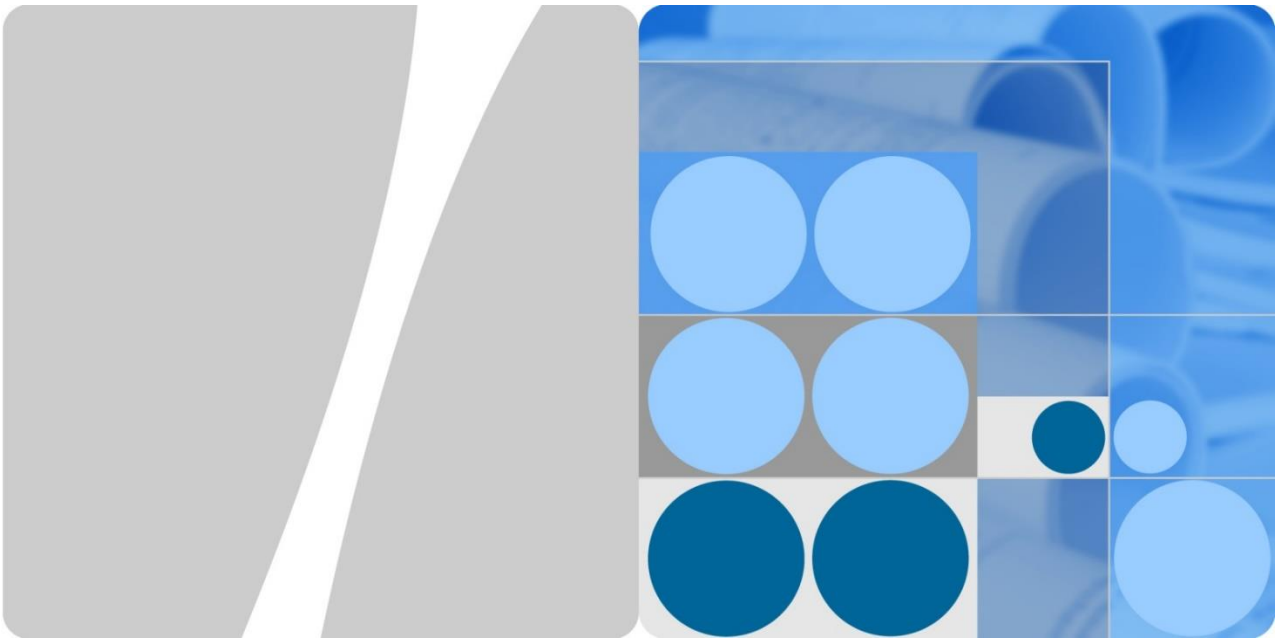


Huawei CloudIVS 3000 V100R019C10

Technical White Paper

Issue 1.1

Date 2018-12-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

Contents iii

1 Architecture Design 1

1.1 Background 1

1.2 Differences Between the CloudIVS 3000 and the CloudIVS 9000 1

1.3 Logical Architecture of the CloudIVS 3000 2

1.4 Constructing O&M Capabilities of the CloudIVS 3000 Based on the CSP OM 4

1.5 Integrating VCN and VCM Architectures in the CloudIVS 3000 4

1.6 CloudIVS 3000 Product Models 7

1.7 Critical Business Services 7

1.7.1 Analysis Service 7

1.7.2 Recording and Forwarding Services 8

1.7.3 Data Search Service 9

1.7.4 Middleware 10

2 Key Technologies 11

2.1 Differences and Similarities Between VMs and Docker Containers 11

2.2 Comparison Between VMs and Docker Containers 12

2.3 HASEN and Docker Containers 12

2.4 CSP Edge 13

2.5 UVP 13

3 CloudIVS 3000 Key Features 14

3.1 Data Safe Technology 14

3.2 Safevideo: Fast RAID Initialization 15

3.3 Safevideo: No Copyback of Hot Spare Disks in the RAID Group 16

3.4 Safevideo: Continuous Readability in the RAID Group 18

3.5 Safevideo: Load Balancing Among RAID Groups 19

3.6 SafeVideo+: Writability Upon Failure 21

3.7 SafeVideo+: Online Capacity Expansion 22

3.8 Cloud-based Cluster Management Technology 23

3.9 Media Format Processing 24

3.10 Search Acceleration 25

3.11 Distributed Computing 26

3.12 Multi-Algorithm Warehouse 28

3.13 Video Quality Diagnosis 28

3.14 Video Surveillance O&M Tool 29

3.15 Cloud-Edge Synergy 30

3.16 Centralized Management of Containers and VMs 30
3.17 GDPR Compliance 31
4 Analysis Algorithm Features and Principles 32
4.1 Vehicle Recognition 32
4.1.1 Application Scenario 32
4.1.2 Customer Benefits 32
4.1.3 Technical Principle 32
4.1.4 Function Description 34
4.2 Facial Recognition 35
4.2.1 Application Scenario 35
4.2.2 Customer Benefits 35
4.2.3 Technical Principle 36
4.2.4 Function Description 39
4.3 Person Search by Image 40
4.3.1 Application Scenario 41
4.3.2 Customer Benefits 41
4.3.3 Technical Principle 41
4.3.4 Function Description 41
4.4 Video Synopsis 43
4.4.1 Application Scenario 43
4.4.2 Customer Benefits 44
4.4.3 Technical Principle 44
4.4.4 Function Description 47
4.5 Video Search 47
4.5.1 Application Scenario 47
4.5.2 Customer Benefits 48
4.5.3 Technical Principle 48
4.5.4 Function Description 49
4.6 Behavior Analysis 50
4.6.1 Application Scenario 50
4.6.2 Customer Benefits 50
4.6.3 Technical Principle 51
4.6.4 Function Description 52
5 Sensitive Feature Disclaimers 59
6 Appendix A References 61
7 Appendix B Acronyms and Abbreviations 62

1 Architecture Design

1.1 Background

In lightweight scenarios, CloudIVS 3000 series provide a lightweight architecture and cloudification features, use bare-metal containers, and provide a container-based framework based on Cloud Service Platform Edge (CSP Edge) and local hard disks. Intelligent Video Surveillance (IVS) services are deployed in containers. TheV100R 19C10 version adds support for virtual machines.

The CloudIVS 3000 is designed to focus on lightweight deployment scenarios. Due to limited hardware resources, containers are used to replace the IaaS layer. Besides, the architecture is adjusted and resources are downsized for IVS and CSP services.

The CloudIVS 3000 shall deploy and run service applications through the lightweight container technology based on the physical server operating system and keep the features of a cloud-based system such as elastic scaling as well as automatic deployment and upgrade. This helps lower virtualization resource consumption and build a cloud-based system whose performance is equivalent to or outcompetes that of peer vendors' bare-metal processes. Therefore, a container-based application life cycle management solution needs to be developed to build a high-performance container network and effectively manage container storage volumes. Additionally, a container-based application reliability solution shall be provided.

1.2 Differences Between the CloudIVS 3000 and the CloudIVS 9000

Based on the cloud-based architecture of the VM running environment, CloudIVS 9000 uses FusionSphere as the management platform at the IaaS layer as well as FusionStage or PaaSCore+CSP as the management platform at the PaaS layer, and remould VCN and VCM into CloudVCN and CloudVCM.

In lightweight deployment scenarios, Application services are deployed based on servers, HostOS (EulerOS), and bare-metal containers to reduce the resource occupied by the IaaS and PaaS layers. At the same time, the boundary between the VCN and the VCM is blurred due to edge intelligence. In the minimum configuration scenario, just one physical CloudIVS 3000 node can support video access, storage, forwarding, video analysis, video search, alert deployment, and provide interface APIs.

1.3 Logical Architecture of the CloudIVS 3000

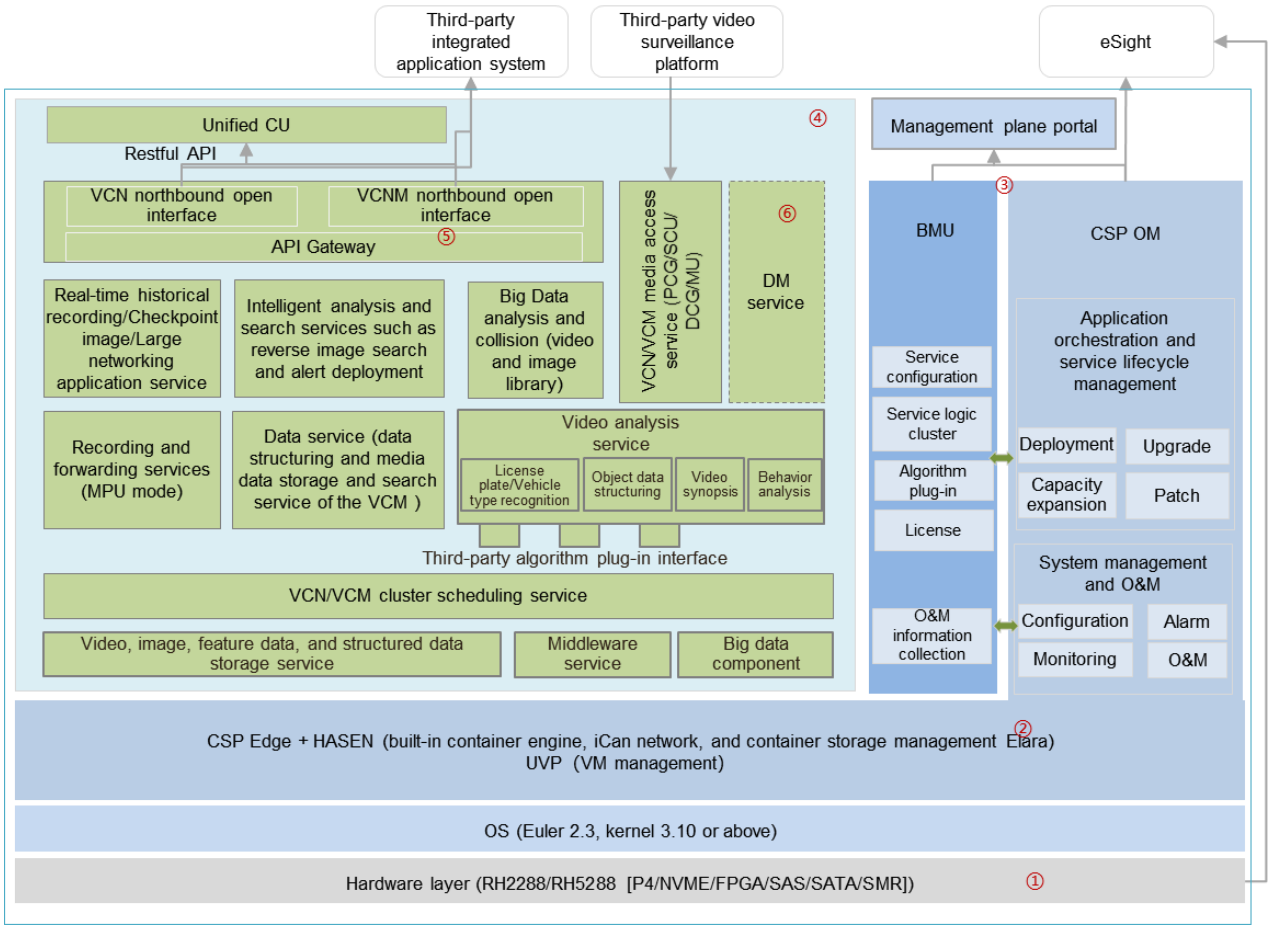
The CloudIVS 3000 adopts the lightweight cloud-based architecture based on bare-metal containers. The CloudIVS 3000 uses Central Software Institute's High-Performance and Advanced Scheduling Engine (HASEN) technology to manage containers throughout the life cycle (including deployment, capacity expansion, upgrade, and patch installation); uses Central Software Institute's iCanal technology to manage the container network; uses the Central Software Institute's ELARA technology to manage container storage volumes.

