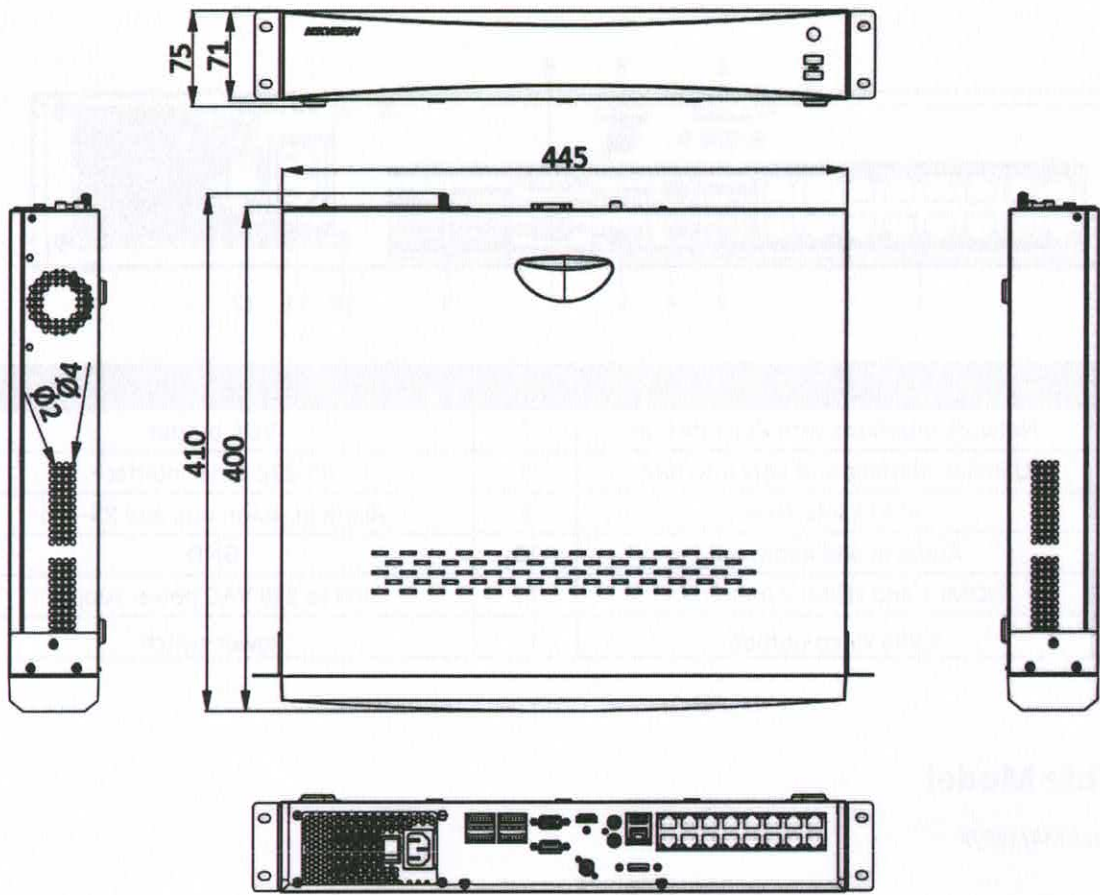
Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization, throwing objects from Building, motion detection2.0 schedule recording or evento.
AI by Camera	Facial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection2.0, ANPR, people counting, VCA
Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 20 face picture libraries, up to 100,000 face pictures in list library, up to 20,000 face pictures in stranger library, up to 5,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)
Face Picture Comparison (Captured from Camera)	16-ch (8-ch for each engine); Comparison speed: 48 pictures per second
Facial Detection and Analytics Performance	16-ch 2 MP (8-ch for each engine), up to 8 MP
Perimeter Protection	
By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP
By Camera	All channels
Video Structuralization	
Structured Analysis	Supports simultaneous detection and capture of human body, Obtains 7 facial characteristics, mask, gender, type and color of clothing, hat, glasses
Face Picture Library	Up to 20 face picture libraries, up to 100,000 face pictures in list library, up to 20,000 face pictures in stranger library, up to 5,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)
Face Picture Comparison	16-ch; Comparison speed: 32 pictures per second
Event Basic	
By NVR	Motion detection, video tampering alarm, Linkage Upload to FTP, Video Loss
By Camera	All channels
ANPR	
By Camera	All channels
Vehicle Attributes	Plate number, license plate color, license plate type
Plate Attributes	Vehicle brand, vehicle color, vehicle type

