**Technical specifications**

**Table of Content**

**Technical specifications** 1

1 Background and General Requirement 5

1.1 Background 5

1.2 General Requirement 5

2 Video Surveillance Technical Requirement 6

2.1 Overall Requirement 6

**2.1.1** Video Management Platform 7

**2.1.2** IP Cameras 7

2.2 Technical Specifications 8

**2.2.1** The video surveillance platform 8

**2.2.2** IP Fixed Dome Camera (Indoor Type) 11

**2.2.3** IP Bullet camera (Outdoor Type) 12

**2.2.4** IP PTZ ​​Dome Camera (Outdoor Type) 14

**2.2.5** Camera site 15

2.3 ANPR Technical Requirement 20

**2.3.1** Composition of Checkpoint system 20

**2.3.2** Composition of Checkpoint front-end subsystem 20

**2.3.3** Site layout diagram of Checkpoint front end subsystem 22

**2.3.4** Technical Specifications 23

3 Express Penalty System 24

3.1 Overall requirement 24

3.2 Technical specification 25

**3.2.1** General specification 25

**3.2.2** API specification 27

4 Emergency Communication System Requirement 34

4.1 Overall requirement 34

**4.1.1** Video, Voice, and Data Convergence 34

**4.1.2** Authentication 34

**4.1.3** IPSec for Base Station 34

**4.1.4** Remote Handset Disable and Enable 34

**4.1.5** Geographic Redundancy 35

4.2 Broadband Trunking Multimedia Dispatching 35

**4.2.1** General Requirements 35

4.3 Base Station 35

**4.3.1** General Requirements 35

**4.3.2** BBU Requirements 36

**4.3.3** RRU Requirements 36

4.4 Core Network 37

**4.4.1** General Requirements 37

4.5 Terminal 37

**4.5.1** High Class Handset 37

**4.5.2** Medium Class Handset 38

4.6 Vehicle Mounted Terminal 38

**4.6.1** Voice trunking requirements 38

**4.6.2** Multimedia dispatching requirements 39

**4.6.3** Hardware 39

4.7 Telephony Gateway 39

4.8 Trunking Gateway 40

4.9 SIP/SDK Interface 40

4.10 Aerial surveillance (UAV) 40

**4.10.1** Overall requirement 40

**4.10.2** Technical requirement 41

5 Command center technical requirement 42

5.1 Overall Requirement 42

**5.1.1** Command Center Overview 42

**5.1.2** Emergency Call Centre (ECC) 42

**5.1.3** Dispatch Control Centre (DCC) 45

**5.1.4** Meeting Room 47

5.2 Technical Specifications 48

**5.2.1** Integrated communication platform 48

**5.2.2** Computer Aided Dispatch System 50

**5.2.3** Geographic Information System (GIS) 51

6 Data Center 52

6.1 Data Center (Layer1) 52

**6.1.1** General Description 52

**6.1.2** Racks and Aisle Containment 52

**6.1.3** Uninterruptable Power Supply (UPS) 52

**6.1.4** Cooling System 53

**6.1.5** Door Access System 53

**6.1.6** DCIM (Data Center Infrastructure Management) 53

6.2 Data Center (Layer2 & Layer3) 54

**6.2.1** Intelligence Analysis System 54

**6.2.2** Video Management Platform 54

# Background and General Requirement

## Background

Safety in Uganda is in grave difficulties. Robberies and shootings are rising, creating a greater sense of urgency to optimize safety conditions.

Legacy security systems have the following challenges:

1. Difficult to perceive onsite conditions

Communication lines are unavailable and fixed cameras are not deployed at the scene. Mobile terminals fail to backhaul real-time voice and video from the scene to the command center. The call-taking capacity of a single line for each department is too small and easily congested. Power supply for communication facilities and surveillance sites is not reliable. The mains supply is unstable. Engine generators deployed in places where the mains supply is unavailable are easy to be stolen or sabotaged.

1. Inefficient consultation and command

Instructions cannot be accurately sent to remote scenes where signal coverage is unavailable. Point-to-point (P2P) communication based on mobile phones is inefficient. Phone-based P2P communication is inefficient, hindering cross-departmental collaboration. Rescue resources cannot be located promptly, unable to support decision-making. Decision makers may fail to make accurate decisions because of insufficient knowledge about onsite conditions.

1. Unable to support the communication of sensitive data

No independent communication network is available. Office data and public networks are not isolated, increasing data leak risks. Civil mobile communication terminals are easy to be damaged in harsh environments.

1. Scattered surveillance information

Surveillance systems were separately deployed, resulting in insufficient information and passive incident response. Devices must be managed in a unified manner to ensure system controllability and manageability.

The government decides to enhance emergency response efficiency by innovating ICT technologies. The government wants an HD video surveillance system, emergency response platform, intelligent video analysis platform, and radio system to implement real-time, dynamic, and global security surveillance and emergency response.

## General Requirement

The Uganda government wants the solution to provide communication services for the response to national security events, emergencies, and natural disasters. The new solution must deploy a private network to extend voice communication and video surveillance to specified key locations. In addition, the new solution must implement audio and video communication across government agencies in case of emergencies. The project includes the following parts to provide emergency services to citizens.

1. A public-safety answering point (PSAP), or called "public-safety access point", is a call center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services. Trained telephone operators are also usually responsible for dispatching these emergency services. Each PSAP has a 'real' telephone number that is called when the emergency number (999 or 112) is dialed. The telecommunications operator is responsible for associating all landline numbers with the most applicable (often the nearest) PSAP, so that when emergency number is dialed, the call is automatically routed to the most suitable PSAP.
2. A converged command center must be built to reinforce emergency response capabilities. The EOC shall have the capability to monitor all regions in real time, receive incidents reported via diverse channels, and dispatch incidents in a unified manner. An emergency operations center (EOC) is a central command and control facility responsible for carrying out the principles of emergency preparedness and emergency management, or disaster management functions at a strategic level during an emergency, and ensuring the continuity of operation of a political subdivision or other organization. The functions of the EOC's is to collect, gather and analyze data; make decisions that protect life and property, maintain continuity of the organization, within the scope of applicable laws; and disseminate those decisions to all concerned agencies and individuals.
3. A video surveillance system must be deployed in key locations to help public safety agencies sense emergencies in a timely manner.
4. A dedicated, secure, high-performing, and reliable voice and video trunking communication system is required to guarantee internal communication across public safety agencies.
5. With economic development, the number of motor vehicles is growing. Motor vehicle violation is one important reason to cause traffic disorder, traffic jams and accidents. How to strengthen the management of motor vehicle drivers is the major issue in the traffic engineering work. Electronic police system against running red light, as an important part of urban intelligent traffic management, is of great significance in aspects of regulating traffic safety, enhancing awareness of safe driving, preventing red light running and combating the phenomenon of criminal acts.
6. A data center is required to support the reliable operation and maintenance of the preceding systems.
7. New HD video image collection points in the solution need to ensure over 25 frames per second for 1080P videos. The dedicated fiber bearer network needs to meet needs of live video surveillance, video distribution, and interconnection with the dedicated city video network and secure isolation.
8. The solution is complex very much and composed of many subsystems. So the management is also important.
9. Introduce end to end network security for whole system, include IT security and CT security.

# Video Surveillance Technical Requirement

## Overall Requirement

The CCTV system should ensure full coverage of new capital pre-defined, recording and image management 24h \*7 days. The video should be stored not least than 60 days.

The management of this component is provided by HQ is responsible for managing any region.

The system consists of the video management platform, IP cameras

### Video Management Platform

The video management platform should be interoperable, scalable and with advanced functions.

The platform should have an open, standardized architecture. It should use SUSE Linux operating system to ensure platform stability and security.

The platform should have secondary development interfaces to support IOC with uplink service systems.

A multi-level architecture platform should be adopted to implement management requirements, which support:

The operation and command center located at the HQ can access and use all the cameras.

The system must ensure the possibility of adding other command and operations centers.

All the platform and decoder should be the same brand as the cameras, and they must support H.265, and be compatible to H.264;

Allows recording data in undamaged disks to be read when multiple disks in the RAID group are damaged.

Allow multiple nodes to go down simultaneously with no bad effect to the normal operation of the business and the N+0 cluster will enable automatic balancing between cluster nodes when the faulty nodes recover.

Embedded video quality diagnosis helps to achieve real-time maintenance.

Provides built-in video surveillance software that supports PU access, media scheduling, video storage, service management, storage management, device management, and system management to one system, It should support concurrently store at least 512-channel video at 1024 Mbit/s bandwidth, forward at least 512-channel video at 1024 Mbit/s bandwidth for live view, and play back 512-channel video at 1024 Mbit/s bandwidth and 10GE interface.

Transmits video after being encrypted using AES256 to ensure data security.

### IP Cameras

At filed, considering hash environment we required standard surveillance site and make sure the site stable and easy to deploy and maintenance. The standard surveillance site Including Video surveillance subsystem, network access subsystem, power supply subsystem, and structural support subsystem.

In indoor and outdoor environment, we choose dome camera and bullet camera to cover these areas.

At the square, PTZ dome cameras are used to cover these areas, Will monitor the square for 24 hours at a proper angle.

All the cameras should support H.265, and be compatible to H.264.

It shall support 20% anti-packet loss to protect the image quality when the qualities of IP network get worse.

It should support User name and password authentication, 802.1x, and HTTPS digital certificate, IP address filtering, digital watermark and Streams encrypted through AES 256 to protect the data security.

It should at least support ONVIF 2.5 Profile S/G and the manufacturer company shall be the member of at least one of the organizations of ONVIF and camera vendor also will be the member of providing H.265 CFP (Call for Proposal) and the quantities of technical proposals is at least 4%.

It should support embedded invisible infrared function for monitoring some sensitive areas and the distance of infrared light is not less than 30m.

It should support excellent Anti-corrosion: IEC60068-2-11:1981, pass at least 10 days of salt fog test and provide the environment test report.

It should at least support AC24V±25%, 24 V DC±20% to guarantee the stability of power supply.

## Technical Specifications

### The video surveillance platform

To reduce the complexity of the system, the video surveillance platform must integrate video surveillance, storage and all the services and functionalities required in a single device (All in One).

This equipment must be stackable in order to add resources and ensure redundancy by adding another node.

The video surveillance platform (one node) must meet the following requirements:

| **Type** | **Description** |
| --- | --- |
| Hardware | The device must be installed in a standard 19 "enclosure, has two independent system disks that can be RAID 1 configured to ensure system disk security, supports at least 40 data disks for a single device |
| Redundant and hot-swappable power supply. |
| A redundant basic input / output (BIOS) system to improve system security |
| Adopts modular design and separates system disks and data disks to improve system reliability |
| Hot replacement of faulty drives; |
| 64-bit processor with at least six-core. |
| Provide DDR4 memory of at least  16GB |
| Configure at least four network ports 10/100/1000 Mbit / s, provides the ability to redundant connections, |
| Adopts the block storage mechanism (BS), which is, the storage does not depend on the operating system or files and the repeated rewriting of the data does not generate fragments of disks. |
| Allow data to be saved to discs in good condition for playback even when multiple disks in the RAID array are damaged. (At least two disks in RAID 5 are faulty). |
| Supports RAID 5 |
| Supports load balancing between RAID groups (at least two RAID groups are required) |
| Supports a dynamic hot spare |
| Supports data security function, which makes multiple copies of key data from the system disk to the data disk, which allows fast restoration of data when the system disk is defective |
| Supports Video surveillance, automatic management of the distribution of cameras, and elastic extension of cluster nodes |
| Allows multiple nodes in the cluster to go down simultaneously without negative effect for normal business operation and the cluster will automatically enable swing between nodes of the cluster when the defective nodes are recovered. |
| Supports integrated diagnostics of video quality that contributes to real-time operation and maintenance. Automatically detects the following image exceptions: definition exception, image noise, brightness exception, color cast, stripe interference, image freezing, image jitter, lens block, and video signal loss. |
| Provides integrated video surveillance software that supports media scheduling, video storage, service management, storage management, device management, and management system |
| Supports at least 512video access channels, 512 video transmission channels, 512 video storage channels, and 128 video playback and download channels for a single device. |
| Supports at least 1024 Mbps for video access, 1024 Mbps for video transfer, 1024 Mbps for video storage, and 1024 Mbps for video and download playback |
| Supports auto-stacking of 16 devices, provides a unified view of resources, prevents a defective device from affecting other normal devices, and allows the stack to support up to 1024 devices. |
| Software | Supports multi-level and multi-domain management, interconnection of more than 128 external domains, and interconnection of up to eight platform levels |
| Supports at least 5000 users for a single domain and allows 2000 users to connect at the same time and 500 users to perform operations at the same time |
| Displays live video information, including the camera name, bit rate, frame rate, and encoding format |
| Supports auto-adaptive aspect ratio window size adjustment. |
| Transfer of video stream from PUs to CUs in direct connection mode |
| Supports live and recorded digital video zoom (even video taken by non-PTZ cameras are supported) |
| Supports playback of at least 25 records at the same time; Allows users to play at least eight videos recorded simultaneously; Allows users to control playback (fast forward, slow play, and jump to a specific time point) |
| Allows users to play back recordings using the following controls: slow reverse (1 / 4x and 1 / 2x), fast forward (2x, 4x, 8x and 16x), slowdown (1 / 32x, 1 / 16x, 8x, 1 / 4x and 1 / 2x), rewind (2x, 4x, 8x and 16x), drag and frame |
| Allows users to view monitoring sites on the electronic map and playback of video shot by cameras at a specified monitoring site; Allows users to zoom in on an area by scrolling the mouse wheel, dragging and moving the map, viewing the map in full screen, panning up, down, left, and right, and controlling the map Scale of the map |
| Allows users to add cameras and alarm source icons to the electronic map |
| Allows users to create sensitive areas. |
| Allows users to start the live video display in an independent window by clicking on the camera icons on the cards; Allows users to take snapshots, record video to local disk, bookmark video, and allow 3D positioning in the video window displayed in real time |
| Allows users to receive, query, and alarms processing and set severity of alarm (warning, minor, major or critical) |
| Links the central platform to perform the following actions when an alarm is triggered: video recordings, captures takes, invokes predefined positions, displays video on clients or video walls, and provides Boolean value outputs; Allows users to manage protection zones |
| Supports scheduled recording by specifying a time segment on the timeline. |
| Allows users to set triggered snapshot alarm policies, including the amount and interval of snapshots; Allows snapshots taken by the cameras to be automatically downloaded to the image server; Allows users to query, preview, delete, download and print snapshots |
| Manage system logs, alarm logs, device logs and logs; Allows users to query logs by user, time, type, or level; Allows users to export logs to an XLS or CSV file |
| Allows users to create organizational trees and allocate cameras to management organizations. |
| Allows users to add equipment; Supports automatic equipment upgrade, equipment batch configuration, and unified configuration and equipment management |
| Supports centralized authorization and certification and refined rights control; Supports role-based management; |
| Allows the administrator to query user sessions and force a user to log out |
| Allows users to connect to the system by using Windows domain accounts |
| Added watermarks to video to prevent video from being forged, altered, repudiated, or copied |
| Transmission video after being encrypted using AES256 to ensure data security |
| Query cameras to detect network bandwidth. Based on this information, the cameras dynamically adjusts the frame rate and codec quality to ensure smooth video |
| Allows the platform to function as a transmission server. The transmission server can send live video requests to the domain to which the device belongs and multicast the live video streams obtained to the clients. |
| Supports backup of live video and camera recordings on the specified backup server |