The CSP platform encapsulates the preceding container technologies, implements the container software warehouse and enhanced reliability features, and develops the CSP Edge solution for scenarios whereresources are limited.

The CSP Edge and CSP have the same basic architecture, ensuring the architecture base consistency between the CloudIVS 3000 and the CloudIVS 9000. The IVS encapsulates VCN and VCM service components in containers and implements application deployment and operating status management based on the CSP Edge. It implements all-cloud features based on bare-metal containers, converges traditional video surveillance services with intelligent video analysis services, provides unified APIs to build an open ecosystem, and enhances design for DFX capabilities such as reliability and serviceability.

CloudIVS 3000 V100R019C10, based on CloudIVS 3000 V100R019C00, adds the bare-metal virtualization feature to support third-party applications and allows the Huawei Unified Virtualization Platform (UVP) to be directly deployed on physical machines to create and manage VMs.

Figure 1. Logical architecture of the CloudIVS 3000



The following describes the logical architecture of the CloudIVS 3000 in detail:

① Supports software and hardware decoupling. To deploy a new hardware device that is not included on the list of supported hardware, it needs to verify the hardware performance and specifications and streamline the end-to-end processes such as configurator configuration, installation, and deployment.

② The infrastructure layer supports container operating systems, application installation and deployment based on bare-metal containers, container life cycle management, heterogeneous resource management and scheduling (HASEN), and container network and storage management. And through the UVP to achieve virtual machine life cycle management and other functions.

③ The CSP Edge is used to support service installation and deployment, upgrade and capacity expansion, and O&M capabilities.

④ VCN and VCM service components are split into loosely coupled services that can be deployed on different physical nodes as required. The service capabilities can be shared, blurring the boundary between the VCN and the VCM.

⑤ The CloudIVS 3000 opens northbound interfaces of the VCN and VCM through the API Gateway and supports coarse-grained scenario-based interfaces.

⑥ (Optional) The CloudIVS 3000 integrates the Device Management (DM) service, enabling configuration and algorithm upgrade for a large number of IP Cameras (IPCs).

1.4 Constructing O&M Capabilities of the CloudIVS 3000 Based on the CSP OM

Currently, the VCN has the VCN OMU service and the VCM has the VCM SEM service to provide device O&M functions separately. The VCN and VCM have an independent database separately. This increases OM architecture redundancy and maintenance workloads. To integrate the O&M capabilities of the VCN and VCM, the CloudIVS 3000 migrates all O&M capabilities to the CSP.

In CloudIVS 9000, the CSP supports IVS installation, upgrade, and deployment. In CloudIVS 3000 all O&M functions such as configuration, alarm, monitoring, log, information collection, and northbound interconnection are migrated to the CSP that is connected through the CSP OM SDK for O&M management. The alarm, monitoring, log, information collection, and eSight interconnection management functions of the OMU and SEM are switched to the CSP. Each service invokes the CSP SDK interface to communicate with the CSP to complete service processing.

At the same time, the following configurations which are available on the VCM_APP Portal (B/S client for users) in are migrated to the OM in CloudIVS 3000: VCM upper- and lower-level domain configuration, VCN interconnection configuration , electronic map service interconnection configuration, and AD domain interconnection configuration. . Additionally, the static map configuration which is available on the VCN client is also migrated to the OM in CloudIVS 3000.

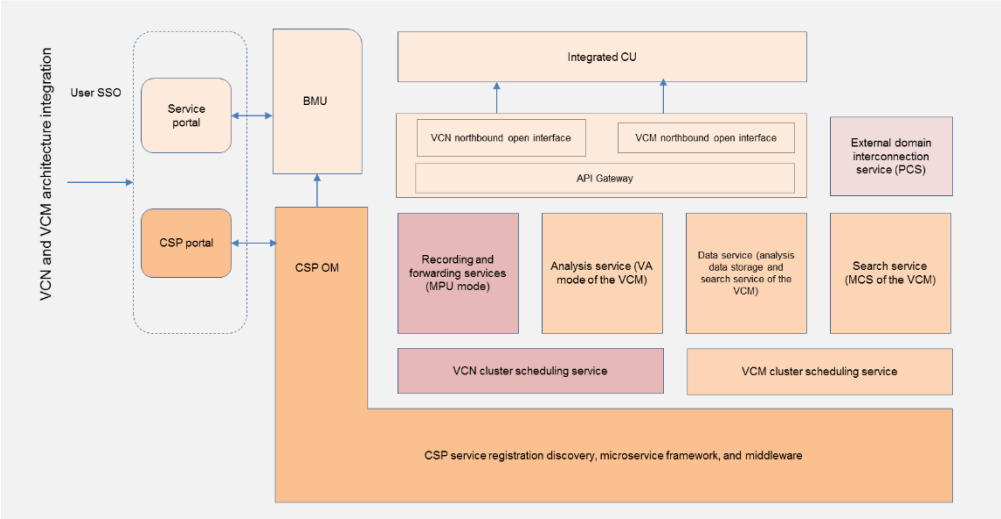
1.5 Integrating VCN and VCM Architectures in the CloudIVS 3000

In the CloudIVS 3000, the VCN and VCM are co-deployed on a CloudIVS 3000 physical node. Therefore, the boundary between the two products is blurred and their architectures are converged. The following describes the architecture integration:

- The VCN and VCM are deployed on the same CSP Edge platform, so they are displayed as only one application from the perspective of the platform.
- The VCN and VCM share the same service components such as GAUSSDB, ZooKeeper, and Cluster Management Unit (CMU).
- Two business management services (OMU and SEM) are combined into one Business Management Unit (BMU) to simultaneously manage the special management plane logic of VCM and VCN service components (general O&M functions are migrated to the CSP OM).
- Open RestFul interfaces are developed to create a unified CU for VCN and VCM services (CloudIVS V100R019C20).
- If customers require only VCM services, the corresponding service of VCN can be deployed to enable the entire system to connect to video of third-party video surveillance platforms for further analysis.
- The VCM uses the SafeVideo service component of the VCN to manage local SATA disk storage space.

Figure 2 shows the integration of the VCN and VCM service architectures.

Figure 2. VCN and VCM architecture integration

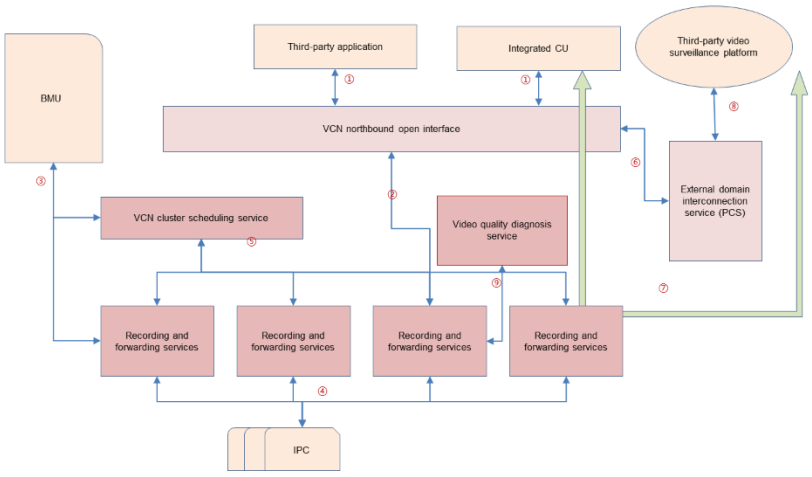


The integrated architecture has the following features:

- Unified entry of the management portal, unified login, unified UI style
- VCN/VCM client integration
- Sharing the same middleware and business services with the VCN and VCM
- Hybrid deployment of services on physical nodes as needed

Figure 3 shows the VCN service process.