Video and Audio	
IP Video Input	16-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Incoming Bandwidth	256 Mbps
Outgoing Bandwidth	256 Mbps
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.
Video Output Mode	HDMI1/VGA1 simultaneous output, HDMI1/HDMI2 independent output, multi-screen viewing divided into 1, 4, 8 and 16.
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	1-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 kΩ)
VGA Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+/MPEG
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25 fps)/16-ch@4 MP (30 fps)
Synchronous Playback	Allows you to search recording by date, time, alarm, motion detection, intelligent search
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/D1/720p/VGA /4CIF/DCIF/2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMP, NFS, iSCSI, ISUP, UPnP™, HTTP, HTTPS, UDP, Filter IP e FTP
API	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	1, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface

PoE	
Interface	16 RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
Power	≤200W
Standard	IEEE 802.3 af/at
Auxiliary Interface	
SATA	4 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 20 TB capacity for each HDD
Serial Interface	1 RS-232, 2 RS-485 (full-duplex), 1 keyboard
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0
Alarm In/Out	16/4
General	
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian
Power Supply	100 to 240 VAC, 50 to 60 Hz
Consumption	≤ 50 W (without HDD and PoE off)
Working Temperature	-10 to 55° C (14 to 131° F)
Working Humidity	10 to 90%
Dimension (W × D × H)	445 × 400 × 71 mm (17.5" × 15.7" × 2.8")
Weight	≤ 5 kg (without HDD, 11 lb.)
Certification	
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS
FCC	Part 15 Subpart B, ANSI C63.4-2014
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:2019, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020

Handwritten signatures and initials in blue ink, including a large signature and several smaller initials, located below the table.

Dimension



scale/1:1;Unit/mm

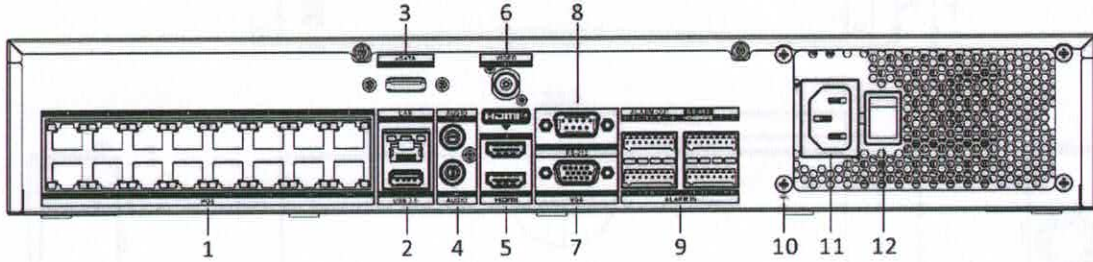
Dec M

Page 1

Bm

H

Physical Interface



No.	Description	No.	Description
1	Network interfaces with PoE function	7	VGA output
2	USB 3.0 interface and LAN interface	8	RS-232 serial interface
3	eSATA interface	9	Alarm in, alarm out, and RS-485
4	Audio in and audio out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	CVBS video output	12	Power switch

Available Model

IDS-7716NXI-M4/16P/X

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information:



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq



iDS-7732NXI-M4/16P/X (C) DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16-ch@4 MP/32-ch@1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 32-ch IP cameras can be connected, plug & play with 16 power-over-Ethernet (PoE) interfaces
- Intelligent analytics based on deep learning algorithm
- Up to 24-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 32-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
Support double verification for playback and downloading
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability
- System Embedded Linux System

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 4 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm

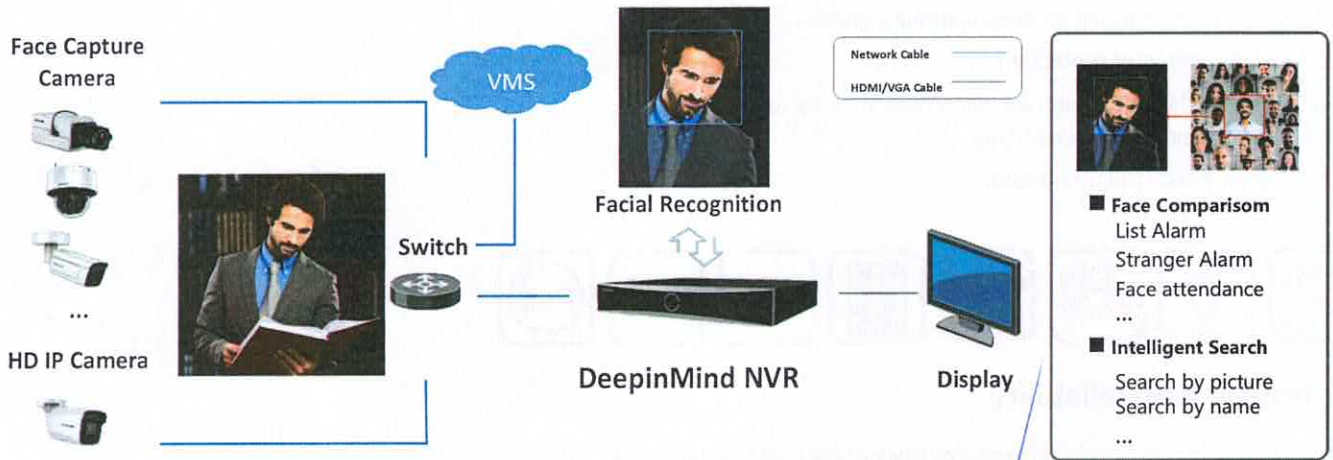
Network & Ethernet Access

- 1 self-adaptive 10M/100M/1000M Ethernet interface
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Support feature for searching cameras on the network

Typical Application

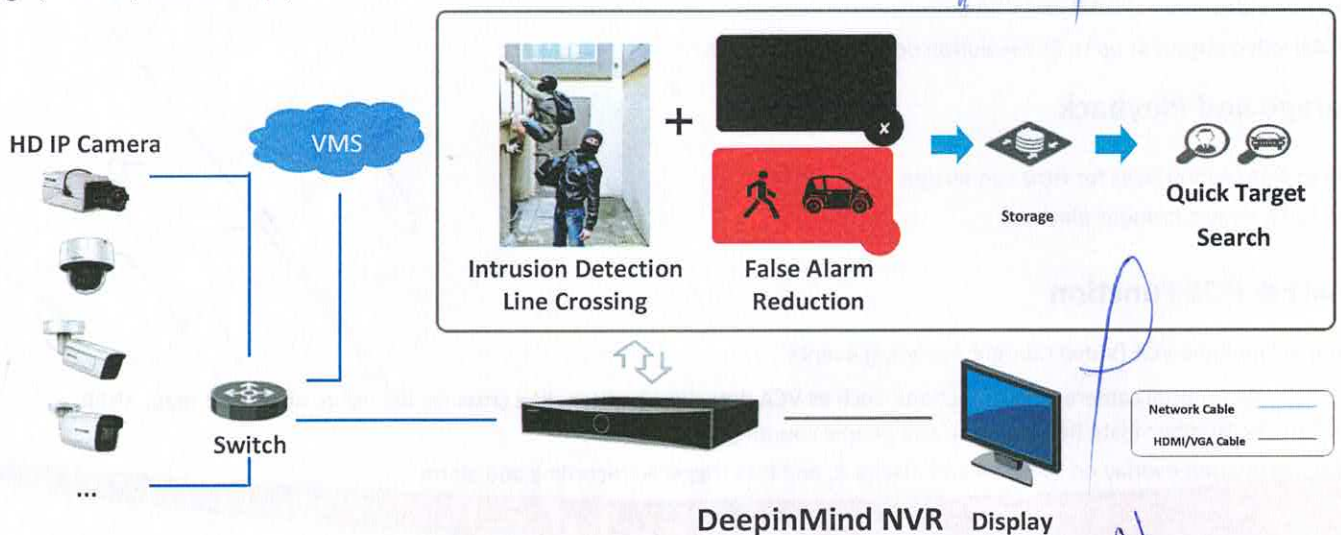
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