### IP Fixed Dome Camera (Indoor Type)

| **Feature** | **Description** |
| --- | --- |
| Type | Dome Camera |
| Basic Requirement | 1 / 2.8 "2 Megapixel Progressive Scan CMOS |
| Effective Pixels 1920 (H) x 1080 (V) |
| Minium illumination: multicolor: 0.02 lux (F1.4,), B/W: 0.012 lux (F1.4,) |
| Focal 2.8mm ~ 12mm, 4.3X, Power Lens |
| Has a day / night functionality with a removable filter section automatically infrared (IR) |
| Function | Support for the Corridor mode (aspect ratio: 9:16) |
| Support ROI |
| Automatic defogging and manual de-mist activation. |
| Intelligent Infrared Lamp, not less than 80m |
| WDR: not less than 120 dB |
| Intelligent analysis, support for Tripwire detection, loitering detection, intrusion detection, detection of abandoned objects, detection of object removed |
| Backhaul Metadata support for intelligent analysis |
| Supports 20% anti-packet loss to protect image quality when IP network qualities are degraded. |
| SD card-based recording |
| Support 1-channel input alarm and 1-channel alarm output (pigtail); Support a self-adaptive RJ45 Ethernet port |
| Video and audio encoding | Video encoding supports H.264 / H.265 and MJPEG, Audio encoding format: G.711a / G.711u / G.726 / OPUS |
| Supports triple streaming; Support for independent encoding of primary and secondary streams in full HD resolution (1080p). |
| Support auto-adaptive bandwidth, smooth streaming, quality QoS parameters, configurable MTU, and IP address filtering. |
| Support for encryption algorithms for bit streams such as AES 128/192/256. Digital watermark support. Support of the authentication function of a user by the username and password; 802.1x support (required to support EAP-TLS), 802.1X PKI access authentication (can be configured via web pages); Support HTTPS. |
| Operating environment | DC12V ± 25%, ± 25% DC24V, AC24V ± 25%, PoE (IEEE 802.3at / af) , Power in hot standby mode, PoE preferred, non-polarized DC power supply |
| -30 ° C to + 60 ° C |
| Reliability during power failure, supports configuration backup file in 2 + 1 mode to avoid power failure in case of configuration |
| IK10 / sealing IP66 or more |
| Certificate | CE, FCC, and compatible with IEC standard 60068-2-11 |

### IP Bullet camera (Outdoor Type)

| **Feature** | **Description** |
| --- | --- |
| Type | Bullet camera |
| Basic Requirement | 1 / 2.8 "CMOS video resolution: 1920 x 1080.  Frame rate: 60 fps.  Resolution 2 Megapixels |
| Minimum illumination: Colour≤0.036 lux at F1.4, B/W≤0.024 lux at F1.4, 0 lux with IR on |
| Lens: 7~22mm Varifocal, Remote focus and zoom, DC-Iris control |
| WDR: 120 dB. |
| The distance of infrared light is not less than 50 m |
| It features day / night functionality with an automatically removable infrared (IR) cut filter. |
| Function | Support image stabilization. |
| Automatic defogging and manually de-mist activation. |
| Support for highlight suppression to reduce reflections especially at night |
| Intelligent detection support (tripwire, intrusion,loitering, abandoned object, and object removed) |
| Supports transmission of video metadata such as color object, classifications of people and vehicles. |
| Supports 20% anti-pack loss to protect image quality when IP network qualities are degraded. |
| Hardware interface | Supports 2 channels of alarm input and 2-channel alarm output; |
| Support 1-channel audio input and 1-channel audio output; |
| Support for an Ethernet RJ45 interface. |
| Video and audio encoding | Video encoding: H.264, H.265 and MPEG. |
| Supports triple flows; Support for independent encoding of primary and secondary streams in full HD resolution (1080p). |
| Support for stream encryption algorithms such as AES 128/192/256. Digital watermark support. Support of the authentication function of a user by the username and password; Support 802.1x, support HTTPS. |
| Support smooth streaming, auto-adaptive bandwidth, QoS quality parameters, configurable MTU, and IP address filtering. |
| Operating environment | Supports DC12V ± 25%, DC24V ± 25%, AC24V ± 25%, and Power PoE. The DC and PoE power adapter serves as a redundant power source. |
| Temperature of operation: -40 ℃ To 60 ℃ |
| Waterproof: IP66 or higher |
| IK10 (excluding front window) |
| Certificate | CE, FCC, and compatible with IEC standard 60068-2-11 |
|  |  |

### IP PTZ ​​Dome Camera (Outdoor Type)

| **Feature** | **Description** |
| --- | --- |
| Type | Speed ​​Dome Camera |
| Basic Requirement | 1 / 2.8 "CMOS video resolution: 1920 x 1080.  Maximum frame rate: 60 fps.  Resolution 2 Megapixels. |
| Minimum illumination: colour≤0.03 lux at F1.6, black≤0.002 lux at F1.6, 0 lux with IR on. |
| Varifocal 4.5-135mm (zoom) lens, 30x optical zoom, 16x digital zoom. |
| The distance of infrared light is not less than 150 m |
| It features day / night functionality with a removable, infrared (IR) filter cut. |
| WDR: not less than 120dB |
| Nail Rotation: Horizontal 0 ° ~ 360 °, Vertical -10 ° ~ 90 ° |
| Horizontal rotation speed: 0.1 ° ~ 240 ° / s, Vertical speed: 0.1 ° ~ 200 ° / s |
| Function | Supports the Gyroscopic-Sensor to ensure image stabilization. |
| Automatic defogging and manual de-mist activation. |
| Highlight suppression to reduce reflections especially in the evening |
| Intelligent support analysis (tripwire, loitering, intrusion, abandoned object, and object removed |
| Supports the transmission of video metadata like the color object, classifications of people and vehicles. |
| Supports Patrol Scan and Scan Pattern |
| Video and audiol encoding | Video encoding supports H.264 and H.265. Audio encoding supports G.711a / u, G.726 and OPUS. |
| Support for encryption algorithms for streams such as AES 128/192/256. Digital watermark support. Support of the authentication function of a user by the username and password; 802.1x support; Support HTTPS. |
| Supports 20% anti-packet loss to protect image quality when IP network qualities are degraded. |
| Supports triple flows; Support for independent encoding of primary and secondary streams in full HD resolution (1080p). |
| Support stream smoothing, auto-adaptive bandwidth, QoS QoS parameters, configurable MTU, and IP address filtering. |
| Hardware Interface | Support 4-channel input alarm and 1-channel output alarm |
|  |
| Ethernet RJ45 interface. |
| Operating environment | Operating temperature: -40 ° C to 60 ° C |
| Waterproof: IP66 or higher |
| Power supply: POE++ |
| IK10 (excluding front window) |
| Certificate | CE, FCC, and compatible with IEC standard 60068-2-11 |

### Camera site

* + - 1. General requirements

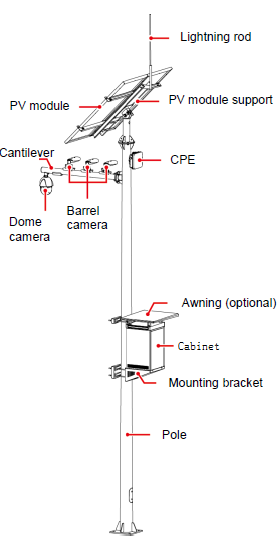
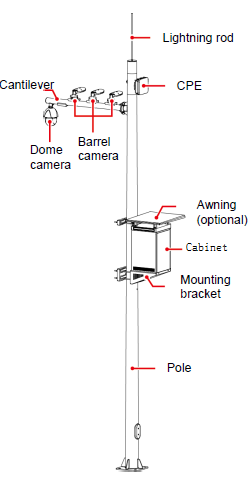
|  |  |
| --- | --- |
| **S/N** | **Description** |
| 1 | The system could output different format of electricity directly to different devices without any kinds of adaptors, including 12Vdc, 48Vdc, and 24Vac. |
| 2 | The power system shall maximum utilize unstable grid in Pakistan, and design protection function for 24 hours at 415V and for 10 minutes at 500V, reducing system damage risk and replacement cost. |
| 3 | The power should be of lightning protection ability (3kA/5kA 8/20μs). |
| 4 | Grid and solar provide power for system, when there is enough sunshine, use the solar energy priority. |
| 5 | The MPPT Tracking technology should be used for solar involved solution, the efficiency of the solar supply unit (SSU) should be 98%, while the tracking precision reaches to 98%. |
| 6 | In order to reduce battery maintenance cost, high temperature battery should be used, the battery could provide serving life as 800 cycles @ 50%℃ DOD,45℃, and the charging current could be 0.3C10 for fast charging |
| 7 | The cabinet should be of high protection level at least IP55 |
| 8 | The bidder is requested to provide a centralized and unified peration support system (OSS) to manager all field site power systems and cameras deployed at camera and eNodeB sites. |
| 9 | The power OSS system shall adopt complete B/S, web-based management structure. C/S management structure plus web browser interface software is not acceptable. |
| 10 | The bidder is requested to provide a centralized and unified operation support system(OSS) to manager all field site power systems and cameras deployed at camera and eNodeB sites. The power OSS shall provide various network KPIs report function, which includes busbar voltage, battery charge/discharge current, load current, battery temperature, active alarms, accumulative load power consumption, battery charge/discharge times, automatic detection for state of health (SOH) of the battery and so on. |
| 11 | The power OSS shall support APP login and operate from a mobile device, which helps users set parameter, view the site status，learn critical alarms and KPI information of sites in real time, thereby ensuring site security. |

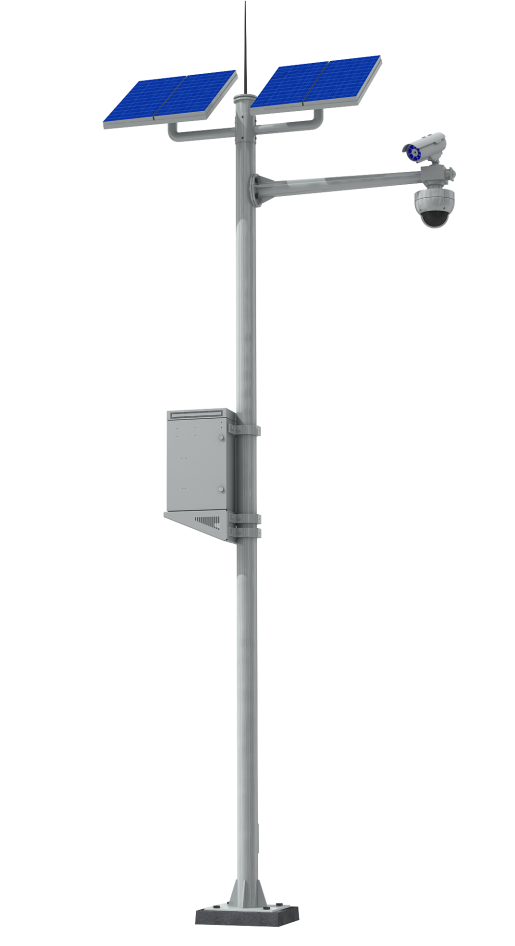
* + - 1. Technical requirements

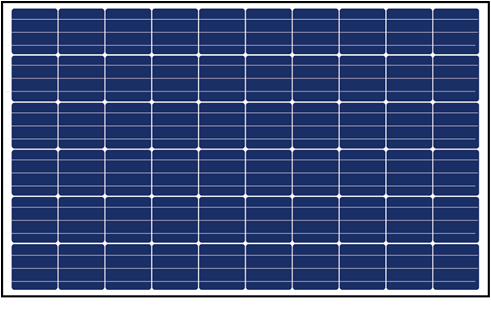
|  |  |
| --- | --- |
| **Item** | **Description** |
| CCTV Camera Pole | Surface treatment: Hot Dip Galvanized and Plastic Spraying(White)  Cantilever height:6m  Cantilever length:1.5m  Wind resistant level:40m/s  Service life: More than 10 years  Control cabinet pole-mounted height:3n  Pole-mounted bear weight：max 200kg |
| Rectifier | Function Module, 1U high and 48VDC-3000W output rectifier with 96% efficiency. |
| Battery | Dimensions (H x W x D): 180 mm x 165 mm x 197 mm  Weight: 13.2 kg  Rated voltage:12V  Maximum charge current:9A  Operating temperature: –20°C to +50°C  Cycle life :800 cycles @ 50%℃ DOD,45℃, and the charging current could be 0.3C10 for fast charging |
| Power cabinet | It includes 12 VDC, 24 V AC, 48 V DC, and 220 V AC. It can provide power for cameras and transmission equipment such as the small-sized router, passive optical network (PON), customer premises equipment (CPE), and access point (AP).  Dimensions (H x W x D): 750 mm x 480 mm x 480 mm  Weight: About 55 kg  Cooling: Free cooling  Operating temperature–5°C to +45°C (When the ambient temperature is above 40°C, an awning is required.)  Cabling mode: Routed in and out from the bottom  Maintenance mode: Operated and maintained from the front  Installation mode: Mounted on a pole or wall  Space for customer equipment:1U  Surge protection：48 Vdc: 10kA/20kA, 8/20µs; 12 Vdc: 3kA/5kA; 24 Vac: 2kA/6kA  Protection level：Equipment cabin: IP55, battery cabin: IP34 |
| Solar panel | Maximum Power\* (Pmax):265W  Rated Voltage at Pmax:30.8V  Rated Current at Pmax:8.62A  Open Circuit Voltage:37.9V  Short Circuit Current:9.25A  Max. Fuse Current rating:15A  Module efficiency:16.3%  Cell size:156\*156mm(6 inch)  Dimensions (L×W×H):1640mm×990mm×35mm(64.6×39.0×1.4inch) |

|  |
| --- |
|  |

* + - 1. Sample of the CCTV Sites.



## ANPR Technical Requirement

### Composition of Checkpoint system

The design of the system is based on the centralized management strategy of distributed system, hierarchical structure design is used, and it is divided into three layers from logical relations: Checkpoint front end subsystem – IP network - Checkpoint access platform. The schematic diagram of the Checkpoint system structure is as follows:

The Checkpoint system consists of Checkpoint front end subsystem, network transmission and back-end access management platform. To achieve the collection, transmission, processing, analysis and centralized management of traffic information. The Checkpoint system access platform is set up with management and control function.

The Checkpoint system consists of Checkpoint front end subsystem, network transmission and back-end access management platform. To achieve the collection, transmission, processing, analysis and centralized management of traffic information.

1. Checkpoint front end subsystem

Be responsible for the collection of vehicle comprehensive information, including vehicle feature photos, license plate number and license plate color, etc.. And complete the image information identification, vehicle speed detection, overspend identification, data caching and compression uploading and other functions. It is mainly composed of high definition capture camera, light-compensating lamp, control (management) host, out-field industrial switch, fiber optic transceiver, switching power supply, lightning protection device and other equipment.

1. Checkpoint access platform

It is responsible for the convergence, processing, storage, application, management and share of relative data in the city, consisting of management platform and storage system. Management platform consists of servers carrying platform software modules, including: Management server, application server, Web server, image server and database server, etc..

### Composition of Checkpoint front-end subsystem

Vehicle Checkpoint system consists of vehicle detection and speed measuring unit, capture and identification processing unit, light-compensating unit, front-end storage unit, network transmission unit and other engineering accessories.

Vehicle detection unit: It has ground sensing coil and vehicle detector, and video detection is implemented in the camera;

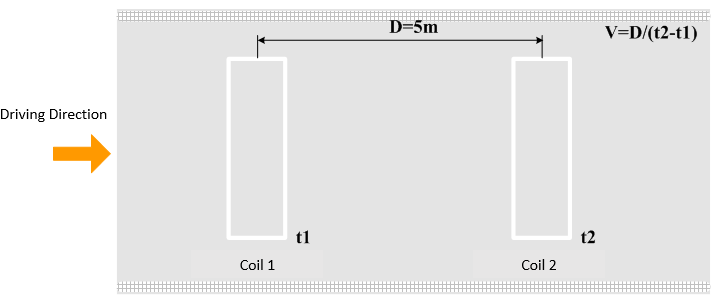
Image acquisition and identification processing unit: It has high definition Checkpoint capture camera, light-compensating lamp and flash;

Front-end storage unit: That is, the control host, which is used to store the front-end video monitoring unit video, Checkpoint image temporary storage and forwarding;

Network transmission unit: Include intersection switch and optical fiber transceiver;

1. Vehicle detection and speed measuring unit

The system uses double coil method for vehicle speed detection, to record the time points the vehicle passes the two coils and calculate the difference value, then calculate the speed of vehicle according to the distance between the coils, and transmit the corresponding speed information to the high definition capture camera at the same time of passing vehicle trigger. Speed detection principle is as shown in the figure below:



Schematic diagram of double coil vehicle speed detection principle

1. Capture and identification processing unit

The capture and identification processing unit is composed of high definition integrated embedded camera, high definition lens and an outdoor protective cover, wherein, the protective cover is provided with 1 network lightning protection device and 1 power supply lightning protection device.