Figure 3. VCN service process



① Open northbound service access interfaces

② Service access

③ Multi-level and multi-domain networking, cluster setup, and network management

④ IPC access and registration

⑤ Service cluster management and scheduling

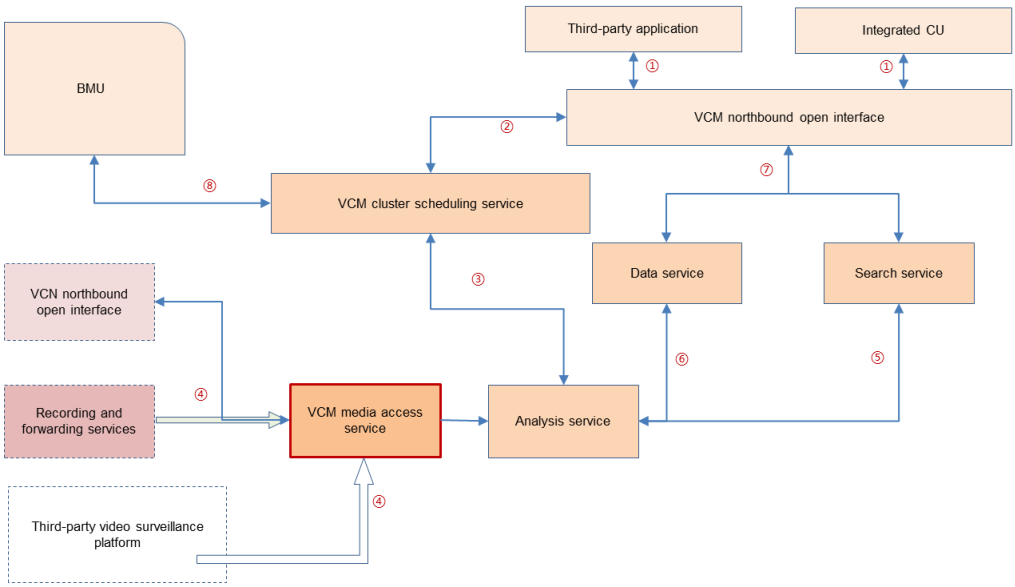
⑥ External domain service access

⑦ Media stream forwarding

⑧ GB/T 28181 protocol interface

⑨ Obtain video streams for video quality diagnosis

Figure 4. VCM service process



⑩ Open northbound service access interfaces

⑪ Deliver analysis tasks

⑫ Schedule analysis tasks

⑬ Add the media access service to obtain video streams from the VCN or a third-party platform

⑭ Send feature data in analysis results to the search service

⑮ Send structured data and images in analysis results to the data service

⑯ Search for analysis results at the service layer

⑰ Perform system deployment, upgrade, and O&M, and service component cluster deployment

1.6 CloudIVS 3000 Product Models

The CloudIVS 3000 (V100R019C10) is divided into six product models based on the function type.

No.	Product Model	Function
1	CloudIVS 3000S	Storage only, 4U
2	CloudIVS 3000SC	Storage and computing, 4U
3	CloudIVS 3000SCR	Storage, computing, and search, 4U
4	CloudIVS 3000C	Computing only (CPU) , 2U
5	CloudIVS 3000R	Search only (without FPGA) , 2U
6	CloudIVS 3000CR	Computing and search, 2U

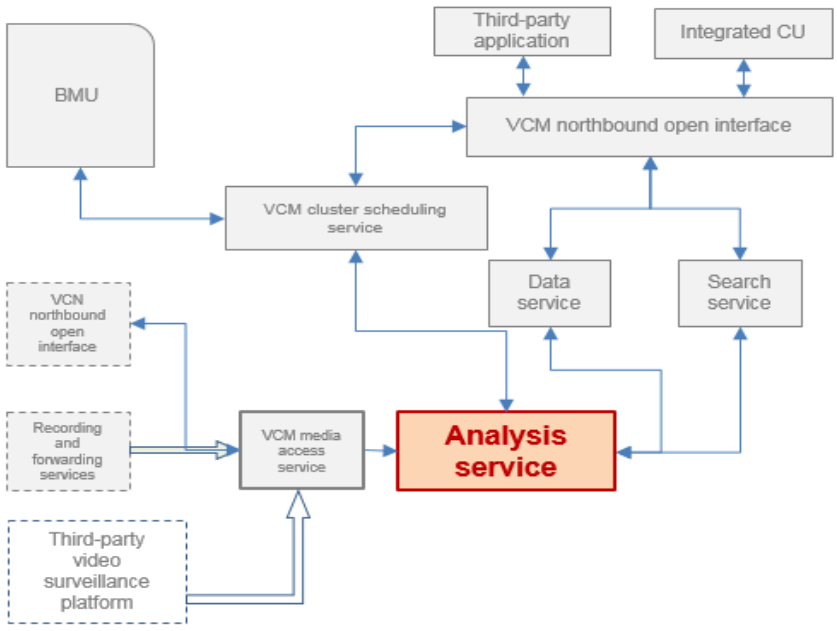
1.7 Critical Business Services

Key business services have direct and significant impact on business functions and performance counters of the system. Key business services include the analysis service (GPU and CPU analysis), recording and forwarding services, analysis data processing and search service, and business support middleware service.

1.7.1 Analysis Service

Figure 5 shows the position of the analysis service in the entire system service process.

Figure 5. Position of the analysis service in the entire system service process

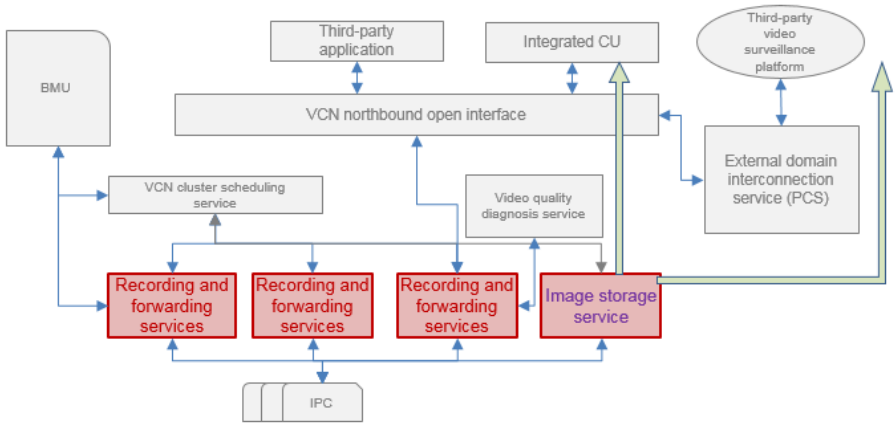


Service	Function Description
C_P4_VA	Analysis service of the GPU (P4) card type, which is used to extract features of faces, people, and in-depth features of vehicles for video- or image-based analysis.
C_P4_VA_S	Analysis service of the GPU (P4) card type with slightly lower specifications. This service is deployed on physical nodes with many management businesses. Additionally, the analysis service of the C_P4_VA_S type and the analysis service of the C_P4_VA type can be deployed in the same scheduling cluster at the service layer.
C_CPU_VA	Analysis service of the CPU type, which is used for outside-China license plate recognition (Q-Free), behavior analysis, video synopsis, video search, track search and other video analysis services.

1.7.2 Recording and Forwarding Services

The recording service (C_MPU_R) and forwarding service (C_MPU_T) are major business services of the VCN. They provide a variety of functions such as IPC access management, video and image storage, video forwarding, and recording search and download. The following figure shows the position of the recording and forwarding services in the entire system service process.

Figure 6. Position of the recording and forwarding services in the entire system service process



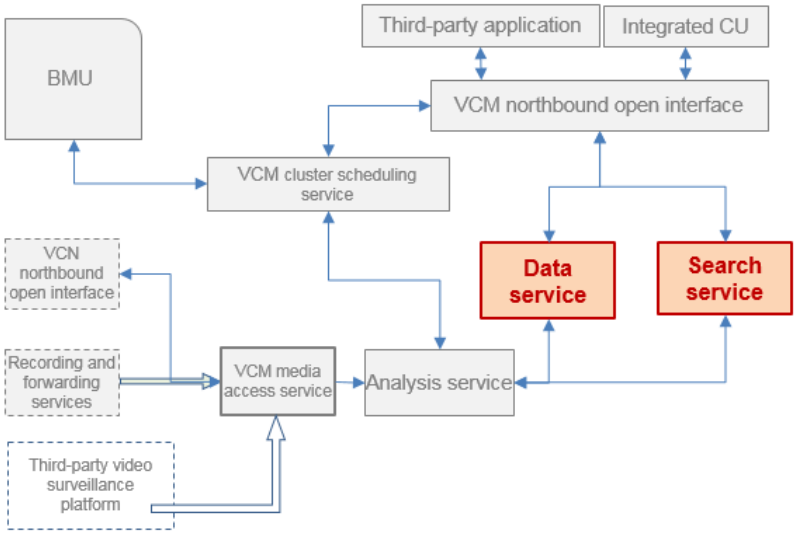
Service	Function Description
C_MPU_R	VCN media service, which is responsible for IPC access, video storage, recording download and playback, media stream forwarding, and checkpoint image storage. It also supports IPC migration among cluster services.
C_MPU_T	VCN media service that supports pure forwarding of media streams.
C_DT_MP	Image storage service, which is used to store and search for images in

Service	Function Description
	analysis results.

1.7.3 Data Search Service

The data search service is a key service of the VCM. It determines the implementation of service functions such as reverse image search, facial recognition, personal feature recognition, and vehicle recognition. The following figure shows the position of the data search service in the entire system service process.

Figure 7. Position of the data search service in the entire system service process



Service	Function Description
C_DT_MCS	Feature data search service that directly connects to NVMe disks. It is used to search for facial feature, personal feature, and other feature data. The data can be applied in service applications such as reverse image search, 1:N face match, N:N face match, and personal information archiving.
C_DT_MCS_HD	Feature data search service of the hard disk type (without NVMe disks). Compared with C_DT_MCS, C_DT_MCS_HD has lower search service specifications and can function as a search node of the RH5288 type.
C_DT_KAFKA	Message middleware service that decouples the analysis service from the search service. The analysis result is sent to the Kafka service, and the search service obtains analysis result data from the Kafka service.
C_DT_DPC	Service that obtains structured data in the analysis result from the Kafka service and sends the obtained data to the MongoDB or

	Solr service for storage.
C_DT_MONGO	MongoDB service, which is used to store and search for structured data in the analysis result.
C_DT_SOLR	Solr service, which is used to search for structured data in the analysis result in fuzzy mode.

1.7.4 Middleware

Middleware includes MongoDB, Solr, and Kafka.