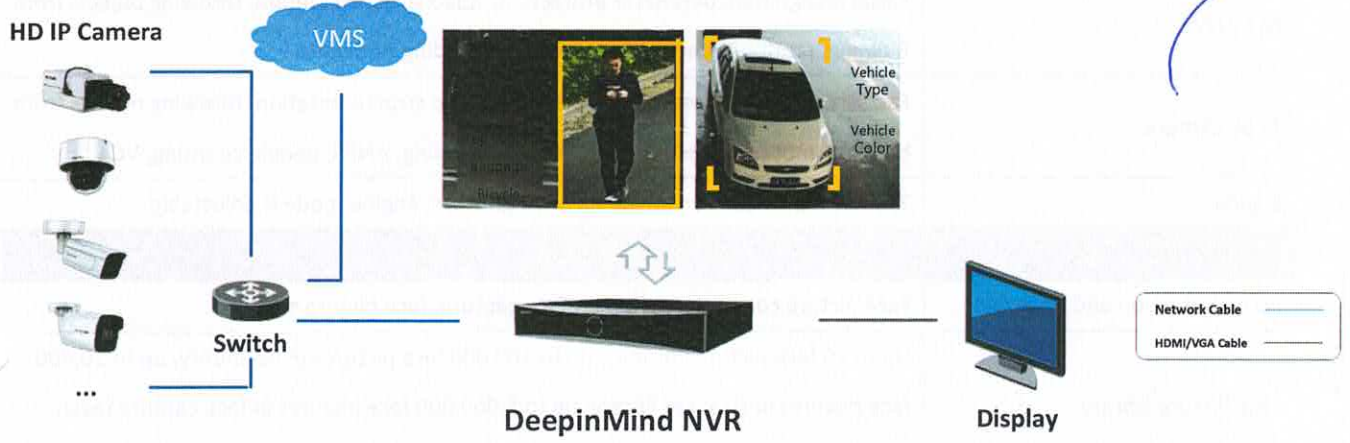
Perimeter Protection

Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.



Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles.