Each lane is deployed with a set of 2 million pixels or more capture and identification processing unit. In principle, 1 set of capture and identification processing unit covers 1-2 motor vehicle lanes, or covers 1 to 2 non-motorized vehicles and sidewalks. High definition capture camera has image acquisition, image processing, virtual loop video detection, license plate identification, vehicle speed measurement, real-time alignment, traffic statistics, data storage and other functions, and it can adapt to a variety of climatic environment, it has stability, reliability and anti-interference ability, data storage, transmission and self-healing function, and time display, character overlap and other functions.

High definition capture camera can outputs high-definition photos and license plate identification data at the same time, and it has strong inhibition function, which can weaken the influence of strong light in the day on high definition capture camera and night light vehicle headlamps on high definition capture video camera shooting. The photos can clearly show the positive image of the vehicle, license plate and facial features of the drivers and passengers.

1. Light-compensating unit

The light-compensating unit of each lane includes 1 set of lighting equipment. Lighting equipment is connected to the high-definition video camera via a signal control line, the flash and light-compensating of the lighting equipment are controlled by the high-definition camera, to ensure clear high definition photos can be captured. Auxiliary lighting and high-definition camera achieve the same frequency control, to ensure the imaging effect of the continuous high definition video shot is always at the best light-compensating moment.

1. Front-end storage unit

The front end storage unit is installed in the control host which is located in the floor cabinet. It is a high performance embedded host, and it is mainly to complete storage and forward function of high definition photos and passing vehicle information. The control host is designed with embedded low power and no fan, which can work normally in the severe outdoor environment. It can provide remote redundant backup of Checkpoint data. The control host can temporarily store traffic data when in poor connection with the center application server network, which will be automatically uploaded and added to the center centralized storage device when the link is restored. This ensures that all vehicle traffic information will not be lost due to network anomalies. The front-end storage device can be configured with industrial hard disk of corresponding capacity according to the specific needs of the project.

1. Network transmission

The network transmission is mainly composed of intersection industrial switch, optical fiber transceiver and optical fiber link, to realize the interconnection between the Checkpoint front end subsystem and the center management platform subsystem. Fiber optical transceivers as well as optical fiber link are provided by the telecom operators.

### Site layout diagram of Checkpoint front end subsystem

The design uses 1 2 million pixel high definition Checkpoint capture video camera covering 1 lane (GB width 3.75m), to ensure full coverage of the field range, in addition to capture normal driving vehicles in the driveway, it also has the function to capture cross-line driving vehicles.

High definition Checkpoint capture video camera and light-compensating lamp are installed on the same pole, and the pole height is generally 6 meters. The projection position of high definition Checkpoint capture video camera and the leading edge of the rear coil are 25-28 meters away. Install holding pole equipment box in the suitable pole position, for mounting the vehicle detector and other accessories. It is necessary to ensure the holding pole equipment box has certain anti-riot ability, it should be made of high quality metal materials and have the characteristics of high temperature prevention, corrosion proof and rain proof.

### Technical Specifications

| **Serial No.** | **Item** | **Description** |
| --- | --- | --- |
| 1 | Vehicle capture rate | For the normal driving vehicles with running speed at 5km/h~200km/h:  Coil detection mode: All-weather vehicle capture rate ≥95%  Video detection mode: All-weather vehicle capture rate ≥90% |
| 2 | License plate identification rate | license plate can be identified; |
| 3 | License plate color can be identified | Black, white, blue, yellow, green |
| 4 | Body color types that can be identified | It can identify common white, gray (silver), yellow, red, green, blue, black and other body colors |
| 5 | Velocity measurement equipment error | Coil velocity measurement mode When the vehicle speed is less than 100km/h, the road measurement error should not exceed -6km/h ~ 0km/h; When the vehicle speed is greater than or equal to 100km/h, the road measurement error should not exceed -6% ~ 0% of the vehicle speed; |
| 6 | Vehicle model identification | Vehicle models include cars, buses, large trucks and small trucks |
| 7 | Image resolution | 2 million pixels is 1600 x 1200 pixel |
| 8 | Image format and space occupation | JPEG, 24bit color, 2 million pixels per image, about 300KB; |
| 9 | vehicle record form | Capture 1 for normal traffic vehicles, and capture 2 for speeding vehicles; |
| 10 | Front-end storage | The control host has large capacity image storage function, to ensure that the traffic records will not be lost at communication failure. The vehicle information storage capacity:≥1 million vehicle images and traffic information. |
| 11 | Network communication interface | RJ45 port, 1000Mbps Ethernet, TCP / IP protocol |
| 12 | Mean Time Between Failures MTBF | ≥5000h |
| 16 | Protection level | The capture controller and the camera are not less than IP65, and other outdoor parts are not less than IP54 |
| 17 | Service voltage | 100VAC～240VAC,48Hz～52Hz |
| 18 | Total system power consumption | ＜900W |
| 19 | Ambient temperature | -10℃～+70℃ when there is no heating or cooling device |
| 20 | Ambient humidity | < 95%@40℃ (no condensation) |

# Express Penalty System

## Overall requirement

The EPS system is expected to provide an integrated technology solution that will:

1. Automate the road transport processes;
2. Centralize road transport data and provide secure access to this data to citizens and stakeholder organizations;
3. Provide online access to citizen services;
4. Allow real time tracking and monitoring of PSV vehicles;
5. Support intelligent traffic management; and
6. Automate enforcement of traffic laws.

System Architecture

The system is designed based on the ESB (ENTERPRISE SERVICE BUS) architecture, due to many interactions with 3rd party systems and all the system functions are released to public services. The architecture is as follow:



ESB is used to integrate all the internal applications, the system then becomes an integrated system, rather than various information islands. All the systems interact with each other through the ESB.

ESB is developed based on the Service-Oriented Architecture (SOA). SOA describes an application integrated model for IT infrastructure. Software components are mutual coupled in a clearly defined hierarchical architecture. ESB is an encapsulated SOA. All the software components and work flows in the TIMS (Transport Information Management System)are published as services through the ESB.

TIMS builds up CDR to achieve the centralized storage and access of road transport related data, including the vehicle registration data, driver’s license data, vehicle inspection data, police enforcement data, and TLB/PSV data. TIMS builds up access secure mechanism to achieve user’s authorization management, the system users include the duty personnel of road transport department, citizens and other organizations.

TIMS supports English, applies HTML, Javascript, CSS and client apps (desktop apps, mobile apps, and flash).

TIMS demonstrates, computes, and transfers data, system working time is from Jan. 1st 1898 to Dec. 31st 2107.

TIMS applies portal technology for the applications, each license application is operated on portal based Portlet. Portal technology can modularize the business services, application Portlet can be applied by inserting license into the Portal platform, so the latest developed license related apps can be visited on the existing websites via browser.

## Technical specification

### General specification

1. Data Integration

For existing data of base system, electronic and manual data, do analysis for its system architecture, data structures and relationships, using the data conversion and integration function to import data leaved in the database and electronic and manual data possibly into a central database, and ensure quality and integrity of the data through finding the intrinsic relationship within data and monitoring data to identify anomalies.

1. Adapters

Can be easily used in common transmission communication protocols: HTTP, FTP, e-mail, file systems, JMS protocols, for third-party systems / product and electronic payment platform, it can develop a corresponding adapter to finish the docking.

1. BMP Workflow

With flexible and customizable workflow management, and release these processes the BPM workflow can help to complete the business process of motor vehicles registration, driver's license registration, transportation business registration, transportation license registration. When there is a change occurring in the registration process, the user can modify the registration process to adapt to new business requirements.

1. Intelligent Route

The service request will be sent to the appropriate service provider in accordance with certain routing rules. In the system, there are some complex business processes, such as to make judgment according to the content of request, to make selection according to the pipes and filters.

1. Service Management

Provide management function for all business services. A large number of services in the system is a big challenges for service management, ESB (ENTERPRISE SERVICE BUS) will become difficult to use and not maintainable if not provide disaggregated view, publish, stop, update service functions, so a strong service management is our guarantee for stable operation of the system.

1. Security Authorization

Provide service authorization according to different user to ensure the safety of services. There are a large number of services registered in ESB (ENTERPRISE SERVICE BUS), using secure authorization is an important guarantee system security.

1. Data Analysis

The analysis and mining to historical data in data warehouse, can provide real-time or regular data analysis services, produce accurate data for reporting and analysis and find the trends from the data, provides strong support for decision-making.

1. Business Service

Based on SOA (SERVICE-ORIENTED ARCHITECTURE), Service is our core business, it integrate various business services, workflow services and report analysis.



1. Vehicle service set

This service set includes motor vehicle registration service, dealer registration service, foreign vehicle permit application and issuance service, vehicle transfer service, and motor vehicle documentation management service.

1. Driver service set

This service set includes DL application service, driving test application service, driving test management service, driver information management service, driver point management service, conductor license management, and DL documentation management service.

1. Vehicle inspection service set

This service set includes vehicle inspection service, outsourced inspection center/garage management service, vehicle registration validation service, and inspection booking service.

1. TLB/PSV service set

This service set includes PSV route management service, SACCO/company management service, TLB license management service, TLB documentation management service, and PSV timetable management service.

1. Enforcement service set

This service set includes traffic offence management service, accident management service, stolen vehicle management service, and offence documentation management service.

1. Electronic payment service set

Every module has a payment service, including payment for vehicle registration, driving testing, driver license issuance, vehicle inspection, and offence fine. The payment services do not interact with the e-payment platform directly but through the ESB.

1. Report and analysis service set

Statement Analysis service set mainly includes: motor vehicle-related reporting services, reporting services related to driver, vehicle inspection reports related services, transportation cards and bus services and the related reports of the statements of enforcement-related services;

1. ETL Service Set:

ETL Service Set mainly focuses on the conversion and processing for the Motor Vehicle Details, Driver / Conductor Details, TLB Data Details, MVIU data Detail, to guarantee data quality and integrity, to achieve the uniform information, to achieve the target of single data source.

1. Service API and Application System

Services in system are all registered in the ESB (ENTERPRISE SERVICE BUS), and let the ESB (ENTERPRISE SERVICE BUS) to manage and give authorization to the appropriate users. These services collections or services are released as API by ESB (ENTERPRISE SERVICE BUS), these API includes: motor vehicle service set API for vehicle registration module, driver service set API for driver testing, vehicle inspection service set API, bus transport service set API, law enforcement services API, as well as the report analysis service set API. These API are integrated together for the self-service portal, for relevant public API to achieve a portal business functions. The isolation between internal API and external API ensures the safety.

1. Third-Party Systems

All the third-party systems and related data sharing and integration are in charge by ESB(ENTERPRISE SERVICE BUS), which including: Motor vehicle registration module integrated part, driving licensing examinations and driving license information sharing module, vehicle inspection module integrated part, transport permit system bus management module integrated part, law enforcement information sharing module is part. ESB (ENTERPRISE SERVICE BUS) will be responsible for third party systems products, and is responsible for release the data out in the form of internal or external API.