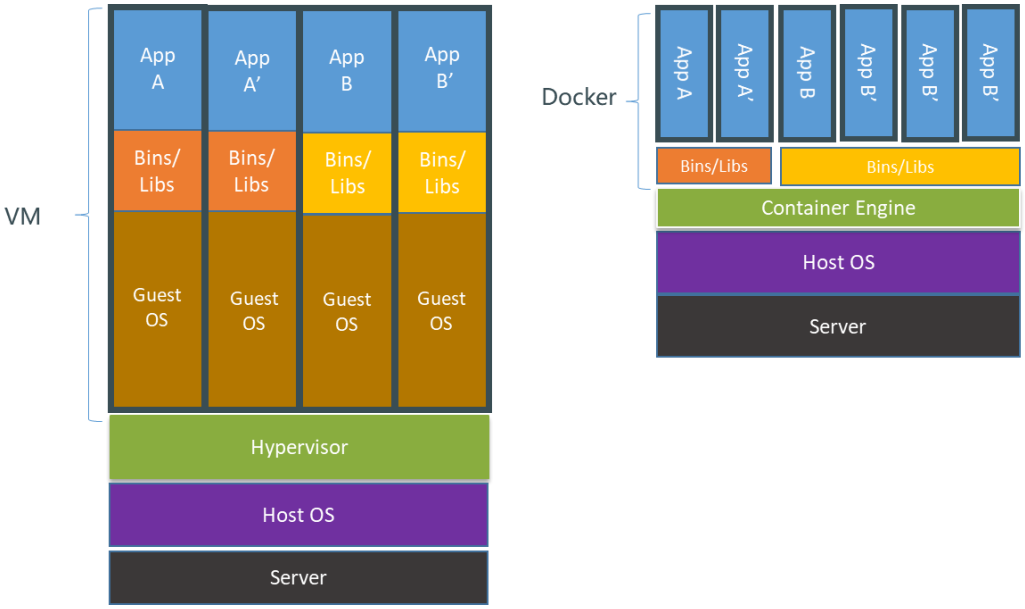
Kafka: message bus, which is responsible for subscribing to and distributing feature data and structured data obtained through video analysis as well as signaling messages of some tasks

MongoDB: NoSQL database that stores structured data of people, vehicles, cases, video synopsis, and behavior analysis as well as the raw data

Solr: search engine that creates inverted indexes for unique IDs and key fields in MongoDB records to provide search and fuzzy search functions

2 Key Technologies

2.1 Differences and Similarities Between VMs and Docker Containers



The VM uses the hardware-level virtualization technology to provide multiple independent virtual hardware running environments, ensuring high isolation (including security and reliability). The VM has the following features:

Similarities between VMs and containers	They both use the virtualization technology to virtualize a resource object into multiple resource objects. The virtualized resource objects are isolated from each other.
Differences between VMs and containers	Different virtualization layers The VM provides the virtual hardware running environment at the hardware layer. The container provides the virtual operating system running environment at the operating system layer. Different isolation capabilities

	Multiple VMs are isolated in terms of hardware. Multiple containers are isolated in terms of operating system software. System performance and costs VM: large hardware overhead, high memory usage, and slow system boot Container: no hardware overhead, low memory usage, and fast system boot

- Multiple VMs are isolated in terms of hardware.
- Provides independent virtual hardware running environments and interfaces.

The container uses the operating system virtualization technology to provide multiple independent virtual operating system running environments. Containers are isolated from each other but share the same operating system and system-level binary files and libraries. The container has the following features:

- Multiple containers are isolated in terms of operating system software.
- Provides independent virtual operating system running environments and interfaces.

2.2 Comparison Between VMs and Docker Containers

VM	Container
High isolation and independent guest OS	× Shared kernel and OS; weaker isolation compared with VMs
Virtualization performance loss (5 – 15%)	✓ No computing/storage loss; no memory consumption (about 200 MB) by guest OS
Large VM image size (several GB to dozens of GB); sharing unavailable during instantiation	✓ Small Docker container image size (200 – 300 MB); sharing available during instantiation of public basic images
Lack of unified standards for VM images	✓ Docker provides container application image standards, which are further standardized by Open Container Initiative (OCI).
Slow VM creation (> 2 minutes)	✓ Fast container creation (< 10s)
Slow VM startup (> 30s)	✓ Fast container startup (< 1s, excluding application startup)
Low resource virtualization granularity: 10 – 100 VMs for a physical machine	✓ More than 1000 containers for a physical machine

Summary: The advantages of the container technology are lightweight, flexible, and high utilization. The disadvantage of the container technology is that its security isolation is inferior to that of the VM.

2.3 HASEN and Docker Containers

The single-server operating system manages hardware resources of a physical machine, while the Data Center Operating System (DCOS) helps enterprises manage cluster resources of the entire data center. HASEN is a DCOS developed by Central Software Institute.

HASEN abstracts cluster resources into a unified resource pool, implements cluster resource sharing for different applications (including application frameworks), and provides capabilities such as cluster application deployment and resource scheduling.

For the CloudIVS 3000, HASEN has a built-in container engine and is a container management platform. It is responsible for container template orchestration, container scheduling, resource management, and container network deployment.

2.4 CSP Edge

The CSP Edge is responsible for service installation and deployment, upgrade and capacity expansion, and O&M capabilities. The CSP Edge integrates HASEN to implement edge container resource management and application deployment.

2.5 UVP

UVP is called Unified Virtualization Platform, which means unified virtualization platform. CloudIVS 3000 V100R019C10 integrates the UVP to create and manage VMs.

The UVP is a key technical platform for data center solutions based on cloud computing. It virtualizes physical resources, such as CPU, memory, and I/O, into a group of logical resources. The logical resources can be centrally managed, flexibly scheduled, and dynamically allocated, and they create an environment on a single physical server for multiple isolated VMs to run simultaneously.

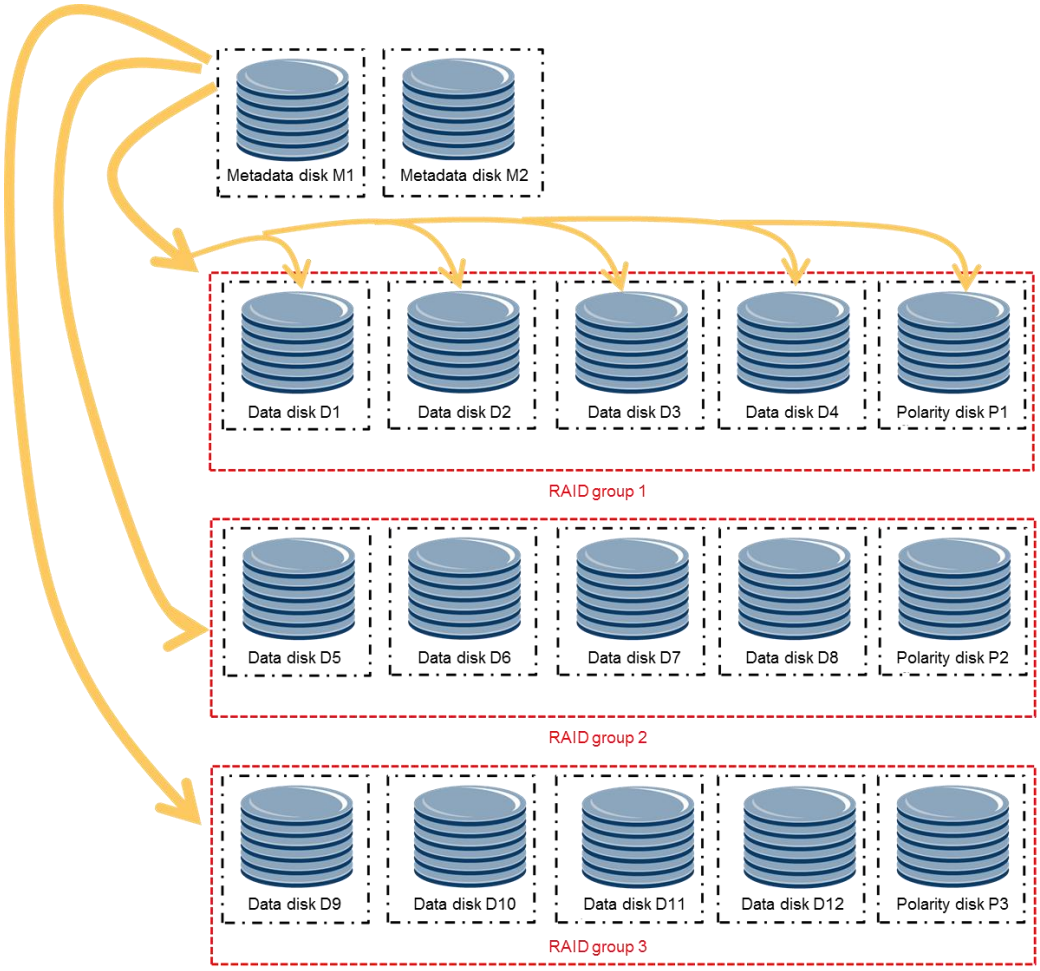
The UVP provides the following functions:

- VM lifecycle management, including creating, starting, shutting down, deleting, and restarting VMs
- VM information query, including utilization query of vCPU, memory, disk (only support self-developed VM, third-party VM does not support. If it needs to support third-party VM, third-party VM should integrate UVP VMTOOLS)