Handwritten signature

Handwritten signature

• Specification

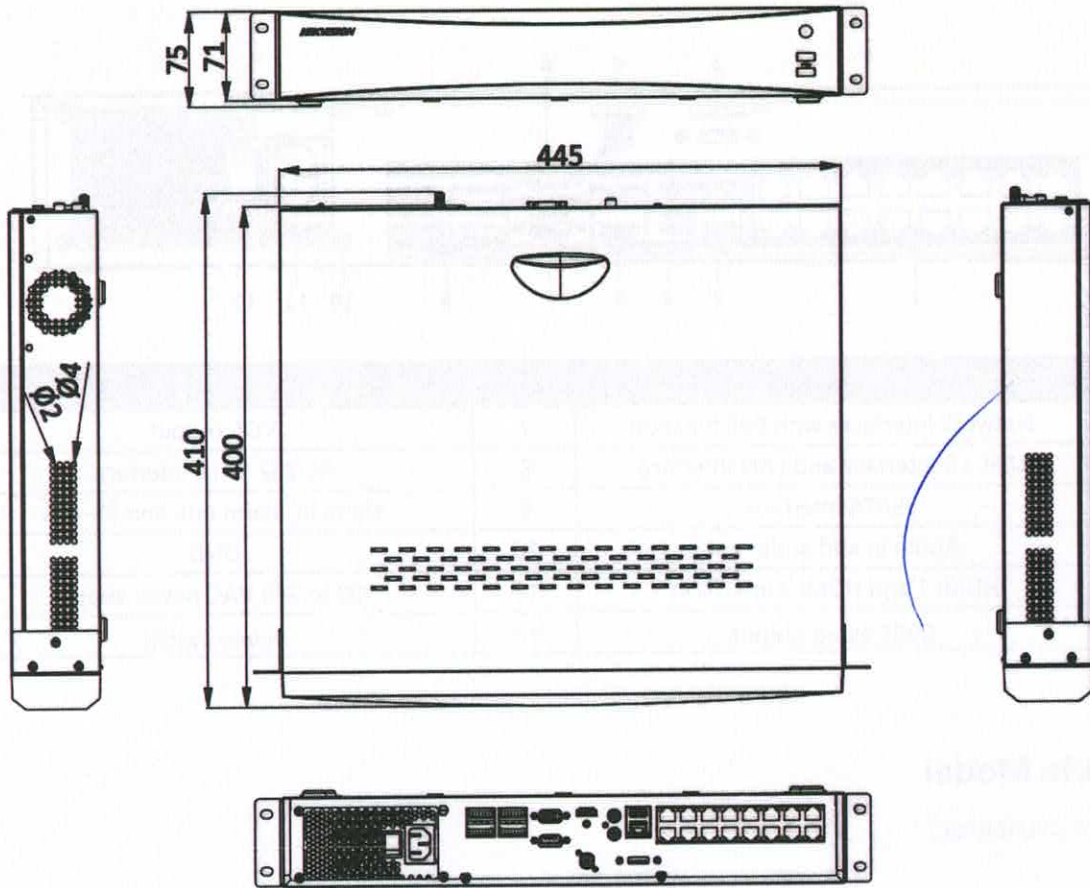
Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization, throwing objects from Building, motion detection 2.0 schedule recording or event.
AI by Camera	Facial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2.0 schedule recording, ANPR, people counting, VCA
Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 20 face picture libraries, up to 100,000 face pictures in list library, up to 20,000 face pictures in stranger library, up to 5,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)
Face Picture Comparison (Captured from Camera)	32-ch (16-ch for each engine); Comparison speed: 48 pictures per second
Facial Detection and Analytics Performance	16-ch 2 MP (8-ch for each engine), up to 8 MP
Perimeter Protection	
By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP
By Camera	All channels
Video Structuralization	
Structured Analysis	Supports simultaneous detection and capture of human body, Obtains 7 facial characteristics, mask, gender, type and color of clothing, hat, glasses
Face Picture Library	Up to 20 face picture libraries, up to 100,000 face pictures in list library, up to 20,000 face pictures in stranger library, up to 5,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)
Face Picture Comparison	16-ch; Comparison speed: 32 pictures per second
Basic Events	
By NVR	Motion detection, video tampering alarm, Linkage Upload to FTP, Video Loss
By Camera	All channels
ANPR	
By Camera	All channels
Vehicle Attributes	Plate number, license plate color, license plate type
Plate Attributes	Vehicle brand, vehicle color, vehicle type

Video and Audio	
IP Video Input	32-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Incoming Bandwidth IA	320 Mbps
Outgoing Bandwidth IA	400 Mbps
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.
Video Output Mode	HDMI1/VGA1 simultaneous output, HDMI1/HDMI2 independent output, multi-screen viewing divided into 1, 4, 8 and 16 and 32 channels;
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	1-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 kΩ)
VGA Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Decoding	
Decoding Format	MJPEG /H.265/H.265+/H.264/H.264+
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25 fps)/16-ch@4 MP (30 fps)/32-ch@1080p (30 fps)
Synchronous Playback	Allows you to search recording by date, time, alarm, motion detection, intelligent search
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/D1/720p/VGA /4CIF/DCIF/2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMP, NFS, iSCSI, ISUP, UPnP™, HTTP, HTTPS, FTP, UDP, Filter IP.
API	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	1, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface

3000 1000 11

PoE	
Interface	16 RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
Power	≤200W
Standard	IEEE 802.3 af/at
Auxiliary Interface	
SATA	4 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 20 TB capacity for each HDD
Serial Interface	1 RS-232, 2 RS-485 (full-duplex), 1 keyboard
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0
Alarm In/Out	16/4
General	
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian
Power Supply	100 to 240 VAC, 50 to 60 Hz
Consumption	≤ 50 W (without HDD and PoE off)
Working Temperature	-10 to 55° C (14 to 131° F)
Working Humidity	10 to 90%
Dimension (W × D × H)	445 × 400 × 71 mm (17.5" × 15.7" × 2.8")
Weight	≤ 5 kg (without HDD, 11 lb.)
Certification	
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS
FCC	Part 15 Subpart B, ANSI C63.4-2014
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:2019, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020