### API specification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API name** | **API definition** | **Module** | **Type** | **Invoking Method** |
| vehicle information read interface | [1] read vehicle basic information | Vehicle registration | Information reuse | 1. Vehicle queryVeh(String plateType,Sring plateNo) |
| [2] read vehicle under handling services information | 2. VehBiz queryVehBiz(String sn) |
| [3] read vehicle information through serial number | 3. VehOperatin queryVehOperatinBySn(String sn) |
| [4] read vehicle information through vehicle plate number | 4.VehOperatin queryVehOperatin(String sn,String plateType,Sring plateNo) |
| [5] read vehicle services log information | 5.VehBizLog queryVehBizLog(String sn) |
| [6] read vehicle paper printing information | 6.VehCertificatePrint queryVehCertificatePrint(String sn) |
| [7] read vehicle which is transferred out or cancelled | 7.VehCancel queryVehCancel(String plateType,Sring plateNo) |
| [8] read vehicle sealed up | 8.VehSeizure queryVehSeizure(String No) |
| [9] read new vehicle sequential number | 9.String queryVehNo(String departNo) |
| [10] acquire new vehicle service serial number | 10.String queryVehSn() |
| [11] acquire vehicle’s next expiration date | 11.String queryVehNextCheckEnd(String validityEnd,String VehType,String useage,String registrationDate) |
| write vehicle inspection information | [1] write vehicle inspection result information | Vehicle registration | Information exchange | 1.ResultMessage wtiteVehCheckResult((String plateType,Sring plateNo,String VIN,String checkResult,String checkDate,String checkDepart ) |
| write vehicle number selected information | [1] write vehicle number selected information | Vehicle registration | Information exchange | 1.ResultMessage wtiteVehNumberSelect(String sn,String plateType,String operator,String no,String printTempPlate) |
| write vehicle charging information | [1] write vehicle charging information | Vehicle registration | Information exchange | 1.ResultMessage wtiteVehCharge(String sn,String plateType,Sring plateNo,String remark) |
| [2] delete vehicle charging information | 2.ResultMessage deleteVehCharge(String sn,String plateType,Sring plateNo,String remark) |
| write vehicle pre-input information |  | Vehicle registration | Information exchange | ResultMessage writeVehPreRecord(VehPreRecord record) |
| write vehicle mid-table information | [1] write vehicle insurance information | Vehicle registration | Information exchange | 1.ResultMessage writeVehInsurance(Insurance insurance) |
| [2] write vehicle mortgage information | 2.ResultMessage writeVehMortgage(Mortgage mortgage) |
| [3] write vehicle paying-tax information | 3.ResultMessage writeVehPayTaxes(PayTaxes paytaxes) |
| write vehicle archive number | [1] write vehicle temporary archive number | Vehicle registration | Information exchange | 1.ResultMessage writeVehTempArchives(String sn,String archivesNo) |
| [2] write vehicle main archive number | 2.ResultMessage writeVehMainArchives(String xh,String archivesNo) |
| write vehicle photo information | [1] write vehicle photo information | Vehicle registration | Information exchange | 1.ResultMessage writeVehPhoto(VehPhoto photo) |
| [2] write vehicle photo mid-table information | 2.ResultMessage writeVehPhotoTemp(VehPhoto photo) |
| write vehicle service hand-over information | [1] write vehicle services log information | Vehicle registration | Information exchange | 1.ResultMessage writeVehBizLog(VehBizLog log) |
| [2] update vehicle service table management department | 2.ResultMessage updateVehBizDepart(String sn,String departNo) |
| write vehicle owner’s contact information |  | Vehicle registration | Information exchange | ResultMessage writeVehOwnerContact(OwnerCantact contact) |
| write temporary plate number information |  | Vehicle registration | Information exchange | ResultMessage writeVehTempPlate(VehTempPlate tempPlate) |
| write vehicle queue information |  | Vehicle registration | Information exchange | ResultMessage writeVehQueue(VehQueue queue) |
| write vehicle scrap mid-table information |  | Vehicle registration | Information exchange | ResultMessage writeVehScrap(VehScrap scrap) |
| driving license information read interface | [1] read driving school information | Driver licensing | Information reuse | 1.List<DrivingSchool>queryDrivingSchool(String issuingOrgan) |
| [2] read learner-driven vehicle information | 2.List<CoachCar> queryCoachCar(String drivingSchoolNo) |
| [3] read examination places information | 3.List<ExamPlace> queryExamPlace(String issuingOrgan,String departNo,String examSubject) |
| [4] read examinees information | 4.List<Examiner> queryExaminer(String issuingOrgan,String departNo) |
| [5] read examinee photo information | 5.String queryExaminerPhoto(String identityNo) |
| [6] read examination plan groups information | 6.List<ExamGroup>queryExamGroup(ExamGroupConcon) |
| [7] read examination plan group details information | 7.List<ExamGroupDetail> queryExamGroupDetail(String groupNo) |
| [8] read examination appointment information | 8.ExamAppointment queryExamAppointment(String identityNo,String examSubject,String orderDate,String examPlace) |
| [9] read driving license basic information | 9.DrivingLicense queryDrivingLicense(String identityNo) |
| [10] read driving license service information | 10.DrivingBizFlow queryDrivingBizFlow(String sn) |
| [11] read driving license under-handle service information | 11.DrivingBizFlow queryDrivingBizFlowOn(String sn,String identityNo,String archivesNo) |
| [12] read test card information | 12.TestCard queryTestCard(String sn,String identityNo) |
| [13] read service log information | 13.BizLogInfo queryBizLogInfo(String sn) |
| [14] read historic printing information | 14.PrintHistory queryPrintHistory(String sn) |
| [15] read driver basic information | 15.DriverBaseInfo queryDriverBaseInfo(String identityNo) |
| write pre-input information interface | [1] first claim service pre-input interface | Driver licensing | Information exchange | 1.ResultMessage writeFirstClaimBiz(ClaimBiz biz) |
| [2] physical examination pre-input interface | ResultMessage 2.writePhysicalExamination(PhysicalExamination exam) |
| examination information write interface | [1] appointment information input interface | Driver licensing | Information exchange | 1.ResultMessage writeExamAppointment(ExamAppointmen appointment) |
| [2] examination result input interface | 2.ResultMessage writeExamResult(ExamResult result) |
| Driver licensing service information input interface | [1] charging information input interface | Driver licensing | Information exchange | 1.ResultMessage writeChargeInfo(String sn,String checkItem,String remark) |
| [2] service log input interface | 2.ResultMessage writeBizLogInfo(BizLogInfo info) |
| [3] service hand-over information input interface | 3.ResultMessage writeBizTransfer(String sn,String departNo) |
| [4] service warning information input interface | 4.ResultMessage writeBizWarning(BizWarning warning) |
| Driver licensing information update interface | [1] driver photo input interface | Driver licensing | Information exchange | 1.ResultMessage writeDriverPhoto(String indentityNo,String photo) |
| [2] driver contact information update interface | 2.ResultMessage writeDriverContactInfo(DriverContactInfo info) |
| vehicle single result upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehSingleCheckResult(VehSingleCheckResult result) |
| vehicle inspection decided result upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehDecideResult(VehDecideResult result) |
| vehicle inspection organization information upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehCheckOrganize(VehCheckOrganize info) |
| vehicle detection line information upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehDetectionLine(VehDetectionLine line) |
| vehicle accident forced insurance record upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehAccidentForcedInsurance(VehAccidentForcedInsurance insurance) |
| vehicle inspection result upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehCheckResult(VehCheckResult result) |
| vehicle check braking force curve upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehCheckBraking ForceCurve(VehCheckBrakingForceCurve curve) |
| vehicle check photo upload interface |  | Vehicle inspection | Information exchange | ResultMessage vehCheckPhoto(VehCheckPhoto photo) |
| vehicle check data result interface |  | Vehicle inspection | Information reuse | VehCheckDataResult queryVehCheckDataResult(String sn) |
| vehicle check result interface |  | Vehicle inspection | Information reuse | VehCheckResult queryVehCheckResult(String sn) |
| violation service information query interface interface | [1] query violation basic information | Law enforcement | Information reuse | 1.ViolationBaseInfo queryViolationBaseInfo (ViolationQueryCon con ) |
| [2] query forced measure voucher (violation handling notice) | 2.ForcedMeasure queryForcedMeasure(ForcedMeasureQueryCon con) |
| [3] query electronic monitor text information | 3.ElectronicMonitorText queryElectronicMonitorText(Sring palteType,String PlateNo,String no,String decisionFlag) |
| [4] query electronic monitor photo information | 4..ElectronicMonitorPhoto queryElectronicMonitorPhoto(Sring no) |
| [5] query log information | 5.ViolationLogInfo queryViolationLogInfo(String no,String decisionNo,String forcedMeasureNo) |
| [6] query bank reconciliation information | 6. BankReconciliation queryBankReconciliation (,String decisionNo) |
| Bank reconciliation information input interface |  | Law enforcement | Information exchange | ResultMessage writeBankReconciliationInfo(BankReconciliation info) |
| electronic monitor input interface | [1] electronic monitor input interface(already review) | Law enforcement | Information exchange | ResultMessage writeElectronicMonitorReview(ElectronicMonitor info) |
| [2] electronic monitor input interface(without review) | ResultMessage writeElectronicMonitor(ElectronicMonitor info) |
|  |  |
| simple decision paper input interface |  | Law enforcement | Information exchange | ResultMessage writeSimpleDecision(SimpleDecision desicion) |
| force measurement(violation handling notice) input interface |  | Law enforcement | Information exchange | ResultMessage writeForcedMeasure(ForcedMeasure measure ) |
| electronic monitor simple program handle input interface |  | Law enforcement | Information exchange | ResultMessage writeElectronicMonitorSimpleProgram(ElectronicMonitorSimpleProgram program) |
| administrative detention receipt information input interface |  | Law enforcement | Information exchange | ResultMessage writeAdministrativeDetention(String decisionNo,String delivery,String inDate,String outdate,String manager) |
| bank reconciliation fine receipt serial number edit interface |  | Law enforcement | Information exchange | ResultMessage updateBankReconciliationFine(String decisionNo,String FineReceiptNo) |
| read incidents of criminal cases information |  | Law enforcement | Information reuse | ResultMessage queryIncidentsOfCriminalCases(String incidentesNo, String identificationNo) |
| write alarm information |  | Law enforcement | Information exchange | ResultMessage writeAlarmInformation(Alarm alarm) |
| write easy accident information |  | Law enforcement | Information exchange | ResultMessage writeEasyAccidentinformation(EasyAccident easyAccident) |
| write site map pictures information |  | Law enforcement | Information exchange | ResultMessage writeSiteMapPictures(SiteMapPictures siteMapPictures) |
| write electronic GIS coordinates information |  | Law enforcement | Information exchange | ResultMessage writeElectronicGIScoordinates(String incidentNo,String incidentType, String electronicCoordinates) |
| write basic results in criminal cases |  | Law enforcement | Information exchange | ResultMessage writeBasicResultsInCriminalCases(BasicResultsInCriminalCases basicResultsInCriminalCases) |
| write record of inquiry information |  | Law enforcement | Information exchange | ResultMessage writeRecordOfInquiry(RecordOfInquiry recordOfInquiry) |
| write transcript information |  | Law enforcement | Information exchange | ResultMessage writeTranscript(Transcript transcript) |
| query vehicle decks information |  | Law enforcement | Information reuse | ResultMessage queryVehicleDecks(String plateTypes, String plateNo, String SurveillanceRange) |
| query inform information | [1] query vehicle inform information | Law enforcement | Information reuse | ResultMessage queryVehicleInform(String plateTypes,String plateNo) |
| [2] query driver inform information | ResultMessage queryDriverInform(String IssuingAuthority, String identificationNo) |
| [3] query vehicle triple repeatedly and inform information | ResultMessage queryVehicleTripleRepeatedlyInform(String plateTypes, String plateNo) |
| [4] query vehicle offense violation inform information | ResultMessage queryMotorVehicleOffenseInformOffsite(String plateTypes, String plateNo) |
| write vehicle decks information |  | Law enforcement | Information exchange | ResultMessage writeVehicleDecks(VehicleDecks vehicleDecks) |
| query passenger and freight driver information |  | Law enforcement | Information reuse | ResultMessage queryPassengerAndFreightDriverInformation(String companyNo, String unitName) |
|
| write vehicle pending business informed |  | Law enforcement | Information exchange | ResultMessage writeMotorVehiclePendingBusinessInformed(String informNo, String informUnit) |
| write driver pending business informed |  | Law enforcement | Information exchange | ResultMessage writeDriverPendingBusinessInformed(String informNo, String informAuthorities) |
| write vehicle triple repeatedly violation informed |  | Law enforcement | Information exchange | ResultMessage writeVehicleTripleRepeatedlyInform(String informNo, String informAuthorities) |
| write vehicle offense violation informed |  | Law enforcement | Information exchange | ResultMessage writeMotorVehicleOffenseInformOffsite(String plateTypes,String plateNo) |
| write vehicle deck pictures information |  | Law enforcement | Information exchange | ResultMessage writeMotorCarDeckPictures(String suspectVehicleNo, String no, String picture) |
| SACCO/company information query interface |  | TLB/PSV | Information reuse | ResultMessage queryCompanyInform(Company company) |
| TLB license application interface |  | TLB/PSV | Information exchange | ResultMessage writeTlbLicenseApplication(TLBLicenseApplication tlbcenseApplication) |
| TLB license information query interface |  | TLB/PSV | Information reuse | ResultMessage querytenseApplication(TLBLicenseApplication tlbcenseApplication) |
| bus route information query interface |  | TLB/PSV | Information reuse | ResultMessage queryBusRouteInform(BusRouteInform busRouteInform) |
| bus timetable query interface |  | TLB/PSV | Information reuse | ResultMessage queryBusTimetables(BusTimetables busTimetables) |
| user login confirmation |  | TIMS | Information exchange | ResultMessage queryUserLogin(User user) |

# Emergency Communication System Requirement

## Overall requirement

### Video, Voice, and Data Convergence

The proposed solution must support data and voice services. Data services must include not only the video service, message service, Internet data service, and location based service but also other application services.

The proposed solution must support the combination of services, such as video services (video surveillance/distribution/upload) and non-video services (the call from PSTN/PLMN, individual call, and group call) concurrently.

### Authentication

When a user attempts to access the radio system, the system will verify and validate the radio identity number of the user. If the radio identity number of the user is invalid, the user will be barred from accessing the system.

The system should support the bidirectional authentication between the network and MS.

### IPSec for Base Station

The proposed system must support Internet Protocol Security (IPSec). An IPSec security gateway is added between Base Station and core network. An IPSec tunnel is created between the Base Station and the security gateway to ensure the security of data transmitted between them.

### Remote Handset Disable and Enable

The proposed system must support the system administrator to remotely temporarily stun a handset in the network. If a Handset is temporarily stunned, it can only use the services related to mobility management.

### Geographic Redundancy

The core network, network management system, multimedia dispatching system must support the geographic redundancy function.

## Broadband Trunking Multimedia Dispatching

### General Requirements

The dispatcher is easy-to-use and achieves real-time allocation of personnel and resources.

The dispatcher is comprised of the multimedia dispatching and processing center, multimedia recording and playback server, Dispatch Console and inter-system connection gateways.

The MDC (Multimedia Dispatching and processing Center) is a customized server and controls all services and processes media streams. Different dispatching servers apply to different scenarios, including the vehicle scenario, single station scenario, small network scenario, and large network scenario.

The DC （Dispatching Console） is a terminal platform installed on laptops, desktops, or workstations where dispatchers work. The DC provides man-machine interfaces (MMIs) for dispatching trunking voice services, HD (high definition) videos, and high speed data. The dispatchers can view the user information, the group information, the camera information, the video messages, SMs, and MMs, and can also provide video functions, such as distributing, monitoring, recording, transcoding, and transferring videos to a TV wall.

The MRS (Multimedia Recording and playback Server) provides on-demand services, media recording and media management functions, and access to cameras.

The dispatcher supports hierarchical deployment, with dispatchers serving as either an upper-level dispatcher or a lower-level dispatcher in a network.

The dispatcher supports configuration of one or more virtual private networks (VPNs). VPN services are separate from each other. Logically, users, groups, scheduling server, audio and video server, and gateways are divided into own different network permissions.

With this feature, dispatching systems work in equipment-level redundancy modes. If the active dispatching system cannot provide services because of power-off or other reasons, the standby dispatching system can still provide services.

## Base Station

### General Requirements

The proposed base station must support a frequency band of 1.4GHz（1447MHz~1467MHz）or 400MHz（380MHz~450MHz）for TDD.

The base station must support scalable spectrum bandwidth configuration as below description, for TDD 3 MHz (Supported only by 400M), 5 MH, 10 MHz, 20 MHz are supported.

The proposed base station must support the distributed architecture including base band unit (BBUs) and remote radio unit (RRUs). BBUs are connected to RRUs through optical cables over the common public radio interface (CPRI).

The proposed base station must support “Fallback Mode”. When the communication of core network device and base station is failed, the base station starts the “Fallback Mode”. Voice Trunking service under the base station work normally.

Each base station must support a maximum of 3600 active users at channel bandwidth of 5 MHz/10 MHz/20 MHz.

The proposed system must support uplink power control and dynamic downlink power allocation. Vendor must provide detailed information about the power control mechanism.

The proposed base station must support trunking service and the maximum group number per cell needs to be 160 groups (20 MHz channel bandwidth).

Trunking group call set up time of the base station must be less than 300 ms.

The proposed base station must support the redundant and hot swappable power supply modules.

The proposed base station must provide alarm notification when the cabinet is open, or overheat occurs.

The radio module of proposed BBU must support cascade and the maximum number of cascade is not less than 6.

The proposed base station must support the Fallback Mode, this feature allows the base station disconnected from the CN to support basic functions of PTP calls and group calls within its coverage area.

### BBU Requirements

The BBU must support GPS synchronization.

The proposed BBU must support 12 cells per Base Station.

The proposed BBU must be installed in a free space no more than 19-inch width and 2U height.

The proposed BBU must support two FE/GE optical interfaces.

The proposed BBU must provide an Operate and maintenance channel towards operate and maintenance center (OMC).

The proposed BBU must provide clock ports for clock synchronization, alarm monitoring ports for environment monitoring, and a Universal Serial Bus (USB) port for commissioning the use of a USB storage device.

The proposed BBU must manage the entire base station by means of operation and maintenance (OM) and signaling message processing.

The proposed BBU must support the IP Sec protocol to provide secured backhaul transmission.

The proposed BBU must be modularly assembled to meet different requirements of network capacity and faulty board replacement.

The proposed BBU must have an expansion capability by inserting boards without impacting the existing service and system performance.

Normal power supply for the BBU must be -48V DC (-38.4V DC to -57V DC).

The proposed BBU should be support work in environment temperature of -20°C~+50°C.

### RRU Requirements

The RRU can be installed close to the antenna to shorten feeder length, reduce signal loss, and improve system coverage.

The RRU must be serve to modulate and demodulate baseband signals and RF signals, process data, amplify power and detect standing waves.

RRUs must support 40 W output powers per channel.

Normal power supply of the RRU must be -48V DC (-36V DC to -57V DC).

The RRU must support the natural cooling mechanism instead of a fan.

The RRU can be deployed remotely and the maximum distance between an RRU and a BBU must be no less than 38 km.

The RRU must support environment temperature from -40°C to 55°C (without solar radiation).

## Core Network

### General Requirements

The proposed CN must be modular expandable to increase call capacity, radio site capacity, and gateway capacity. Expansions during the lifetime of the infrastructure must not require replacement of equipment.

The proposed CN must support different services (such as subscriber data management, mobility management, voice trunking, and gateway) with a coherent range of equipment in order to avoid separate and unmanageable solutions.

The proposed CN must use non-proprietary OSs as the basis for all software- and firmware-based components in order to ensure long-term maintenance of the products, and must be certified in real time for carrier grade availability and performance.

The proposed CN hardware must allow software upgrades during the lifetime of the system in order to deliver new functions and bug fixes, without replacing or upgrading equipment.

The vendor must provide high integrated core network. The hardware solution must be compact. It enables the MME, P-GW, S-GW, and HSS to be deployed in one cabinet.

## Terminal

The proposed vendor must provide a series of terminal products, which are not limited to broadband trunked handset terminal, including mobile office terminals, USB dongles, vehicle mounted terminals, broadband access terminals, and mini PCIe LTE cards for customization.