3 CloudIVS 3000 Key Features

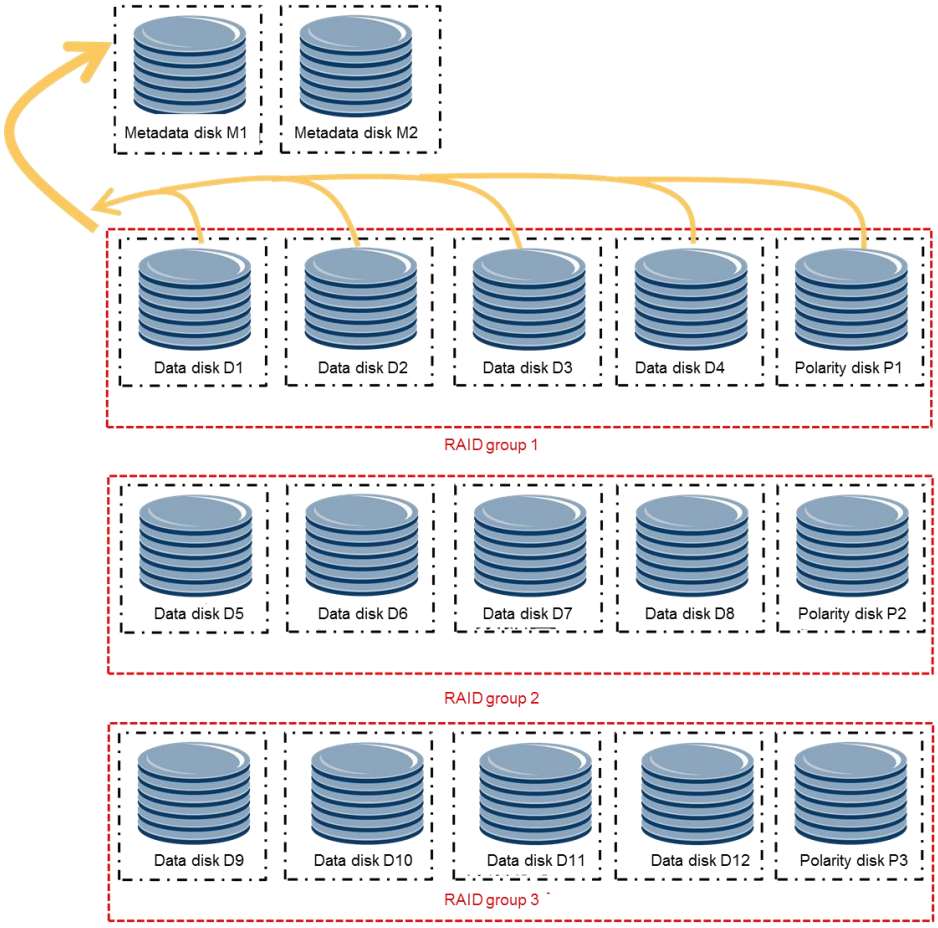
3.1 Data Safe Technology

When a high-speed SAS disk is damaged, metadata such as the recording indexes stored in the SAS disk is also lost. The Data Safe technology is enabled by default to automatically save metadata such as indexes to the recording data storage area without manual intervention, as shown in the following figure. Generally, each RAID group backs up data, but the backup content is distributed to each data disk.



When the old SAS disk is faulty, a new SAS hard disk (built-in new software obtained from Huawei standard warranty services) is installed in the slot after removing the old SAS disk. The system automatically restores the metadata in the recording data storage area. In this way, all recording data is available. As long as one RAID group is intact, metadata such as indexes can be restored. As shown in the following figure, the most complete

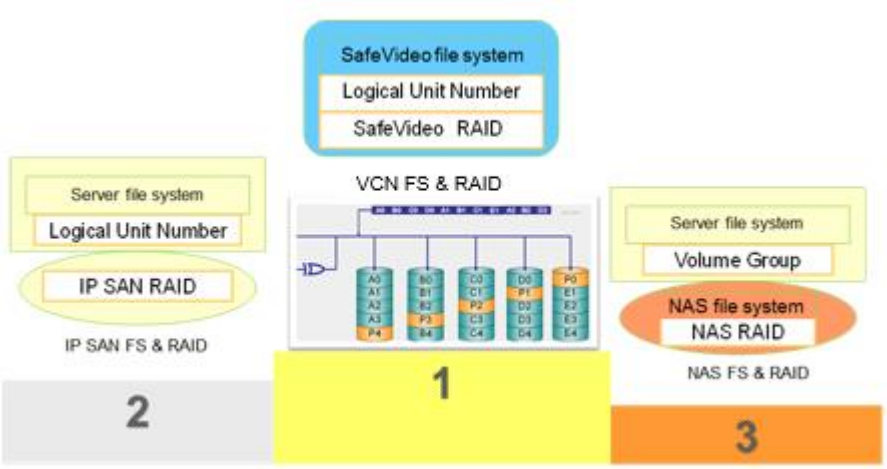
index metadata is selected for restoration.



3.2 Safevideo: Fast RAID Initialization

Widely-used HD cameras require a high-performance video storage system to collect, store, and use mass video data. In addition, disk technology evolution brings disks with larger capacity and lower costs. Traditional storage technologies face challenges in system efficiency and data stability of RAID groups that have large-capacity disks.

SafeVideo uses the innovative plug-and-play design to well resolve these two problems for RAID-based storage solutions that use large-capacity disks.



The preceding figure shows the ranking in terms of the RAID initialization duration. Each enclosure can be defined as a hierarchical step. In the three solutions, the VCN needs to perform four steps, the IP SAN needs to perform five steps, and the NAS needs to perform six steps. Therefore, the preceding figure can also be understood as the ranking in terms of the initialization speed.

SafeVideo has the following features:

- Web-based configuration: Based on traditional NVR security philosophies in the preceding chapter, SafeVideo allows a common user who has no solid technical knowledge to quickly create and delete RAID groups as well as complete system configuration.
- Optimized fast-initialization algorithm: When started and properly configured, a full-capacity 108-TB RAID group can complete initialization within 15 minutes. Compared with traditional RAID technologies, SafeVideo shortens the system deployment period by over 50 hours.
- Being mechanical parts, disks can go faulty after running for a certain period of time. When two or more disks in a traditional RAID group are faulty, all data is lost. To recover the service system, users need to perform professional configuration and time-consuming initialization. SafeVideo uses innovative technologies and services to switch the faulty RAID group to read state, allowing users to read data from normal disks. After faulty disks are detected and replaced, SafeVideo uses innovative algorithms to automatically reconstruct and quickly initialize the RAID group without compromising service data. The entire process can be completed within an hour, supporting plug-and-play.

  Why can we achieve the minimum duration in RAID initialization? The root cause of the fast initialization algorithm is the media file system and RAID layer convergence technology mentioned in the previous section. This convergence enables RAID 5 group initialization to build RAID 5 storage groups. SafeVideo's RAID 5 group is a virtual RAID layer based on the RAID rules, unlike the traditional IP SAN or NAS that configures the RAID group in the operating system and initializes the LUNs or VGs. The LUN is mounted to the server in an IP SAN environment in accordance with their respective features, and then the same file system is mounted to the server. The file system of its own is formatted in a NAS environment and shared through the NFS. Using SafeVideo, the RAID 5 group can be set up and the corresponding file system can be initialized in one step.

  With such initialization capabilities, Huawei VCN helps integrators achieve faster delivery in large-scale multi-site scenarios, for example, the Safe City, rail transportation, and financial outlets, further improving the customers' construction efficiency.

3.3 Safevideo: No Copyback of Hot Spare Disks in the RAID Group

In traditional storage devices, when a member disk of a RAID group is damaged, a global hot spare disk is added

to the RAID group for reconstruction. After the faulty member disk is replaced, data is copied back to the new member disk. After the data copyback is complete, the global hot spare disk restores its hot spare state.

This process usually takes several hours, bringing pressure to the storage system. Additionally, if another disk goes faulty during the data copyback, the entire RAID group fails. Device performance deteriorates during RAID group reconstruction and data copyback.

Figure 8. Hot spare disk replacement in the case of a fault

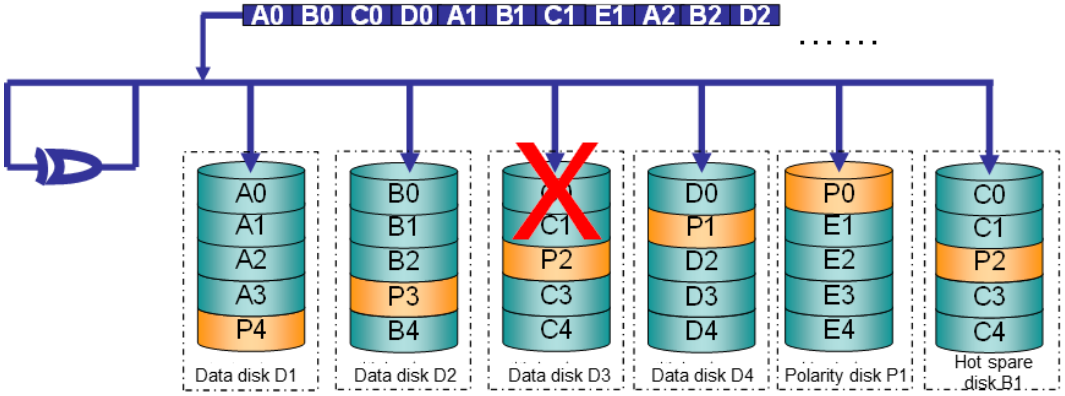
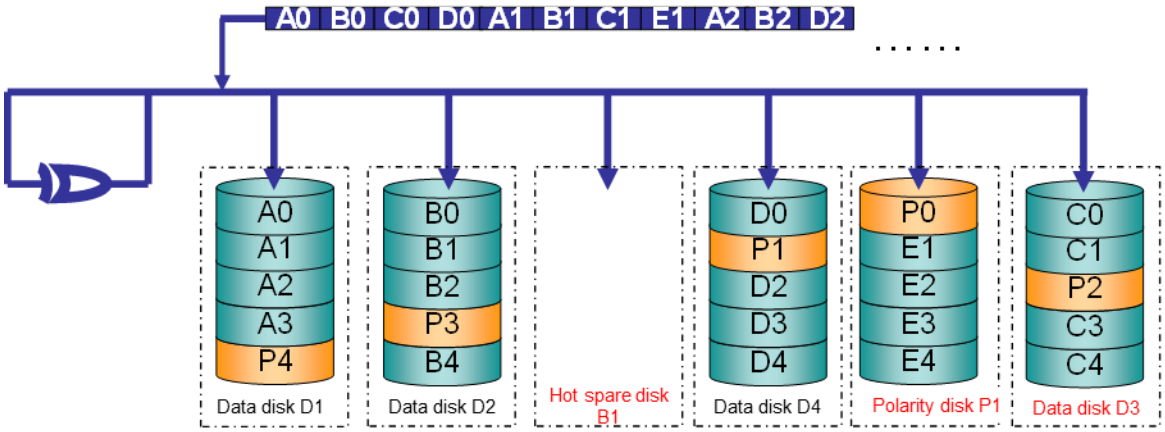


Figure 9. Adding a new disk after a fault occurs



SafeVideo uses the dynamic hot spare disk technology to automatically change a hot spare disk to a member disk in the RAID group. When a disk in the RAID group is faulty, the system uses the global spare disk for RAID group reconstruction. When a new disk is added to the RAID group, the system uses this new disk as the global hot spare disk, preventing stability risks and performance deterioration. No data copyback is required, improving the device work efficiency.