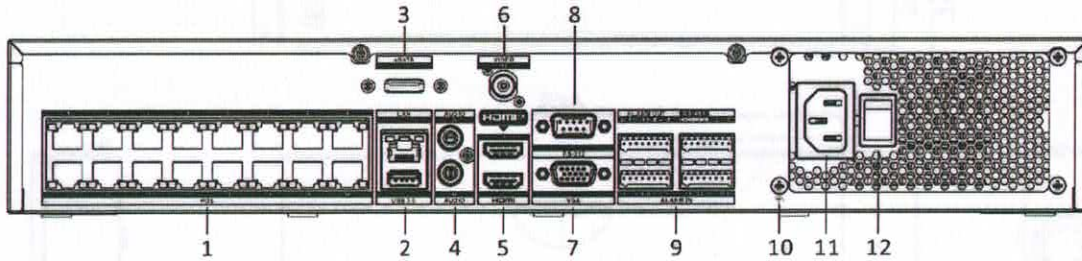
Dimension



scale/1:1;Unit/mm

Handwritten signatures and marks in blue ink.

Physical Interface



No.	Description	No.	Description
1	Network interfaces with PoE function	7	VGA output
2	USB 3.0 interface and LAN interface	8	RS-232 serial interface
3	eSATA interface	9	Alarm in, alarm out, and RS-485
4	Audio in and audio out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	CVBS video output	12	Power switch

Available Model

iDS-7732NXI-M4/16P/X(C)

Headquarters

No.555 Dianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq



DS-3E2528P Gigabit Full Managed PoE Switch



Features and Functions

- DS-3E2528P supports the telecom-level Ethernet-ring protection protocol with a protection shift time of less than 50ms, STP/RSTP, backup of active and standby uplinks, and LACP link aggregation to cater to the requirements of high reliability of carriers;
- DS-3E2528P has powerful ACL functions to access and control L2-L7 data, providing carriers flexible and various policy control methods;
- DS-3E2528P supports In-Service Software Upgrade (ISSU) to ensure the unremitting data forwarding during system upgrade;
- DS-3E2528P supports various L2 multicast functions such as IGMP-snooping, user fast-leave mechanism and trans-vlan multicast copy;
- DS-3E2528P supports IEEE 802.3AF/AT standard, built-in large power supply, no need of external power supply, that is, 24-port AF full-load power supply.
- DS-3E2528P supports the configuration of Base-T port priority when the power is inadequate.
- DS-3E2528P supports POE port and up to 4KV power thunder-proof.
- DS-3E2528P supports priority retagging and complicated flow classification based on VLAN, MAC, source address, destination address, IP or priority to better streamline carrier's services;
- DS-3E2528P provides flexible bandwidth control policies, supporting port-/flow-based flow limit, and ensuring the line speed forwarding of each port to make sure the high quality of network services;
- DS-3E2528P supports multiple queue schedule algorithms such as SP, WRR, or "SP plus WRR";
- Equipment-level security: The advanced hardware infrastructure design realizes the level-based packet schedule and packet protection, prevents DoS-/TCP-related SYN Flood, UDP Flood, Broadcast Storm or large traffic attacks, and supports level-based command line protection, endowing different levels of users with different management permissions;
- Perfect security authentication mechanisms: IEEE 802.1x, Radius and BDTacacs+;
- DS-3E2528P supports storm/multicast/unicast limit which ensures the normal running of equipment in harsh network conditions;
- DS-3E2528P supports perfect ring detection mechanism which ensures the long-term stable running of network;
- DS-3E2528P supports port isolation within the same VLAN, DHCP-Snooping, and IP plus MAC plus Port binding for ensuring user data security;
- DS-3E2528P supports many management modes such as the console port, Telnet, SSH;
- DS-3E2528P supports the WEB management mode, which is easy and efficient so that it makes installation and debugging convenient;
- DS-3E2528P supports TFTP-patterned file upload/download management;