### High Class Handset

The contractor must provide handset terminal with no less than 4.5 inch touch screen.

The proposed handset terminal must integrate private calls, PTT (with entity PTT button), SMS/MMS, video surveillance, and video dispatching for easy operation and smooth collaboration.

The proposed handset terminal must comply with IP67 protection for dust-proof and waterproof.

The proposed handset terminal must comply with MIL-STD-810G standards for anti-drop. The handheld terminals must be robust, waterproof, and enclosed by a die-cast chassis or can withstand dropping test at 1.2 m above concrete ground without any damage.

The proposed handset terminal must provide emergency buttons on the equipment. The emergency buttons must be designed not to be evoked easily by an inadvertent action.

The proposed handset terminal must support dual microphone to guarantee the work in a noisy environment, and speaker output should not less than 2W.

The proposed handset terminal must support 802.11b/g and Wi-Fi hot spot.

The proposed handset terminal and set must support to connect to camera via USB interface and others. Video quality must be up to D1. Video data can be simultaneously displayed in the local and be uploaded to the command center.

The proposed handset terminal must support  specific interface for connecting to a PC

The proposed handset terminal must support the Push To Video(One click Video/ image uploading)

The proposed handset terminal must support digital DMO function and can be used for communication when an area has no LTE signal

### Medium Class Handset

The proposed handset terminal must integrate private calls, PTT, broadband data, SMS/MMS, video surveillance, and video dispatching for easy operation and smooth collaboration.

The proposed handset terminal must comply with IP67 protection for dust-proof and waterproof.

The proposed handset terminal must comply with MIL-STD-810F standards for anti-drop. The handheld terminals must be robust, waterproof, and enclosed by a die-cast chassis or can withstand dropping test at 1.5 m above concrete ground without any damage.

The proposed handset terminal must provide emergency buttons on the equipment. The emergency buttons must be designed not to be evoked easily by an inadvertent action.

The proposed handset terminal must support dual microphone to guarantee the work in a noisy environment.

The proposed handset terminal must support 802.11b/g and Wi-Fi hot spot.

The proposed handset terminal must support two cameras. The rear camera resolution must be no less than 5M pixel and the front camera resolution must be no less than 1.3M pixel.

The proposed handset terminal must support to connect to USB camera. Video quality must be up to D1. Video data can be simultaneously displayed in the local and be uploaded to the command center.

The proposed handset terminal must support the USB 2.0 interface for connecting to a PC.

The proposed handset terminal must support the One click video/image uploading

## Vehicle Mounted Terminal

### Voice trunking requirements

The proposed vehicle mounted terminal must support DMO mode operation.

### Multimedia dispatching requirements

The proposed vehicle mounted terminal must integrate with the following functions private calls, group calls, SMS, MMS, video uploading.

The proposed vehicle mounted terminal must support 1080P 25fps high definition video transmission, dispatching and distribution.

The proposed vehicle mounted terminal must support attached FE cameras for applications in complicated environments.

The proposed vehicle mounted terminal must support one-click video uploading and one-click image uploading.

### Hardware

The proposed vehicle-mounted terminal must support the operation at 5MHz、10MHz and 20 MHz frequency bandwidth.

The proposed vehicle-mounted terminal must support 2.4 inches QVGA resolution (240\*320) TFT screen at least.

The proposed vehicle-mounted terminal must support an intelligent operating system that allows customized development based on industry requirements.

The proposed vehicle-mounted terminal must support air interface encryption and remote activation or deactivation of the terminal.

The proposed vehicle-mounted terminal must comply with IP54 protection for dust-proof and waterproof.

The proposed vehicle-mounted terminal must support the external antenna interface for better coverage.

The proposed vehicle-mounted terminal must support 802.11b/g and Wi-Fi hot spot.

The proposed vehicle-mounted terminal should support the operating temperature from -20°C to 60°C.

The proposed vehicle-mounted terminal must support the 12V DC power supply from vehicle.

The proposed vehicle-mounted terminal must support USB 2.0.

The proposed vehicle-mounted terminal must support the hot MIC function for user's emergency call.

## Telephony Gateway

The telephony gateway needs to provide the cross communication between the digital trunking radio subscribers and an existing telephony system.

The telephony gateway needs to provide required interfaces for existing and legacy telephony systems.

The telephony gateway needs to provide required interfaces for existing wireless and wired telephony systems, namely, the PSTN, GSM networks.

The telephony gateway needs to provide feature transparency between two networks.

The telephony gateway needs to be integrated into the switch itself.

## Trunking Gateway

The telephony gateway needs to provide trunking communications between the digital trunking radio subscribers and an existing trunking system.

The telephony gateway needs to provide required interfaces for existing wireless trunking systems including the analog trunking, TETRA and so on.

## SIP/SDK Interface

The proposed system shall support SIP interface for 2nd development of gateway to other systems.

The proposed system shall support SDK interface for 2nd development of dispatching console or gateway to other systems.

The proposed system supports heart beat detection mechanism.

The proposed interface shall be based on SIP, SDP, TCP/UDP/IP, and RTP/RCTP.

The proposed system supports PCM voice based on G.711 A-Law/U-Law.

The proposed system supports point to point call with others systems through SIP interface.

The proposed system supports point to point video call with others systems through SIP interface.

The proposed system supports push to talk with others systems through SIP interface.

The proposed system supports provide the interface include user management, group management, terminal management, global parameter management, section management, voice VPN account information management etc.

The proposed system supports provide the interfaces for voice (P2P and group), video, SMS, and MMS services, and bi-directional service interconnection.

The proposed system supports report GIS positioning information to third-party systems.

The proposed system supports pan-tilt-zoom (PTZ) control on fixed cameras in the LTE system can be performed by third-party systems.

The proposed system supports third-party systems to obtain information and status about the user, group, and camera

The proposed system supports provide the SDK development manual to the third party.

## Aerial surveillance (UAV)

### Overall requirement

UAV should support police wireless broadband network above, integrate to multimedia dispatching system and video surveillance system, and then upload video to command center via wireless broadband network directly. At the same time, it is able to upload video to dedicated portable notebook when UAV is out of broadband wireless network coverage.



### Technical requirement

Integrate wireless model

Integrate HD/4K camera

Pin sharp digital images at day and night

Payload up to 1200 grams

Flight time up to 88 minutes

Service ceiling up to 4500 meters absolute altitude

Measurement devices for thermography, gas, and radiation

Configuration flexible according to user‘s requirements

Flight by remote control or autonomously by means of GPS

Waypoint Navigation

Technically most advanced control system for position, height, and direction

Integrated flight data recorder for documentation and analysis

Base station user-friendly, with live broadcast

Extremely low noise

Low maintenance

# Command center technical requirement

## Overall Requirement

### Command Center Overview

The Main Command Center shall be located at the Client headquarter. A new Emergency Call Center for calltaking operations, Dispatch Control Center for dispatch operations, Supervisor operation, Training center and a meeting room shall be built on a turnkey all inclusive basis. Layout samples suggested below shown as Figure 5-1 shall be discussed with client to come up with most ergonomic design based on client provided space at Client premises.

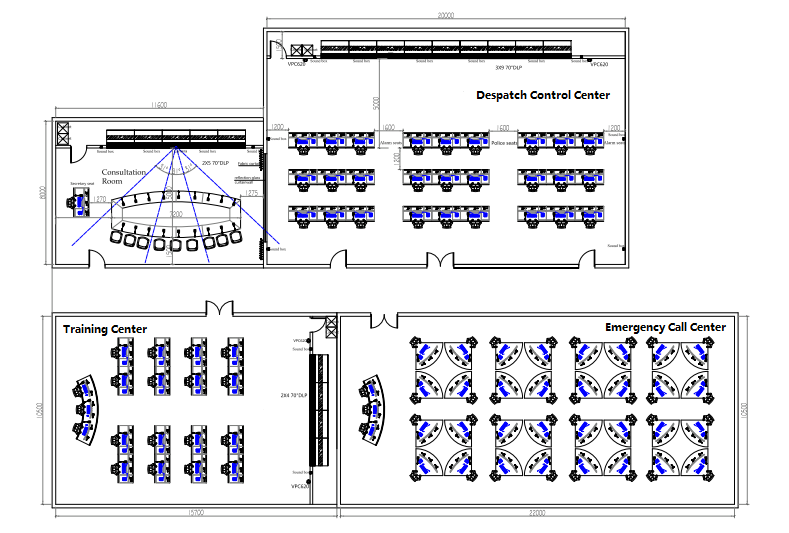


Figure 5-1 Client Main Command Center room layout options

### Emergency Call Centre (ECC)

The Emergency Call Centre (ECC) function is primary point of contact for responding to 999/112 telephony and electronic emergency requests from members of the public, external stakeholders and UPF personnel as illustrated in Figure below.



Figure 5-2 ECC Task*.*

The aim of ECC is to provide support for every emergency request that is received. The service provided by ECC is essentially outward facing, with trained call taking operators handling requests for service from the public and other stakeholders. Calls will either be dealt with and actions completed by ECC operators or they will be transferred, to the appropriate department. The Figure 5-3 below, shows a suggested Call taking and supervisor layout. The Bidder may suggest alternative layout for better and more effective operation.

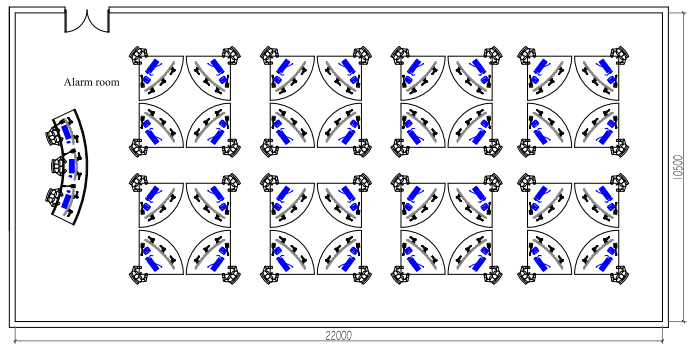


Figure 5-3 ECC room layout example, outlines the layout for the ECC

The requests to the ECC will come from a number of sources and are routed by the Integrated Communication Platform Call Centre (ICP) system to the ECC. These are:

1. A Public Emergency Call – members of the public calling the emergency phone number for the UPF, 999/112.
2. A UPF Internal call – members of the UPF calling the ECC from Police premises.
3. Dedicated Voice Calls – these calls are directed straight to the ECC e.g. VIP emergency calls.
4. Calls from Tetra communication platform provided by field officers (Existing).
5. Possible future (Voice and Video) calls coming from LTE based mission critical communications with video reporting, and video conferencing capabilities.

Once the ECC Operator or Supervisor has received the emergency request, as defined above, an assessment will be carried out using SOPs and FAQs, and an action shall be decided upon. The actions that shall be carried out are:

1. Provide advice and support, with information from FAQs, after which the request will be completed.
2. Create a report that shall be forwarded for action i.e. dispatch may not be required but maybe a visit to the caller number later on if needed.
3. Create a CAD Event Information ticket or report which will be automatically forwarded to the Dispatch Operator by the CAD system.

In the event that an ECC Operator cannot make a decision as to the appropriate action to take he shall send a message through the CAD system to escalate the request to an ECC Supervisor.

In the event that an ECC Supervisor cannot make a decision as to the appropriate action to take he shall notify by sending a message to escalate the request to a DCC Supervisor.

All contacts, either telephony or electronic shall be logged and recorded automatically and annotated with the type of call information.

The ECC shall have the following systems available for the Operator’s use:

1. ICP system - will integrate the telephony system with the external telephony systems used within Uganda and will automatically distribute all incoming telephony to the relevant ECC Control Centre.
2. CAD – will receive and deal with all calls / events distributed from the ICP system using information provided by the following systems:
3. SOPs/FAQs;
4. ANI/LBS/ALI (PACI)/AML (and future eCall)
5. GIS.
6. SOPs/FAQs – shall be the ECC Centre’s repository of procedures and frequently asked questions and answers that will describe how event management, incident management, call receipt, Health and Safety etc. are dealt with.
7. ANI/ALI (PACI) – shall provide location information based on address and shall populate the fields within the CAD.
8. GIS - shall provide a single integrated map of Uganda for the operator and shall integrate with the GAZ i.e. Provide location based information for the CAD and ECC operator showing the event location on a map display screen.

The Emergency Call Centre desktop shall be as shown in Figure 5-5 below:

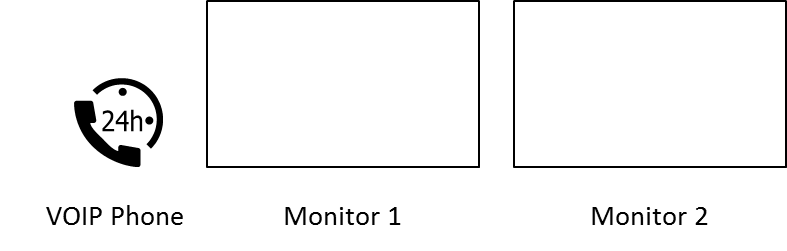


Figure 5-5: ECC Desktop Layout

1. Monitor 1 shall display the CAD system Event Module;
2. Monitor 2 shall display the GIS system Map screen;

The Contractor Shall also provide Video wall (2 Col X 2 row) i.e. 4 discrete LED screens which can display either 1 or 8 images and any supported number in between, for the ECC Supervisors tactical use.

1. 55” Diagonal or higher
2. High definition (1080p)
3. No granular sensation
4. 700Nit
5. Suitable for long term view
6. 7\*24 hours display
7. 05 years continuous operation
8. Video wall controllers for each display area

The number of ECC positions required are 7 Call Takers Supervisor positions and 32 call Takers operators ECC Operator positions per shift.

The Contractor shall provide turnkey furniture for the Control Centre that suits the best possible operation for the call takers and their supervisors.

### Dispatch Control Centre (DCC)

The DCC will provide full primary dispatch and command and control capabilities for the UPF resources that are dispatched to reported events. The Dispatch Operator will organise the dispatch of the resources and will provide support to, and monitoring of, dispatched operational Officers via voice radio and Mobile Data Systems (MDS). A typical DCC is shown in Figure 5-6 below. The Bidder may suggest alternative layout for better and more effective operation.

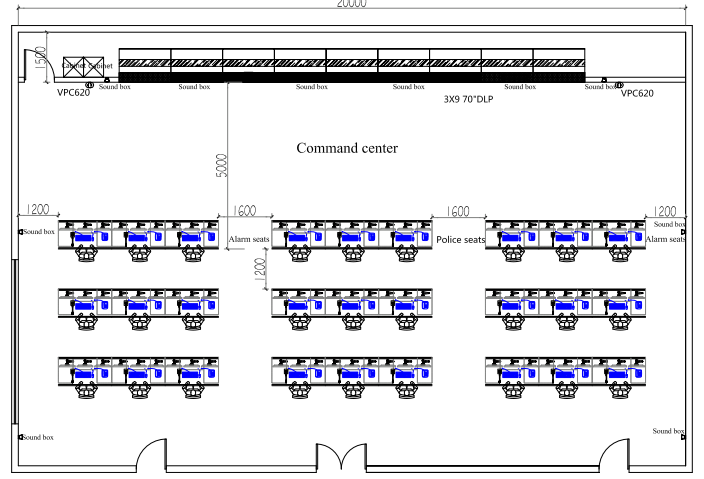


Figure 5-6 Typical DCC room layout example

The DCC workflow. The primary task workflow is shown in Figure 5-7 below. The opened Evened ticket in the CAD system will automatically sent to the Dispatch operator where according to the event types and sub-type the CAD system will define the required security resources types based on certain criteria. The Dispatch operator will be able to quickly dispatch the required resources and follow up with them until the closer of the event.



Figure 5‑7 DCC Layout

The Dispatch Operator shall have access to the Tetra radio network and the IP telephone system.

In the event that a Dispatch Operator is unable to make a decision as to how a CAD event shall be handled, he shall sent a message through the CAD system to escalate the event case to a DCC Supervisor.