When hot spare disks replace faulty disks, the VCN would generate an alarm. Different from traditional solutions that need to wait for the copyback and reconstruction to complete, the operation and maintenance is semi-automatic only if integrators or maintenance vendors add new hard disks onsite in a timely manner. This extends devices' useful lifespan, avoids wasting maintenance manpower, and ensures smooth execution of operation and maintenance in the back-end system. This solution is suitable for Safe Cities, rail transportation, and financial outlets.

3.4 Safevideo: Continuous Readability in the RAID Group

In traditional RAID applications, RAID 5 data and parity check are evenly distributed on all disks. Therefore, when two or more disks (in a RAID 5 group) are faulty, all data in the RAID group is lost and cannot be restored, causing serious consequences.

Figure 10. Free hot spare disks replace faulty disks in a RAID group

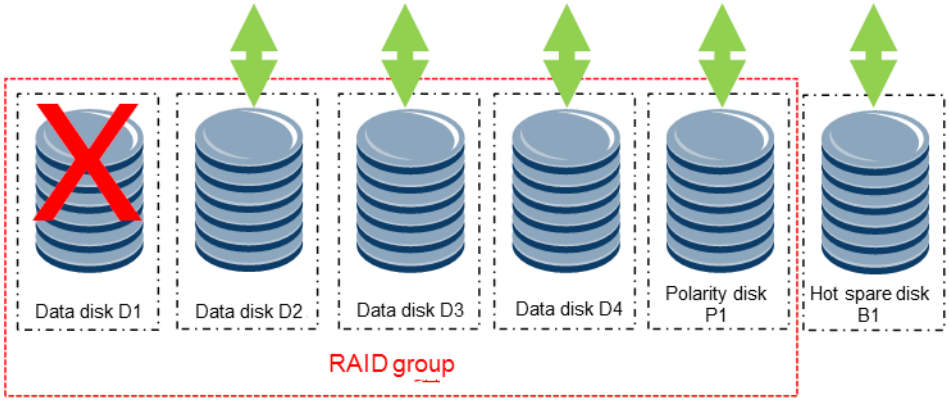


Figure 11. Data is readable and writable in a RAID group without hot spare disks

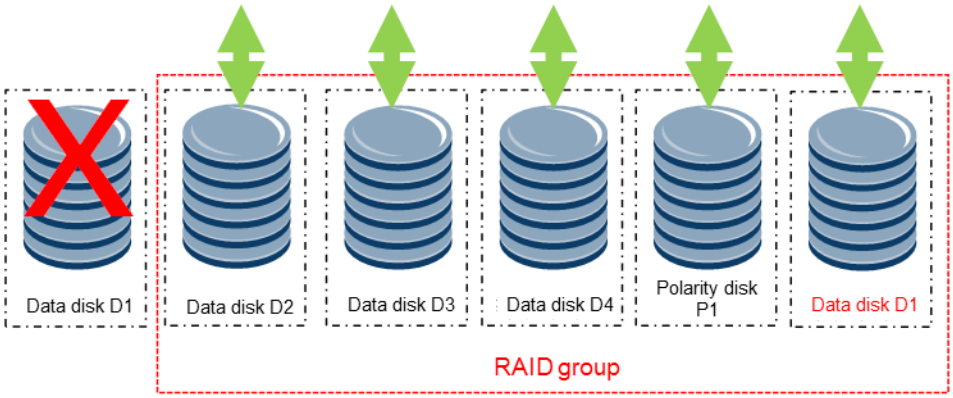
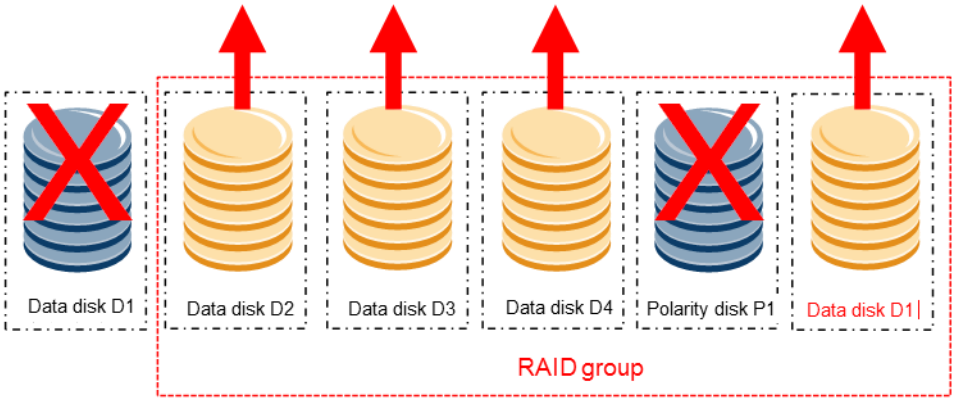


Figure 12. Data is read-only in a RAID group without parity disks



SafeVideo storage technology consecutively writes large video data blocks into disk. In addition to automatic system recovery upon single-disk failure (similar to RAID 5), this technology allows the system to protect data in normal disks when two or more hard disks are faulty simultaneously. Though data in faulty disks will be lost (no available technology can protect data in these disks), SafeVideo can minimize data loss. In typical 11-disk RAID groups, when two or more disks are faulty simultaneously, SafeVideo loses 10% video data while traditional RAID 5 loses all.

Thanks to the block storage technology for the media file system, when multiple disks in a RAID group are faulty, users can still read video data stored in these disks. Degraded reading in a RAID group is suitable for scenarios that have emergency or event assurance requirements, for example, the Safe City, rail transportation, and financial outlets. This ensures important recording playback when the recording fails to be written.

3.5 Safevideo: Load Balancing Among RAID Groups

To ensure that RAID groups synchronously write data, Huawei SafeVideo develops the intelligent load-balancing algorithm by considering factors such as the RAID group capacity and media traffic to enable automatic load balancing among RAID groups. When a RAID group is faulty, the system automatically switches live streaming media data to another RAID group for storage.

Figure 13. Intelligent load balancing among three RAID groups when hot spare disks have not replaced all faulty disks