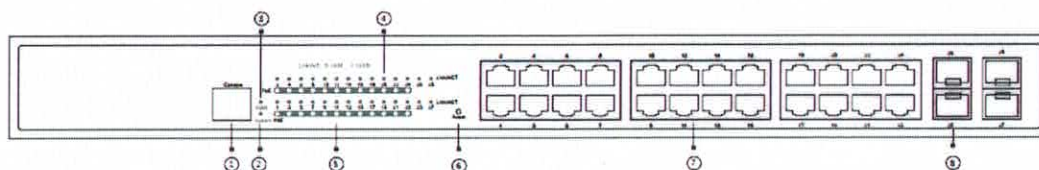


Specifications

Item	DS-3E2528P
Port number	24 x 10/100/1000Base-T PoE ports, 4 1000Base-X SFP ports, 1 Console port
Switching capacity	56Gbps
Packet forwarding rate	42Mpps
MAC address table	8K
Dimensions(L × H × D)	440 mm × 45 mm × 232 mm
Consumption	<15W
POE standard	IEEE802.3af, IEEE802.3at
POE power budget	380W
Power supply	AC : 100V-240V , 50Hz±10%
Environment	Operating temperature/humidity: 0°C-45°C , 5%-95% non-condensing Storage temperature/humidity: -20°C-70°C ; 5%-95% non-condensing
MAC exchange	Static configuration and dynamic MAC learning; MAC browsing and removal Configurable aging time of the MAC address; Limited number of learnable MAC addresses; MAC filtration
VLAN	4K VLAN; GVRP; QinQ; Private VLAN
STP	802.1D (STP), 802.1W (RSTP) and 802.1S (MSTP) BPDU protection, root protection, and loopback protection
Multicast	IGMP v1/v2/v3 IGMP snooping IGMP Fast Leave Multicast group strategy and quantity limitation
QoS	Flow classification based on L2~4 protocols CAR flow limit 802.1P/DSCP priority re-labeling SP, WRR, and "SP+WRR" Congestion avoidance mechanisms like Tail-Drop and WRED Flow monitoring and flow shaping
Security	L2/L3/L4 ACL flow identification and filtration DDoS attack prevention, TCP's SYN Flood attack prevention, UDP Flood attack prevention, etc Broadcast/multicast/unknown unicast storm-control Port isolation Port security, and "IP+MAC+port" binding
Reliability	Static/LACP link aggregation EAPS and ERPS
Management	Console, Telnet, SSH2.0, Web SNMP v1/v2/v3 TFTP RMON

Physical Interfaces

Front Panel



No.	Abbrev.	Name	Description
1	CONSOLE	Console port	Manages the switch locally.
2	SYS	System indicator	If the indicator is always on, the system is being started. If the indicator flickers, the system works normally.
3	PWR	Power indicator	If the switch is powered on, the indicator is on.
4	Link/ACT	LINK/ACT indicator of each port	If the indicator is on in green: 10/100M, If the indicator is on in red: 1000M If the indicator is not on: no signal is transmitted.
5	POE	POE indicator	If the indicator is always on: POE works normally; If the indicator is not on, POE does not work.
6	Reset	Reset switch	Return to the factory setting.
7	/	24 gigabit RJ45 ports	Forwards the 10/100M/1000M Ethernet electric signals and provides with POE functions.
8	/	4 SFP ports	Forwards 1000M Ethernet optical signals.