The DCC operator will have the following systems for the required operation:

1. CAD Dispatch Module – will receive and deal with all Events / incidents , forwarded from the ECC Call Taker and other CAD creating areas, using information provided by the following systems:
2. SOPs/FAQs.
3. ANI/LBS/ALI(PACI)/AML and future eCall.
4. GIS.
5. ICP – will provide access to the Operational resources that are available to the Dispatch Operator.
6. SOPs – shall be the Command Centre’s repository of procedures that will describe how event management, incident management, call receipt, Health and Safety etc. will be dealt with.
7. ANI/ ALI (PACI) – shall provide location information based on address and shall deliver the information to the GIS when requested by an operator action e.g. a mouse pointer overlaying an address.
8. GIS - shall provide a single integrated map for the operator and shall integrate with the ANI/LBS/ALI(PACI)/AML.

The Dispatch Operator desktop shall have the screens shown in Figure 5-8below:

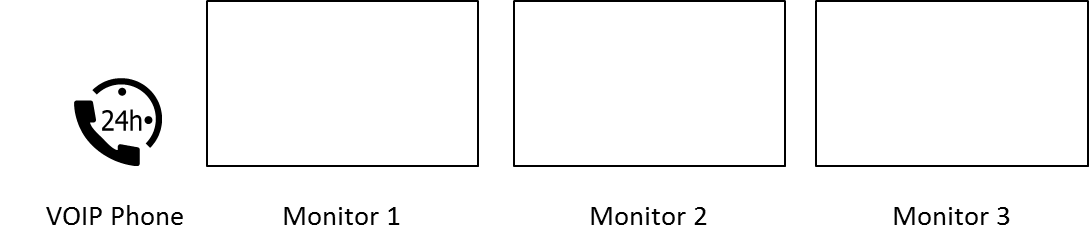


Figure 5‑8 DCC Desktop Layout

1. Monitor 1 to display the related informations system that the Client already have built.
2. Monitor 2 to display the CAD console (Dispatch Module) with SOPs and FAQs, Resources Management System integrated.
3. Monitor 3 to display the GIS Map screen.

The number of Dispatch Operator positions required are 7 Supervisor positions and 35 dispatch Operator positions. 1 Supervisor positions and 7 dispatch Operator positions for each agency: Traffic, GPD, Fire National Security, and Criminal Investigation CID. EMS has existing dispatch operators.

The Contractor Shall also provide Video wall (Left: 5 Col X 2 row, Middle: 10 Col X 2 row, Right: 5 Col X 2 row) i.e. 40 discrete LED screens which can display either 1 or 24 images and any supported number in between, for the DCC Supervisors tactical use.

1. 55” Diagonal or higher
2. High definition (1080p)
3. No granular sensation
4. 700Nit
5. Suitable for long term view
6. 7\*24 hours display
7. 05 years continuous operation
8. Video wall controllers
9. The video wall controller software should take the function to dispatch control video wall system and dispatch surveillance system at one software interface

The Contractor shall provide the furniture for the Control Centre that suits the best possible operation for the Dispatch operators and their supervisors.

### Meeting Room

The Meeting Room shall be equipped but not limited with the following:

1. Dedicated VOIP/Video Conference facility
2. Adequate sitting capacity with training aids like white board and Projectors
3. Video Wall display of 55” with 2x 2 screens
4. Required furniture for the best possible operation of the meeting room

The suggested layout of the meeting room is shown in Figure 5-9 below. The Bidder may suggest alternative layout for better and more effective operation.

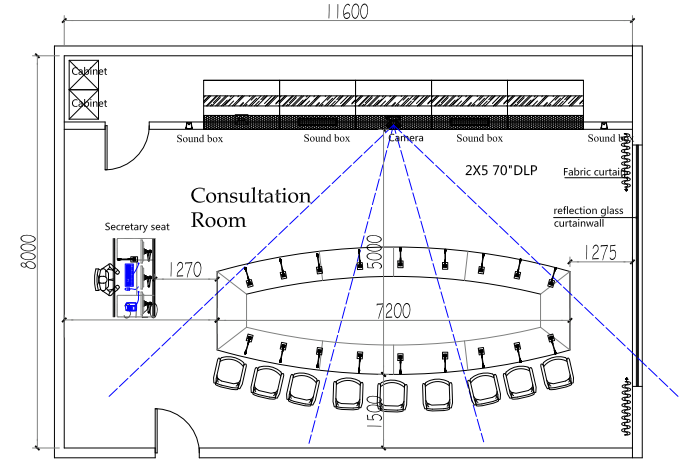


Figure 5-6 Suggested layout of the Meeting Room.

Meeting Room shall have one section for Video wall (2 Col X 2 row) i.e. 4 discrete LED screens which can display either 1 or 8 images and any supported number in between, for the conference use.

## Technical Specifications

### Integrated communication platform

|  |  |
| --- | --- |
| **Multi-channel Alarm Report** | The proposed system should control and distribute calls of different media; it must have the capability to support voice, SMS, and so on. |
|
| One call taker can answer all the alarm channels, such as voice, SMS and so on. Administrator can easily change the multi-channel as their skill. |
| All channel alarms will be in one queue, call takers will answer all the alarms depend on priority and reason not only channel. |
| **Voice & Video Record** | Should support voice conference record， for high recording quality and more safety. |
|
|
|
| One voice record system should support all the call take/dispatch/trunking voice, and have a platform to management all the voice communication. |
|
|
|
| **Converge Call Take & Dispatch** | The proposed system should support call taking and dispatching at the same time and in one meeting, so in emergency cases alarm people and call taker/call dispatcher can talk together and communicate quickly and accurately. |
| All voice terminals can be inducted seamlessly into one conference Integrated communication platform and in this regards, the 1.1.1 Integrated communication platform shall support and integrate the following;  i. PLMN (Public Land Mobile Network),  ii. PSTN (Public Switched Telephone Network),  iii. TETRA Group call (Terrestrial Trunked Radio),  iv. P25 Group call (P25 is a suite of standards involves digital land mobile radio (LMR) services for public safety organizations and agencies),  v. SIP Telephony System, analog phone system. |
| All of the above systems shall be seamlessly inducted into group talking, multiple parties’ conference and other collaboration via integrated communication platform. For example, a Dispatcher shall be able to reach all above types of voice terminals in one single conference so that all related officers can discuss emergency situations together and the Dispatcher can perform one single dispatch to different end recipient source having different voice terminals |
|
| **Trunking Integrated** | The proposed solution should support link to Trunking group, Tetra, LTE, IP Phone, outside terminal can communicate in one meeting. And communication should support PTT function of trunking. |
| The proposed solution should support peer to peer call to LTE trunking group, and answer peer to peer call form LTE. |
|
|
| **Converge Video Dispatch** | In addition, the converged video management and display platform shall be able to show video conferences to allow decision making in conjunction with all video from IP NV and / or LTE being displayed simultaneously along with the video conference. The video conferencing system shall be part of telephony |
| Additional requirements of the converged application platform to support video conferencing is that the integrated communication platform shall provide video conference capability, LTE video, IP NV video and other video terminal (sip or H. 323 based) video in one video conference. |
| INTEGRATED COMMUNICATION PALTFORM functions to administer the video conference shall be at a minimum the following;  i. Display surveillance camera list or LTE handset list;  ii. Initiate video conference;  iii. End video conference;  iv. Preview surveillance or LTE videos;  v. Broadcast Media Channel surveillance or LTE videos;  vi. Perform camera control of PTZ cameras;  vii. Mute/unmute microphones and speakers; and  viii. Display a Social Media Screen in the Video Conference or on the Video wall |
| The converged video can be displayed on the Video walls, operators can change the video wall display in one software platform, and easily do the change. Shall be at a minimum the following;  1.plays video sources from surveillance, trunking, and videoconferencing systems, on video walls by one click. 2. Plays video sources from service systems on video walls by one click. 3. Provided the unified operation page for video sources and devices of which video is played on video walls, and supports unified management and control. 4. Provides SDK that is easy to integrate with GIS and CAD service systems. |
| The proposed solution shall have a converged video platform which integrates video from following sources:  i. IP NV sources,  ii. Video conference Channels,  iii. IP Video from Internet,  iv. 4G/LTE video sources and  v. Any other Video Transmission systems being proposed. |
| **Reliability And Performance** | Any part of our system should run in HA or LB model, so any single point of failure will not affect our business. |
|
| For more maintainability and reliability， every core part of communication platform should be supplied by one company. |
| The proposed system should support different overload control mechanism for rejecting the surge traffic. |
| The system should support high and large traffic capacity.  For one ACD (Automatic Call Distribution) the system should supports the traffic for more than 1000K BHCA (Busy Hour Calling Amount). |
| ACD and record system should support TLS/SRTP. |
|

### Computer Aided Dispatch System

|  |  |  |
| --- | --- | --- |
| **CAD** | Non-voice incident reporting | Allows citizens to report incidents through non-voice means such as SMS messages, and external alarm systems. |
| Integrated incident receiving and handling | Allows call takers to directly dispatch resources without hanging up emergency calls. |
| Wired and wireless incident handling | Adds fixed-line users and trunking users to the same call and supports floor preemption and release. |
| Resting functions for agents | Allows call takers and dispatcher agents to enable and disable suspension or hibernation. |
| Extended incident reception and handling functions | Provides incident takeover request, active incident takeover, incident information update, feedback timeout notification, and SMS message sending functions. |
| **Dispatch system** | Converged commanding | Supports converged commanding and dispatching that integrates wired, mobile, and radio trunk services. |
| **Case analysis system** | Multi-dimensional analysis | Collects statistics on incident reception, handling, and feedback based on multiple dimensions such as incident type, incident severity, incident reporting mode, handling type, jurisdiction, and time. |
| Statistical analysis | Supports overall analysis, criminal incident analysis, public security incident analysis, and key incident analysis. |
| Full-text retrieval | Supports multi-keyword and multi-database synchronous retrieval and allows users to group and filter retrieval results by time, unit, and cause of action. |
| Incident information reporting | Reports incident information daily, weekly, and monthly. |
| Warning analysis | Displays incident trend in an area by different cycles in four colors red, orange, yellow, and green. |
| Research report library | Allows users to upload, download, and query documents. |
| **Integration and connection** | Connection to wireless interface | Allows the ECC software to connect to the radio trunk system. |

### Geographic Information System (GIS)

|  |  |  |
| --- | --- | --- |
| **GIS** | Advanced functions | 1. Users can add, modify, and delete vehicles. 2. The system can analyze the road network to obtain the shortest route between two points. 3. The system allows users to display the real-time police force distribution in an area on the map. 4. The system allows users to specify one or more GPS terminals as key targets to track. 5. The system allows users to display basic information about GPS terminals directly on the map. |
| Radio trunk integration | Supports single call, group call, video call, and SMS message scheduling. |
| Box-select | Users can draw a box on the map to select fixed-line phones and radio trunking terminals in the box to initiate a multi-party call. |
| Box-select Radio terminals to initiate a dynamic group | Users can box-select Radio terminals and add the terminals to a dynamic group that supports voice calling and floor preemption and release. |
| Video surveillance | 1. Supports connection to the IVS system that implements the following functions:  2. Displays video surveillance device locations by device type on maps. 3. Allows users to view live video of cameras on maps. 4. Allows users to control PTZ cameras on maps. |

# Data Center

## Data Center (Layer1)

### General Description

Bidders shall provide two sets of modular data centers for Primary Control Room. For better maintenance and operation, the core components in modular data center must be sourced from one brand, such as modular UPS, precision air conditioner, cabinets, aisle containment and Data Center Infrastructure Management (DCIM) system.

### Racks and Aisle Containment

1. Proposed solution shall support cold/hot aisle containment.
2. Proposed solution shall support single row or double rows deployment.
3. The power density for each rack shall not be less than 6 kW/rack.
4. All racks shall be 42U. The racks shall be used for Servers, Storage, Cabling or networking equipment.
5. Each Rack shall be powered with redundant power supplies.
6. Containment skylight shall be made of toughened glass, and light transmittance shall not be less than 90%. Skylight shall support electromagnetic control, which will be open automatically or manually in case of fire.
7. Internal frame of end door shall be made of toughened glass, toughened glass area shall not be less than 98%, and the thickness of glass shall not be less than 5 mm, and the light transmittance shall not be less than 90%.

### Uninterruptable Power Supply (UPS)

1. TechnicalRequirement

Bidders shall provide two sets of modular UPS system for Primary Control Room and Disaster Recovery Room. Each UPS shall be sized for suitable operation of the proposed system, and batteries shall provide at least 30 minutes back-up time. Bidders shall provide the specific data of the proposed UPS. The power module shall be hot swappable as well as the controller module. The Proposed UPS shall support the following:

* Online double-conversion modular UPS with 3 phase input and 3 phase output.
* High efficiency of up to 96% and the efficiency of commonly used load rate (20%-40%) is no less than 95%.
* High ECO mode efficiency of up to 99%.
* Front maintenance design and possible wall mounted installation.
* Modular design and all the modules shall be hot-swappable, to facilitates capacity expansion and maintenance.
* Wide input voltage and frequency ranges.
* Redundant design for energy controlling module to improve the reliability.
* Output power factor of up to 1, and no derating for capacitive load and inductive load.
* Intelligent battery management to expand battery lifespan not less than 50%.
* Redundant fan system, and each fan can support 30% load.

1. Electrical Characteristics

The following electrical specifications shall be supported:

* Input wiring: 3Ph (L1, L2, L3) +N+PE.
* Input voltage range (Vac): 140-480VAC.
* Input frequency range (Hz): 40Hz-70Hz.
* Input power factor: >0.99 at rated load.
* Output Rated voltage: 380V AC/400V AC/415V AC±1%.
* Overload capacity: 110% overload for 60min; 125% over load for 10min; 150% overload for 1min.

1. Battery

The following Battery specifications shall be supported:

* Battery type: VRLA.
* Intelligent battery management. Moreover, the UPS shall monitor the remaining battery capacity, and predicts the backup time in the case of a mains outage.
* Automatically adjust the minimum battery discharge voltage based on the ambient temperature and takes a battery self-check every 24 hours.

### Cooling System

1. Bidders shall provide in-row precision air conditioner.
2. Cooling system shall be operated in high temperature environment (53 degrees).
3. Specific cooling design for racks consuming above 6kW.
4. Precision Air Conditioner unit shall be equipped with high efficiency DC inverter scroll compressor.
5. Refrigerant of air conditioner shall be R410A.

### Door Access System

1. Access control system shall be auditable and records shall be kept for 6 months.
2. Support both biometric and access card.

### DCIM (Data Center Infrastructure Management)

1. DCIM shall be a unified platform to monitor and manage the data center facilities including power, environment, video, access, and fire alarm.
2. DCIM shall have full functions for operation and maintenance, including management of rights, alarms, logs, reports, views, capacity, power usage effectiveness (PUE), access control and sensors.
3. Support Monitoring, record, and analysis of power usage condition of data center, air conditioners, and power systems.
4. Support raising alarms about capacity thresholds and outages.
5. Support displaying of physical space, load, power and cooling capacity for each cabinet.
6. Support 2-D & 3-D view of the facility including Power distribution schematics.
7. Support real time efficiency monitoring including PUE.
8. Support customizable reports for viewing and export.

## Data Center (Layer2 & Layer3)

### Intelligence Analysis System

1. Vehicle Query with License Plate can track or find the suspects position or activities
2. Support tens of million records can loaded to the analysis platform every day.
3. Support tens of billion records interactive query and analysis from total hundreds of TB data.
4. Thousands cameras provide real-time surveillance of the area. The alarms can be triggered.
5. Video resource sharing effectively supports large-scale video analysis tasks.
6. Dynamic workload awareness of video analysis tasks.

### Video Management Platform

Video Management Platform is designed as an Open Infrastructure Platform for video management system and video content analytics system. It consist of Virtualization operating system, server and storage system. It is recommended that the video management system comply with the following rules.