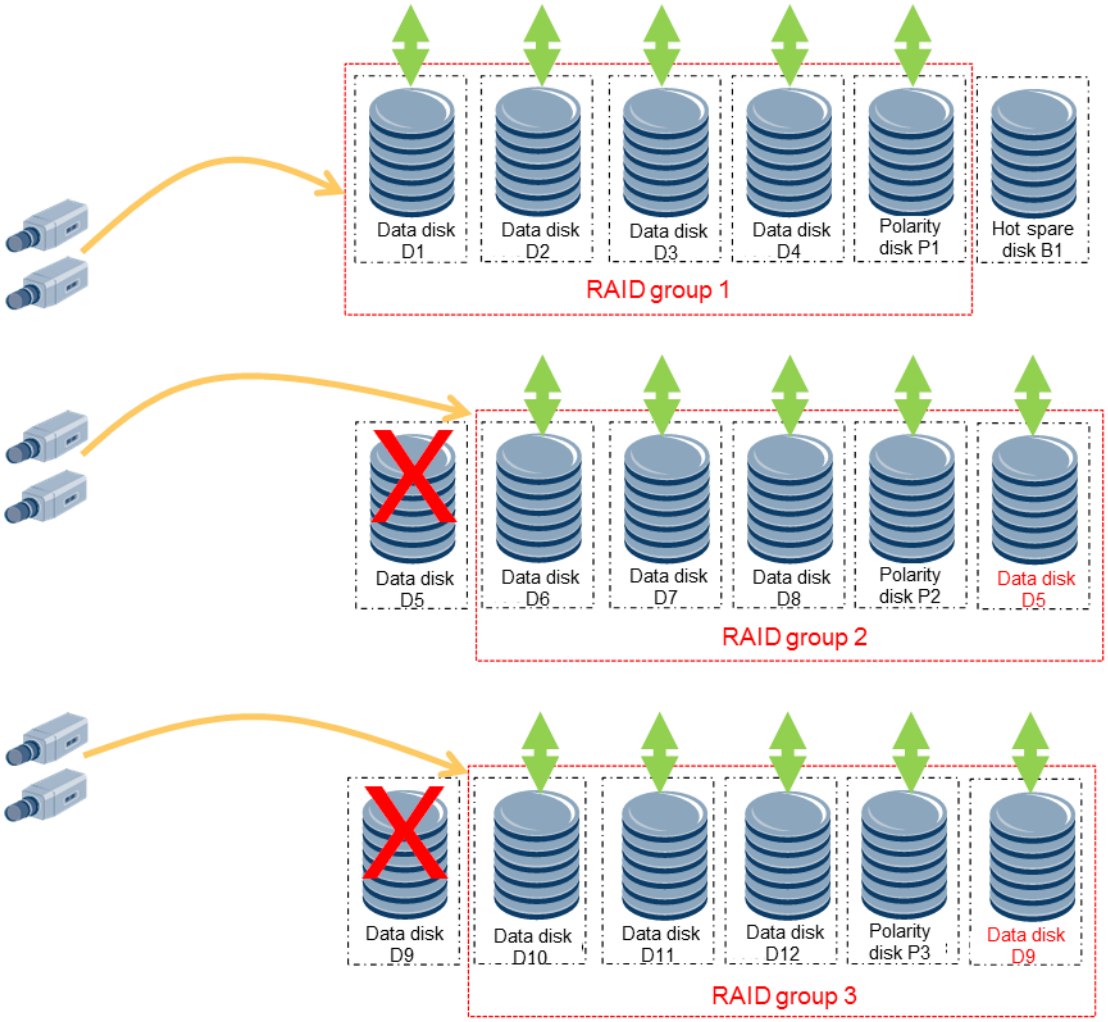
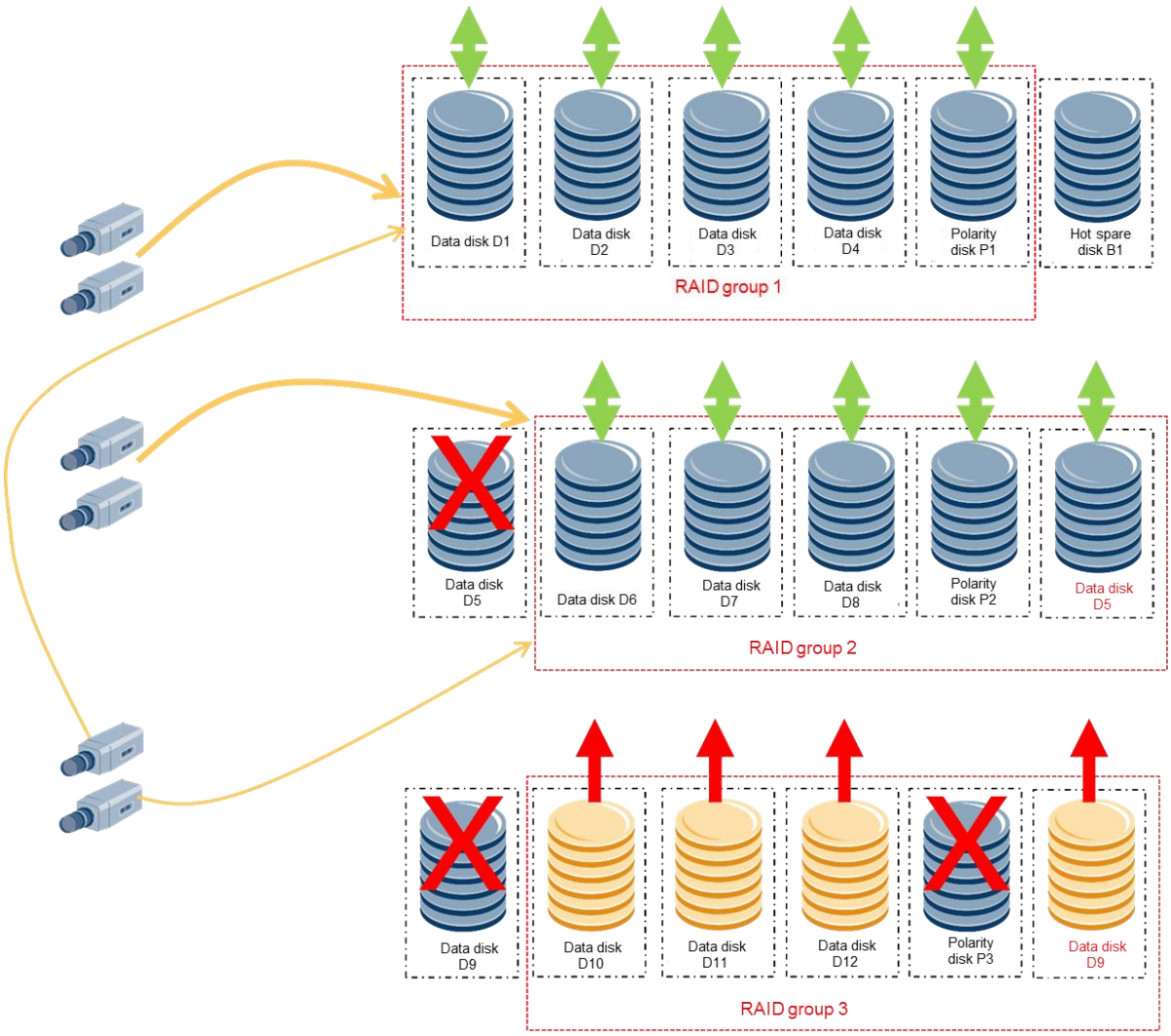


Figure 14. A RAID group is faulty when hot spare disks have replaced all faulty disks

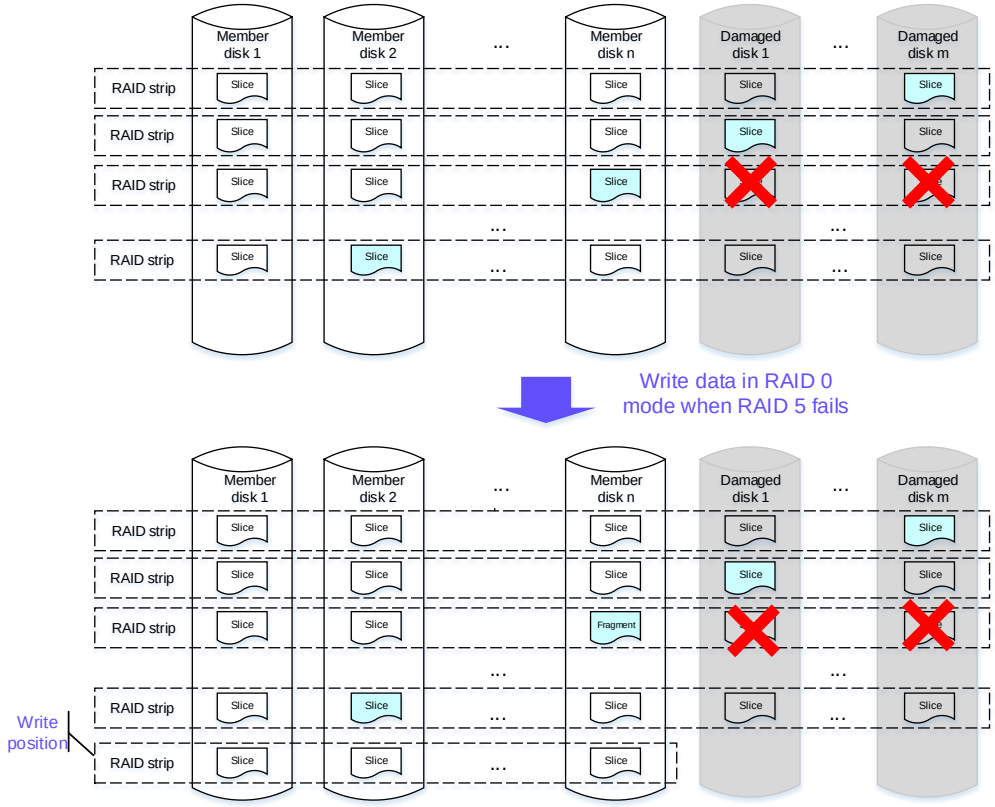


The intelligent load balancing design of RAID groups further improves the data reliability of a single network video storage cloud node. One cloud node is located on a single site in networking scenarios such as rail transportation and financial outlets. The compact single device can run reliably in the event of network disconnection among multiple sites.

3.6 SafeVideo+: Writability Upon Failure

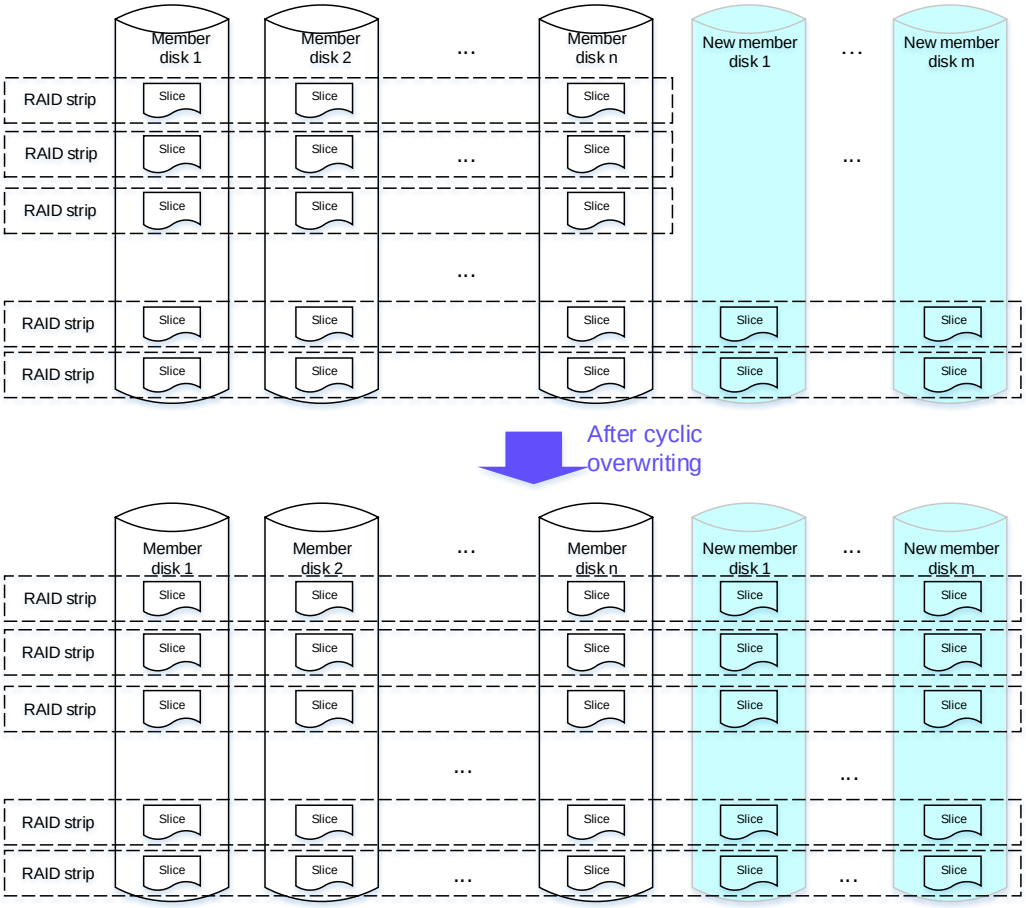
Writability upon failure is a technology that enables new data to be written to the undamaged disks in a RAID group that fails (two or more disks are damaged in RAID 5). After some faulty disks are replaced, the RAID group is still faulty, but data will be written to the new disks in RAID 0 mode. After all faulty disks are replaced, the RAID group automatically restores to the read/write status before the failure.