Distributed by

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

Hikvision USA
T +1-909-895-0400
sales.usa@hikvision.com

Hikvision Italy
T +39-0438-6902
info.it@hikvision.com

Hikvision Singapore
T +65-6684-4718
sg@hikvision.com

Hikvision Europe
T +31-23-5542770
saleseuro@hikvision.com

Hikvision France
T +33(0)1-85-330-444
info.fr@hikvision.com

Hikvision Oceania
T +61-2-8599-4233
salesau@hikvision.com

Hikvision Middle East
T +971-4-8818086
salesme@hikvision.com

Hikvision Spain
T +34-91-737-16-55
info.es@hikvision.com

Hikvision Hong Kong
T +852-2151-1761

Hikvision Russia
T +7-495-689-67-99
saleru@hikvision.com

Hikvision Poland
T +48-22-460-01-50
poland@hikvision.com

Hikvision Canada
T +1-909-895-0400
sales.usa@hikvision.com

Hikvision India
T +91-22-28469900
sales@pramahikvision.com

Hikvision UK
T +44-1628-9021-4
support.uk@hikvision.com

[Handwritten signatures and initials in blue ink]



À
CÂMARA MUNICIPAL DE SUMARÉ
ESTADO DE SÃO PAULO
(Rua Barbara Blumer, nº 41 – Jardim Alvorada)

PREGÃO PRESENCIAL Nº 14/2024
PROCESSO ADMINISTRATIVO Nº 458/2024

TIPO: MENOR PREÇO GLOBAL

EM BRANCO

TERMO DE ENCERRAMENTO



À
CÂMARA MUNICIPAL DE SUMARÉ
ESTADO DE SÃO PAULO
(Rua Barbara blumer, nº 41 – Jardim Alvorada)

PREGÃO PRESENCIAL Nº 014/2024
PROCESSO ADMINISTRATIVO: Nº 458/2024
MENOR PREÇO GLOBAL

Objeto: Contratação de empresa especializada para execução do Projeto de Sistema de Videomonitoramento inteligente, e prestação de serviços de locação de equipamentos, incluindo toda a infraestrutura física e interligação dos prédios sede, Anexo e Escola do Legislativo, da Câmara Municipal de Sumaré

TERMO DE ENCERRAMENTO

A empresa **TALENTECH – TECNOLOGIA LTDA.**, inscrita no CNPJ nº 15.773.416/0001-10, com sede à Avenida Queiroz Filho, nº 1700 – Torre A, Sala 902, Condomínio Vila Lobos Office Park, Bairro Vila Hamburguesa, na cidade de São Paulo, Estado de São Paulo, através de seus representantes legais, o **Sr. João Batista Alves Junior**, portador da Carteira de Identidade R.G. nº 29.112.325 – SSP/SP e inscrito no CPF/MF sob o nº 292.350.078-44 e o **Sr. Adriano Rogério de Souza**, portador da Carteira de Identidade nº 33.284.586-2 – SSP/SP e do CPF nº 284.939.248-06, **DECLARA**, que este volume de “**PROPOSTA DE PREÇOS**”, possui **136** páginas, numeradas sequencialmente de **001** a **136**, incluindo esta.

São Paulo, 09 de outubro de 2024.

TALENTECH – TECNOLOGIA LTDA.

João Batista Alves Junior
Diretor
RG: 29.112.325 – SSP/SP
CPF: 292.350.078-44

Adriano Rogério de Souza
Procurador
RG: 33.284.586-2 – SSP/SP
CPF: 284.939.248-06

TALENTECH – TECNOLOGIA LTDA.

Av. Presidente Altino, 1925 – Galpão 2 Bloco C – Jaguaré - São Paulo – SP – CEP: 05.323-002 – Brasil
Telefone: 55 (11) 3831-6032 - E-mail: licitacoes@tecnologiagto.com.br



[Handwritten signature]

À
CÂMARA MUNICIPAL DE SUMARÉ
ESTADO DE SÃO PAULO
(Rua Barbara Blumer, nº 41 – Jardim Alvorada)

[Handwritten mark]

PREGÃO PRESENCIAL Nº 14/2024
PROCESSO ADMINISTRATIVO Nº 458/2024

TIPO: MENOR PREÇO GLOBAL

Objeto: Contratação de empresa especializada para execução do Projeto de Sistema de Videomonitoramento inteligente, e prestação de serviços de locação de equipamentos, incluindo toda a infraestrutura física e interligação dos prédios sede, Anexo e Escola do Legislativo, da Camara Municipal de Sumaré.

[Handwritten signature]

[Handwritten mark]

“ENVELOPE Nº 01”
PROPOSTA COMERCIAL

[Handwritten signatures]