1. Virtualization OS

Cloud computing platform has the characteristics of on demand service, network access, virtual resource pool, fast flexible architecture, on-demand service and multi-tenant, the cloud computing platform shall satisfy the below requirements.

**Computing Virtualization**

| SN. | Requirement |
| --- | --- |
|  | System must be based on the bare metal architecture. System must make full use of the hardware virtualization technologies of Intel VT and AMD-V and support Intel page expansion. Furthermore, System must be installed on the server hardware that does not have an operating system (OS) installed, and the virtualization software must be able to manage hardware resources. |
|  | System must support SAN boot, host OS can boot from FCSAN. |
|  | System must support CPU QoS configuration to control the minimum and maximum computing capabilities of a VM. |
|  | System must support memory QoS configuration to control the minimum physical memory to be obtained by a VM. |
|  | Different models of CPUs from the same vendor can be grouped into the same logical cluster, which facilitates cluster capacity expansion after the server CPUs are upgraded. |
|  | System must support VM life cycle management, including querying, creating, deleting, starting, stopping, restarting, hibernating, waking up, and cloning VMs. |
|  | System must support secure VM volume deletion that allows users to thoroughly delete all bits of a VM volume, thereby preventing a deleted VM volume from being restored for malicious purposes. |
|  | System must provide the system running recorder function that can automatically store fault information, such as Baseboard Management Controller (BMC) screenshots, CPU sensors, and BMC logs, when the system crashes. The information can be used for fault locating. |
|  | System must support VM affinity rules. VMs that apply the Keep VMs Together rule must run on the same host. VMs that apply the Mutually Exclusive rule must run on different hosts. |
|  | System must support VM HA. |
|  | System must support dynamic power management (DPM) by detecting server load. The system can migrate VMs with light load to other servers and power off the idle servers to save energy, or power on idle servers and migrate VMs from heavy-load servers to the new servers for load balancing. |
|  | System must support dynamic resource scheduling (DRS) that enables the system to flexibly schedule resources and achieve load balancing using the intelligent algorithm based on the system load, thereby enhancing user experience. |

**Network Virtualization**

|  |  |
| --- | --- |
| SN. | Requirement |
|  | Server nodes must support the Open Virtual Switch (OVS) function. The virtual switch must support port aggregation, virtual port management, VLAN management, DHCP isolation, and QoS (traffic shaping and rate limiting) to receive, send, and forward network data packets. |
|  | System must support the distributed virtual switch (DVS) across multiple physical servers. The DVS can be configured on the web client. The virtual ports of the DVS have their own attributes, including the rate, statistics, ACL, and VLAN. The DVS uses port groups to manage the ports with the same attributes. The network port of a VM can be visualized and supports traffic query, DHCP isolation, network QoS (bandwidth limiting and priority setting), and port aggregation. |
|  | System must support binding of the IP address and MAC address of a VM to prevent address snooping and DHCP server snooping. |
|  |  |

**Storage Virtualization**

| SN. | Requirement |
| --- | --- |
|  | System must support the local, IP SAN, FC SAN, and NAS storage devices. These storage resources can be added, deleted, queried, and scanned on the virtualization platform. |
|  | Volumes can be created, queried, attached, detached, deleted, and cleared on storage devices. |
|  | System must be compatible with mainstream SAN and NAS storage devices. |
|  | System must support thin provisioning. The system allocates physical storage space only when data is written into the virtual disk. Storage thin provisioning must support the disk resource shrink function. The shrink function releases the space occupied by the deleted files to increase the available space of the data stores where the virtual disk is stored and improve storage resource utilization. |
|  | System must allow multiple VMs to share one virtual disk, which facilitates the deployment of shared-disk applications on VMs. |
|  | System must support storage QoS configuration to control the I/O upper limit for a VM disk. Any I/O operation from the backend storage device on the VM cannot exceed the configured I/O limit. |
|  | System must support backup for specified disk volume, and save the status of the volume in specified time point, and can create a new volume according to the backup volume to restore the data. |
|  | System must allow users to select whether to thoroughly delete disk data when deleting a user disk, which prevents malicious data restoration using tools and ensures data security. |
|  | System must be capable of virtualizing local disks on hosts into a reliable distributed storage system. A single distributed storage resource pool must support up to 128 resource pools, 49152 local disks, and 4096 hosts. It also must support the full solid-state drive (SSD) deployment mode. |
|  | The distributed storage software must support virtualization deployment on at least VMware, KVM, and XEN virtualization platforms. |

**Enhanced OpenStack Features**

| SN | Requirement |
| --- | --- |
|  | System must support centralized management on physical bare metal servers, System is based on the OpenStack Ironic open architecture and supports the access to and automatic management on standard x86 servers.   * Support resource management and service provisioning and allow automatic loading of mainstream operating systems (OSs) for service deployment on the bare metal servers based on the management system. * Support automatic network configuration for bare metal servers. |
|  | System must support the unified management on mainstream virtualization platforms provided by a third party, for example, VMware.   * Centralized management on newly built VMware vSphere and Openstack operation system * Centralized management on existing VMware vSphere and Openstack operation system * Centralized management operations include unified service provisioning and system maintenance operations on VMs, templates, and networks. |
|  | System must support the Dedicated Cloud (DeC) function. Specifically, a tenant is assigned a cluster of physical servers, and only VMs of this tenant are allowed in this cluster. This ensures the exclusive occupation of physical resources. |
|  | System must support VM high availability (HA) to enable faulty VMs to be automatically restarted in a specific resource pool in the event of a failure, thereby improving VM availability. |
|  | * OpenStack and virtualization platform management nodes must work in active/standby or cluster mode to ensure system reliability. * The heartbeat detection mechanism must be available to monitor the management processes and detect the faulty or zombie management process. |
|  | System must support the automatic backup of management node data so that the management data can be automatically backed up and transmitted to a third-party storage using FTP, S3, or HTTPS. If some or all management nodes are faulty, the backup data can be used to restore the faulty management nodes. |
|  | System must support the following enhanced reliability functions in addition to those provided by the OpenStack community:   * Blackbox: If the Guest OS is faulty, kernel fault information will be stored in the blackbox, facilitating fault locating. * Alarm reporting: If key resources, including hosts, VMs, and network links, are faulty, alarms are proactively reported. * Risk reporting for key processes: If the usage of key resources, including CPU and memory, on key processes exceeds specified thresholds, alarms will be generated, preventing potential system risks. * Exception detection during the VM live migration: If the live migration times out, the system automatically cancels it, preventing resource exhaustion. * MD5 algorithm used for downloading images: This ensures the integrity of downloaded images. * Consistency auditing for management data: This prevents data inconsistency between the management system and computing nodes. |
|  | System must support the following enhanced security functions in addition to those provided by the OpenStack community:   * Data storage encryption: This function encrypts user tokens and passwords. (In the native OpenStack database, a large amount of sensitive information is stored in plaintext. If the database is attacked, severe security risks may arise.) * Data encryption during transmission: The system uses the SSL protocol to encrypt data. (Default data saved in the native OpenStack is transmitted in plaintext. Sensitive user data, for example, tokens, may be leaked, posing security risks.) * Defense against brute force cracking of passwords: If the entered password is incorrect for specified consecutive times, the account will be locked. In addition, the password complexity must meet the specified requirements. (The accounts and passwords of the native OpenStack are easy to be cracked, posing security risks.) * Permission control: Users are granted the minimum permissions to files. (The native OpenStack provides flexible permission control. However, if the system administrator incorrectly configures the system, security risks may arise.) |
|  | System must support dynamic loading of the southbound drive to quickly adapt to heterogeneous hardware devices. |
|  | System must support management of physical devices, including servers, storage devices, and switches. Alarms, performance data, and device status information can be reported in real time. |
|  | System must integrate with the ELK platform log analysis function to provide centralized log management and real-time full-text search, and display search results in graphics. |
|  | System must support the wizard-based installation and deployment tool using Web UI, providing automatic deployment capabilities, simplifying deployment operations, improving the deployment efficiency of the virtualization system, and lowering skill requirements on O&M personnel. |
|  | System must support the wizard-based system upgrade tool using Web UI. Then, the upgrade can be automatically performed with high reliability, improving upgrade efficiency, reducing upgrade risks, and lowering skill requirements on O&M personnel. |
|  | The virtualization platform must support performance optimization of image downloading, improving system service provisioning efficiency. Nova image downloading supports the direct io mode, which enables image downloading directly from the backend storage (S3, Swift, or UDS) without using the image server. This avoids performance bottleneck of the image server in the case of batch image downloading. |
|  | System must support the site replication deployment function. Specifically, you can export the deployed cloud system configuration file and import the configuration file to the new cloud system provided by the same vendor, achieving quick deployment of the cloud system. |
|  | System must support automatic system loading and network configuration using PXE during the replacement of faulty physical hardware. |
|  | System must provide the one-click and wizard-based system health check tool and fault information collection tool. This function simplifies information collection by maintenance personnel and improves system O&M efficiency.   * The health check tool can export health check reports for all components. With the health check reports, technical support engineers and system maintenance engineers can quickly understand system health status in maintenance scenarios including site deployment, inspection, and upgrade. * The fault information collection tool can collect system fault information, facilitating fast fault locating and rectification. System information that can be collected includes OS running environment, hardware and software version information, run logs, performance measurement data, and logs in the blackbox. Logs and system configuration data can also be collected based on requirements. * The fault information collection tool can also collect system logs that record severe system faults, such as blue screen of death (BSOD), Linux panic, no response of the system, and no response of the process. |

**Compatibility and Expansibility**

| SN. | Requirement |
| --- | --- |
|  | System must support x86 servers provided by mainstream vendors and support the management devices that provide the standard intelligent platform management interfaces (IPMIs). |
|  | System must support the IP SAN, FC SAN, and NAS devices provided by mainstream vendors. |
|  | System must support x86 OSs, including Windows Server 2003/2008 R2 and later, Windows XP, Windows 7, and various Linux OSs (such as Red Hat, SUSE, CentOS, NeoShine, NeoKylin, Ubuntu, and Fedora). |
|  | After a physical server with virtualization software installed is added, System must be capable of automatically discovering these new resources and adding them to the virtualization resource pool for centralized management and scheduling. |
|  | System must support smooth expansion of storage devices, disk enclosures, and disks and can add them to a virtualization resource pool for centralized management and scheduling. |

**Requirements for Reliability**

| SN. | Requirement |
| --- | --- |
|  | OpenStack management nodes of System must support the load sharing deployment mode to ensure system reliability. In addition, management nodes can be smoothly expanded to manage clusters in a larger scale. |
|  | The system must provide a web client for data backup and restoration for OpenStack and virtualization platform management nodes to support daily and immediate backup using the third-party FTP server or object storage. The backup period is more flexible. |
|  | System must be capable of monitoring processes of management software in real time and automatically restarting abnormal processes. |
|  | System must support centralized VM HA, independent of management modules. If a VM breaks down due to a server hardware fault or runs improperly due to its OS fault, System must be capable of automatically starting the VM on another properly running server to restore the VM services. |
|  | System must support VM live migration. VMs can be migrated manually or automatically among different physical servers in one cluster without interrupting services. |
|  | System must support storage migration. The volume of a stopped or started VM can be migrated between storage units on the same storage device or different storage devices under storage virtualization management. |
|  | System must support shared nothing VM live migration, which allows VMs to migrate between hosts with different storage media. System must also support shared nothing live migration of the VMs containing snapshots. |
|  | All physical network connections must support dual planes to improve system reliability. |
|  | System must support tenant-level backup, including:   * Enabling tenants to apply for the backup service guided by a wizard * Allowing tenants to configure backup policies and restore VMs through self-service |
|  | System must support agent-free backup. Specifically, you do not need to install the backup agent software on VMs to be backed up. |
|  | System must support LAN-free backup and restoration, reducing impacts on performance of the production server. |
|  | System must support online VM backup. Data of VMs in both running and stopped states can be backed up. |
|  | System must support permanent incremental backup. Only changed data blocks need to be backed up, reducing backup data volume and backup costs. |
|  | System must support the restoration of VM system volume data (installed software, for example). |
|  | System must support flexible backup policies, including:   * Different backup policies for different volume groups * Multiple backup modes, including full backup and incremental backup * Deduplication and compression of backup data * Configurable data backup retention duration and the automatic deletion of expired data |
|  | System must support OpenStack-based cross-DC DR solution, and synchronous and asynchronous replication and DR. The synchronization replication (RPO=0) does not have adverse impact on service hosts.   * Users do not need to install agent software on VMs. * Both system volumes and data volumes on VMs can be restored. * Storage-based replication reduces occupation of computing resources. * DR switchover, DR drilling, and scheduled migration can be implemented by one click, minimizing administrators' manual operations. |

1. Servers for computing platform

The proposed servers are used to provide computing resources for video management system and video content analytics system. Different application system has different requirements of the server detail specification according to application scenarios, so it shall be designed together with application system. But all the servers shall satisfy the below requirements:

Blade Chassis

|  |  |  |  |
| --- | --- | --- | --- |
| **SN** | **Indicator type** | **Indicator** | **Requirement** |
| 1 | Appearance | Device type and height | Integrated blade server  Height: ≥ 10 U |
| 2 | Blade | Quantity | Number of blades in a single subrack: ≥ 16 |
| Co-existence capability | A subrack supports multi-generation Intel processors simultaneously, such as E5 v3, E5 v4, E7 v3 and E7 v4 |
| 4 | Network interconnection module | Switch module slots | ≥ 4 |
| Networking | Supports the GE, 10GE, 40GE, FC, and FCoE switching |
| Eth Switch module configuration | Automatic configuration delivery after hardware replacement |
| 5 | Management | LCD screen | Provides a built-in touch LCD and LCD function description document for users to configure and maintain basic parameters |
| Local KVM | The local KVM function is supported so that all nodes and modules in the chassis can be centrally managed over one physical port |
| DVD-ROM drive | The server can be configured with the DVD-ROM drive |
| Management module | The chassis is configured with redundant hot-swappable management modules. Users can access, manage, and diagnose faults for hardware devices in the blade server architecture locally or remotely using the virtual media and remote KVM |
| Power management | The server provides a power history curve of a single compute node or the entire chassis for one day or one week |
| Stateless computing | The management modules in the chassis provide the stateless computing feature. This feature implements: - MAC address and WWN pooling and allocation - BIOS, NIC, and HBA configuration management - Migration based on blades |
| 6 | PSU | Capacity | Six or more hot-swappable, redundant AC PSUs with a rated power of 2000 W or higher in full configuration |
| Redundancy | N+N |
| Power efficiency | 80 Plus Platinum PSU |
| 7 | Fan module | Fan quantity | ≥ 10 redundant hot-swappable PSUs in full configuration |
| Redundancy | N+1 |
| Maintenance | Fan modules and PSUs are hot swappable and maintained separately. |
| 8 | Environment | Operating temperature | 5°C to 40°C, energy saving and environment friendliness |
| 10 | Service | Maintenance service | The manufacturer shall provide three years of hardware support services since the final system acceptance date. The bidder shall obtain an authorization letter and service commitment letter from the manufacturer |

Blade Servers

|  |  |  |
| --- | --- | --- |
| **SN** | **Indicator** | **Requirement** |
| 1 | CPU | Intel Xeon E5-2600 v3/v4 series processors |
| 2 | DIMM | Memory protection: ECC, memory mirroring, and memory sparing |
| Number of memory slots: ≥ 24 |
| Supports full configuration of processors with the highest power |
| 3 | RAID controller card | Independent RAID controller cards RAID level: 0, 1, 10 |
| 4 | Storage | Built-in disk type: hot-swappable SAS/SATA disk |
| Number of built-in disks: ≥ 2 x 2.5" Capacity of a single disk: ≥ X GB Rotation speed: ≥10000 RPM |
| 5 | I/O module | Number of PCIe3.0 x16 expansion slots: ≥ 2 |
| 7 | Others | Dual SD cards slots, which can be used for creating RAID 1 and on which a boot system, hypervisor, and virtual software can be installed |
| Support 2 Mini SSDs, which can be configured with RAID 1 properties and installed with the system |
| Support PCIe SSDs |
| Support standard PCIe cards |
| One USB flash drive internally |
| 9 | Compatibility | Supports mainstream operating systems (OSs), such as Windows, Redhat Linux, SuSE Linux, and Citrix XenServer |
| 10 | Performance | The SPEC power test result is released to the public at the SPEC website (www.spec.org) for the server model for bidding |
| 11 | Manageability | Manageability and maintainability: 1. Supports integrated system management: - Automatically restarts servers - Monitors and controls fan modules, power supplies, and temperature - Starts and shuts down servers - Restarts servers in sequence - Updates local firmware - Records error logs - Provides a visualization tool 2. Provides GUIs for management and other advanced management functions 3. Provides independent remote management and control ports and GUIs for remote monitoring to implement remote full control over servers independent of OSs. Remote full control includes remote startup, shutdown, and reset, and virtual floppy and DVD-ROM drives |
| Supports the black box function |
| Provides last-screen information |

Storage

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Category | Indicator | Requirement |
| 1 | Architecture | Storage controller | A multi-controller full switching architecture No less than two controllers are configured and connected using high-bandwidth, low latency PCI-E, Rapid-IO or IB high-speed buses, and are not connected using Fibre Channel or IP protocol. The controllers can be expanded to at least four controllers. |
| 2 | Controller load balancing | Host services are balanced among controllers. Controllers need to be switched over due to link faults. Controllers do not need to be reset. The operating system runs properly and services are not interrupted. |
| 3 | Online controller upgrade | One-click online controller upgrade is supported. The storage system can automatically complete internal upgrade and detect the progress of upgrade. |
| 4 | Key hardware indicators | Storage cache capacity | Cache capacity≥ 512 GB |
| 5 | Host port type | Support for 8 Gbit/s Fibre Channel ports, 1 Gbit/s iSCSI ports, 10 Gbit/s iSCSI ports, 10 Gbit/s FCoE ports, 16 Gbit/s Fibre Channel ports, 56 Gbit/s IB ports |
| 6 | Front-end host ports | Supports hot swap of online host port module. Each controller is configured with: 1 x 4x 16 Gbit/s Fibre Channel ports + 1 x 4 x 1 Gbit/s GE host ports+1 x 4 x 10GE host ports |
| 7 | Back-end disk channel | Each controller is configured with: 192 Gbit/s SAS 3.0 disk channels |
| 8 | Supported disk type | Support for SSDs, SAS disks, and NL-SAS disks. |
| 9 | Max. number of disks | The maximum number of supported disk slots must be larger than or equal to 3200. |
| 10 | RAID level | RAID 1, RAID 3, RAID 10, RAID 50, RAID 5, and RAID 6 |
| 11 | Reliability | Fast fault recovery | Fast fault recovery: This is a unique fast recovery technology that minimizes the disk failure period and reduces risks. |
| 12 | Redundancy | Support Redundant power modules, fan modules, controllers, and caches under the power failure protection |
| 13 | Maintainability | Support Hot swappable disks, power modules, and I/O modules |
| 14 | SAN features | Mission-critical service protection software | Support for QoS and user-friendly graphic user interface. Policies are adjusted based on IOPS, throughput, and response time. |
| 15 | Support QoS priority control function |
| 16 | Support Cache partitioning function: This feature ensures sufficient resources for mission-critical services |
| 17 | Support for data destruction. Data can be destroyed using all zeros or randomly written data. |
| 18 | Resource use efficiency improvement | Support for thin provisioning to allocate resource on demand, realize zero detection, and reclaim space that has been deleted to improve space utilization. |
| 19 | Support Automatic storage tiering. The graphic automatic tiering policy adjustment tool is provided to adjust time and tiering method of data tiering and to improve utilization efficiency of storage resources. Hotspot data I/O monitoring can be enabled within a specific time period to automatically migrate data. At least three tiers (SSD, SAS, and NL-SAS) are supported. |
| 20 | Support SSD Cache: This feature improves the response to hotspot data. |
| 21 | Support Multi-tenancy: This feature isolates resources among tenants and implements rights- and domain-based management. |
| 22 | Local data protection | Support Data snapshots. Snapshots at a certain time can be recovered without snapshot loss at other time. |
| 23 | Support Clone |
| 24 | Support Data volume replication |
| 25 | Support Data volume mirroring |
| 26 | Remote disaster recovery protection | Licenses are provided for disaster recovery software based on arrays. Synchronous and asynchronous replication and Fibre Channel and IP link replication are supported. |
| 27 | The GUI can be used to define the time interval for asynchronous transmission of remote data. The time interval for asynchronous transmission is no greater than 10s. Data in the primary data center can be copied to the remote data center through asynchronous array replication. |
| 28 | Support Local high reliability (HA) and active-active storage  Intra-city active-active storage 1) An active-active architecture is provided to realize active-active data backup between two storage systems. The host can concurrently read and write data on a same active-active volume. Breakdown of either storage system will not interrupt operation of the upper-layer service system. 2) The active-active architecture requires an independent third-party arbitration device. When the arbitration device fails, services are not interrupted, and real-time data consistency of the active-active volumes can be kept. 3) Data of active-active engines must be transmitted using Fibre Channel protocol and active-active links (non-IP protocol or IP links). 4) The active-active engines adopt a redundant cluster architecture. Services will not be interrupted when three controllers are faulty simultaneously 5) Capacity licenses are configured for the active-active storage. The capacity is not smaller than that of the disks actually configured. |
| 29 | Compatibility | Compatibility | Support multipathing software: This feature optimizes access path, provides fault switchover and load balancing, and can recognize and optimize three states (available, degraded, and unavailable). |
| 30 | support VMware VAAI, SRM, and VASA compatibility authentication |
| 31 | CTP certificate of SMI-S v1.4 or later |
| 32 | Compatibility authentication of Oracle Database 11g and later versions |
| 33 | Management and maintenance | Manageability | Graphical management software with comprehensive functions: Storage array and volume management software are included. Graphical management software and monitoring software are configured for storage servers. |
| 34 | Unified management | Unified management of full series of storage products |
| 35 | Qualification | Product qualification | CCC, CE, CB, UL, and FCC certificates |

1. Storage for VMS application and VM

The proposed storage are used for cloud platform and VMS application. Provide reliable and high-performance storage resources for video cloud system, it is recommended that the storage system comply with the following rules:

1. Central Storage for video data

Based on customer requirements, the proposed central storage are used as video storage. Provide reliable and high-performance storage resources for VMS system, it is recommended that the storage system comply with the following rules:

**Security and Reliability**

* Supports a distributed architecture.
* Provides high availability in terms of hardware, data, and service, meeting availability requirements.
* Maintains service continuity when the system component damage exceeds the upper limit, although loss of some images is allowed.
* Provides adequate data redundancy and data error tolerance capabilities.
* Employs advanced technologies and mechanisms to ensure data reliability.
* Prevents data loss in the event of storage node damage (including the damage caused by a disk or cabinet fault).
* Implements data self-healing in the event of data corruption.
* Provides effective measures to secure login and access, protecting the network against attacks.
* Prevents data loss in the event of an unexpected power failure. After the power supply recovers, the storage system automatically starts and resumes connections.
* Adopts system components that are capable of working continuously for 24/7 hours under heavy loads.

**Scalability**

* Has robust scalability, supporting data storage at a 50 PB level.
* Supports one-click deployment and installs a single node within 5 minutes.
* Improves performance in line with capacity expansion.
* Uses standard components for flexible replacement and capacity expansion.

**Standard Compliance**

* Complies with international standards.
* Keeps in line with development trends of storage technologies and the IT industry. All used product models have a high-volume production.
* Adopts cutting-edge technologies, making itself constantly up-to-date.
* Presents an industry-leading processing capability and meets future upgrade requirements.

**Openness**

* Supports international standard network storage protocols and open application protocols.
* Works compatibly with mainstream servers.
* Supports mainstream operating systems and applications.
* Enables customized management and maintenance by being integrated with third-party management platforms.
* Provides sufficient scalability for future expansion.

**Maintainability**

* Supports self-healing and provides fully redundant storage space to improve maintenance.
* Provides a multilingual user interface that is easy to use.
* Supports management of permission, logs, and faults and automatic alarm reporting upon faults.
* Simplifies device installation and usage, requiring no professional maintenance personnel.
* Supports on-demand and online system capacity expansion without interrupting services.
* Supports hitless upgrade of system functions.
* Implements web-based or centralized management.

**Cost-Effectiveness**

* Provides the optimal price/performance ratio, compared with counterparts under same conditions.

**Energy Conservation**

* Meets requirements on environmental protection and energy saving, such as low noise, low power consumption, and zero pollution.
* Uses unleaded components.
* Employs energy-saving technologies.
* Obtains environmental management certification, uses recyclable packaging materials, and supports re-utilization.

The storage systems shall satisfy the below requirements:

|  |  |  |
| --- | --- | --- |
| Main Feature | | Requirement |
| Product requirements | | An international brand; non-OEM product with independent intellectual property rights; not developed based on open-source software, such as Lustre and Ceph |
| Vendor qualification | | 1. Independent intellectual property rights and independent hardware/software R&D capabilities to ensure continuity of subsequent products, self-developed file system, which is not based on open source software 2. A company that has the highest right to vote in the Storage Networking Industry Association (SNIA) 3. World famous distributed storage, recognized by Gartner or IDC; providing ranking of key competitiveness on similar products performed by Gartner or IDC |
| System architecture | System architecture | Fully symmetric distributed architecture, with performance and capacity linearly increasing with the number of nodes |
| System scalability | Linearly scalable to at least 144 nodes |
| Global namespace | All nodes can form a complete file system, so that applications can access data in the file system through any node and any frontend network.  All files in the system are accessible (when a user has the required rights) through different network interfaces, such as 10GE, InfiniBand, or GE. |
| Storage capacity | Single file system capacity scalable to a maximum of 50PB; |
| Data protection | Supporting the N+M redundancy mode. Zero data loss can be ensured when up to four nodes fail at the same time (for object storage, zero data loss can be ensured when up to three nodes fail at the same time). The current configuration can tolerate the failure of up to x nodes/controllers and ensure service continuity and zero data loss. Different protection levels can be provided for different data according to the directory-based redundancy ratio policies. |
| Frontend backend network separation | To prevent impact of internal traffic generated by data reconstruction and dynamic storage tiering (DST) on frontend services, and to ensure network security, configure an independent backend network interface card (SAS, Ethernet, or InfiniBand) and switch to carry internal flows. If the switch needs to be shared to simplify the networking, configure VLAN to implement logical isolation. |
| Front-end network connection | Support for 10GE, GE networking modes |
| Back-end network connection | Support for 10GE, 40 Gbps InfiniBand and 56 Gbps InfiniBand networking modes, with 20+ Gbps communication bandwidth between nodes |
| Redundancy | Redundant networking deployment, preventing single points of failure |
| Global cache | Global cache is configured to improve the storage access efficiency |
| Online expansion | Online expansion during system expansion. New capacity and performance of added nodes are available in 12s. The new nodes can balance data with existing nodes. |
| Supported protocols | | Dedicated storage operating system (non-Windows operating system) |
| Supports NFS (V3/V4), SMB (V1/V2/V3), HDFS (supporting interconnection with Cloudera), FTP, NDMP, and OpenStack Swift interfaces. |
| Support for integration rights management on NIS, Microsoft Active Directory, and LDAP |
| hardware | Supported disk types | At least two types among SSD, SATA, SAS, NL-SAS |
| Disk configuration | SATA or NL-SAS disks configured as data disks |
| CPU number of a single node | Dual, Intel Xeon processor |
| NVDIMM | NVDIMM/NVRAM ≥ 8 GB per node |
| Memory | Default: 32 GB  Maximum: 96 GB |
| Data recovery | | To ensure data reliability, the recovery rate should be lower than 1 TB/hour. In this case, data reconstruction for a single disk will take less than 6 hours. |
| NAS Storage Software functions | | 1. Client connection load balancing software can be configured. The load balancing policy covers the CPU usage, network bandwidth, number of TCP/IP connections, round robin, and node capability value. 2. If load balancing is not supported, third-party commercial load balancing devices must be added in the bidding. |
| Support for space quota management based on users, user groups, and directories; support for at least eight layers of directory nesting; and support for integration rights management on NIS, Microsoft Active Directory, and LDAP. |
| Thin provisioning is configured. Storage space is dynamically allocated on demand to ensure an optimal use of storage resources. |
| Support configure Video surveillance image repair, if part of the Video surveillance image lost, the rest Video surveillance image can also be replay |
| Management | Manageability | GUI-based management software with diversified functions Web-based or GUI-based remote management A graphical system structure for monitoring all components of a storage system Statistic reports, monitoring analysis, trend analysis, performance comparison, and diagnosis analysis |
| SNMP | Supported |

1. Video management Software

Video management software must meet the following requirements:

| **Type** | **Description** |
| --- | --- |
| Software | Supports multi-level and multi-domain management, interconnection of more than 128 external domains, and interconnection of up to eight platform levels |
| Supports at least 5000 users for a single domain and allows 2000 users to connect at the same time and 500 users to perform operations at the same time |
| Displays live video information, including the camera name, bit rate, frame rate, and encoding format |
| Supports auto-adaptive aspect ratio window size adjustment. |
| Transfer of video stream from PUs to CUs in direct connection mode |
| Supports live and recorded digital video zoom (even video taken by non-PTZ cameras are supported) |
| Supports playback of at least 25 records at the same time; Allows users to play at least eight videos recorded simultaneously; Allows users to control playback (fast forward, slow play, and jump to a specific time point) |
| Allows users to play back recordings using the following controls: slow reverse (1 / 4x and 1 / 2x), fast forward (2x, 4x, 8x and 16x), slowdown (1 / 32x, 1 / 16x, 8x, 1 / 4x and 1 / 2x), rewind (2x, 4x, 8x and 16x), drag and frame |
| Allows users to view monitoring sites on the electronic map and playback of video shot by cameras at a specified monitoring site; Allows users to zoom in on an area by scrolling the mouse wheel, dragging and moving the map, viewing the map in full screen, panning up, down, left, and right, and controlling the map Scale of the map |
| Allows users to add cameras and alarm source icons to the electronic map |
| Allows users to create sensitive areas. |
| Allows users to start the live video display in an independent window by clicking on the camera icons on the cards; Allows users to take snapshots, record video to local disk, bookmark video, and allow 3D positioning in the video window displayed in real time |
| Allows users to receive, query, and alarms processing and set severity of alarm (warning, minor, major or critical) |
| Links the central platform to perform the following actions when an alarm is triggered: video recordings, captures takes, invokes predefined positions, displays video on clients or video walls, and provides Boolean value outputs; Allows users to manage protection zones |
| Supports scheduled recording by specifying a time segment on the timeline. |
| Allows users to set triggered snapshot alarm policies, including the amount and interval of snapshots; Allows snapshots taken by the cameras to be automatically downloaded to the image server; Allows users to query, preview, delete, download and print snapshots |
| Manage system logs, alarm logs, device logs and logs; Allows users to query logs by user, time, type, or level; Allows users to export logs to an XLS or CSV file |
| Allows users to create organizational trees and allocate cameras to management organizations. |
| Allows users to add equipment; Supports automatic equipment upgrade, equipment batch configuration, and unified configuration and equipment management |
| Supports centralized authorization and certification and refined rights control; Supports role-based management; |
| Allows the administrator to query user sessions and force a user to log out |
| Allows users to connect to the system by using Windows domain accounts |
| Added watermarks to video to prevent video from being forged, altered, repudiated, or copied |
| Transmission video after being encrypted using AES256 to ensure data security |
| Query cameras to detect network bandwidth. Based on this information, the cameras dynamically adjusts the frame rate and codec quality to ensure smooth video |
| Allows the platform to function as a transmission server. The transmission server can send live video requests to the domain to which the device belongs and multicast the live video streams obtained to the clients. |
| Supports backup of live video and camera recordings on the specified backup server |