This technology, leading in the security industry, ensures the reliability of the storage system and greatly reduces the service interruption caused by storage faults.



3.7 SafeVideo+: Online Capacity Expansion

Online capacity expansion allows newly added disks to be directly added to a RAID group. When a new disk is added to a RAID group, some slices on the new disk form a new stripe with the old disks' slices whose retention period expires to store data. Within the entire retention period, this operation continues. In this way, during the period from the time when a new disk is added to the RAID group to the time when the entire retention period expires, the storage space of the new disk can be all used, truly achieving capacity expansion. During the capacity expansion, the original recording is not affected and services are not interrupted. In the traditional solution, all data in the original RAID group must be read to the memory and then written to the new RAID group. The entire process takes more than 10 hours.



3.8 Cloud-based Cluster Management Technology

Cloud-based Cluster Overview

Multiple MPU containers in a domain can be created as a cluster and operate in cluster mode. No planning is required before you add IPCs. The CMU can add an IPC to a proper MPU according to the load of each cluster member. Cluster members can be added and deleted. When a MPU is overloaded, some services on the overloaded MPU can be switched to other MPU. When a MPU is faulty, services on the faulty MPU can be switched to other normal MPU. When the faulty MPU is recovered, some services on other MPUs can be switched to the recovered MPU.

Cloud-based Cluster Management

To facilitate cluster management, the cloud-based cluster allows users to:

- View cluster storage space
- View the status of cluster RAID groups and export information about faulty RAID groups in an Excel file.
- View the status of cluster disks and export information about faulty disks in an Excel file.
- View the status of cluster members and export information about faulty ones in an Excel file.
- View the status of cluster cameras and export information about offline cameras in an Excel file.

- View the status of cluster platform recording plans and export information about cameras that fail to execute the recording plan correctly in an Excel file.

Adding IPCs

The ever-increasing video surveillance system scale and IPC quantity are facing demands of mass data storage. During the initial system construction period, users need to plan the exact recording device to which each IPC is to connect, which involves huge workload. No manual planning is required when users add IPCs to the cluster.

Adding and Deleting Cluster Members

In a traditional video surveillance system, recordings are stored in fixed storage devices. The recording storage duration determines the storage capacity. If the number of storage devices is changed, users need to re-plan IPC storage in the entire system and manually specify the storage device into which recordings of each IPC are stored. The cloud-based cluster allows users to add or delete cluster members . The system dynamically allocates IPCs to proper MPU without manual intervention.

Load Balancing

Traditional industrial N+1 clusters support only the backup function. An IPC is added to a fixed cluster member. However, the cloud-based cluster can dynamically allocate an IPC to a proper cluster member according to the load of each cluster member.

Fault Migration

Traditional industrial N+1 clusters can switch services on only one faulty device to the backup device. However, the cloud-based cluster can balance IPC loads on multiple faulty MPU to other MPUs.

3.9 Media Format Processing

Application Scenario

As the Safe City system scale gradually expands, video feeds of different formats or standards are generated due to a variety of reasons, for example, uneven economic and social development, differentiated vendor capabilities, and unimplemented public safety specifications.

In addition, in the public safety field, the video surveillance system has become a key element for maintaining social order and strengthening social management. Association analysis between mass public security surveillance video resources (including standard video shot by DVs or mobile phones) and cases also has become a powerful means for police officers to find evidence and crack cases.

Video resources are first-hand materials for obtaining the most powerful evidence. However, various video resources result in the following problems:

- Non-uniform video format
- Low storage reliability and easy-to-damage recordings, leading to poor video integrity and low access efficiency
- Huge labor and material costs and low work efficiency for playing a large number video files using different players by trial and error to find evidence

The CloudIVS3000 uses Huawei's proprietary patented media format processing technology to help enhance case solving efficiency.

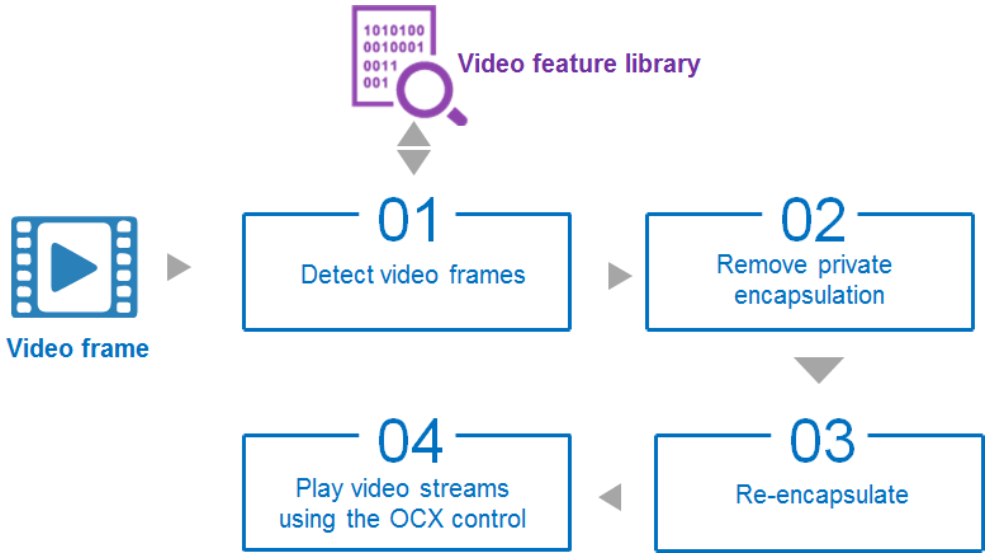
Technical Principle

With Huawei's proprietary media format processing technology, the CloudIVS 3000 allows users to directly upload video without recording models of surveillance devices manufactured by different vendors. The CloudIVS 3000 can automatically identify the video format encapsulation and preprocess video streams. The CloudIVS 3000 supports video provided by mainstream DVRs and NVRs and video shot by mainstream DVs and mobile phones.

The video formats compatible with the system are as follows:

- Video container format: 3GP, FLV, AVI, WMV, MP4, MPEG, MOV, NVS, DAV, MKV, and GE5
- Video encoding formats: H.264, H.265, MPEG4, MJPEG1, MPEG2, MJPEG, WMV1/2/3, H.263, VP6, and VP8

Figure 15. Media format processing



- Video transcoding

  Convert private video formats provided by different vendors to a uniform video format and allow users to use a standard video player to play video of the uniform video format. This provides basic data for video viewing, analysis and search, and case management.

- Corrupted video repair

  Use Huawei's proprietary video repair technology to repair corrupted video (for example, file index loss, file header damage, and video content loss) uploaded to the system.

3.10 Search Acceleration

Application Scenario

With continuous expansion of the system volume and increasing duration required by all industries to keep surveillance data, the data volume of the surveillance system shows an explosive growth, and the basic data volume increases. In the public safety industry, when a case occurs, if a witness only vaguely remembers the license plate number of the suspicious vehicle, the police needs to enter the license plate number in the CloudIVS 3000 to search for the suspicious vehicle. Without search acceleration, it costs at least 30s on the premise of 5 billion basic data records, seriously affecting user experience. After search acceleration, the CloudIVS 3000 returns search results within 3s.

Technical Principle

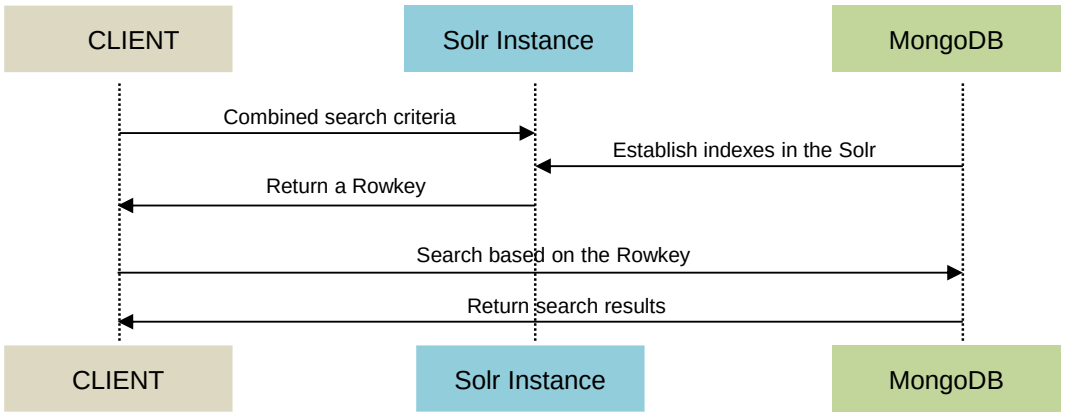
To ensure that the search results are returned within 3s, the CloudIVS 3000 stores data by day or uses the Solr+Mongo search mechanism.

Through storage by day, users can enter the date as search criteria to quickly find the file where data is stored. Besides, although the total data volume remains unchanged, the data volume stored by day is small, shortening the time for returning search results.

The Solr+Mongo search mechanism is used as the key technology. The MongoDB supports only millisecond-level search for Rowkeys, but does not support multi-field combinational search.

In actual applications, data is searched based on a combination of multiple criteria. Taking the advantage of multi-criteria combinational search provided by the Solr, the system first searches data in the Solr for a Rowkey, and then searches data in the MongoDB based on the obtained Rowkey. In this case, the search speed is greatly improved.

Figure 16. Two-level search mechanism



NOTE

1. The data fields in the MongoDB have been indexed in the Solr.
2. A client obtains a Rowkey in the Solr through combined search criteria.
3. The Rowkey is used to search for data in the Mongo. (The Mongo supports millisecond-level quick search using the Rowkey.)

Distributed Search Technology

- Supports load balancing in SHARD mode. Different search servers are responsible for data from different cameras.
- Supports Replicaset. Each SHARD supports multiple copies. There are one master and multiple slave copies. The master and slave copies can participate in the search at the same time to improve the QPS.
- Supports fault rectification. When the master copy is faulty, a slave copy can automatically take over the services of the master copy.

3.11 Distributed Computing

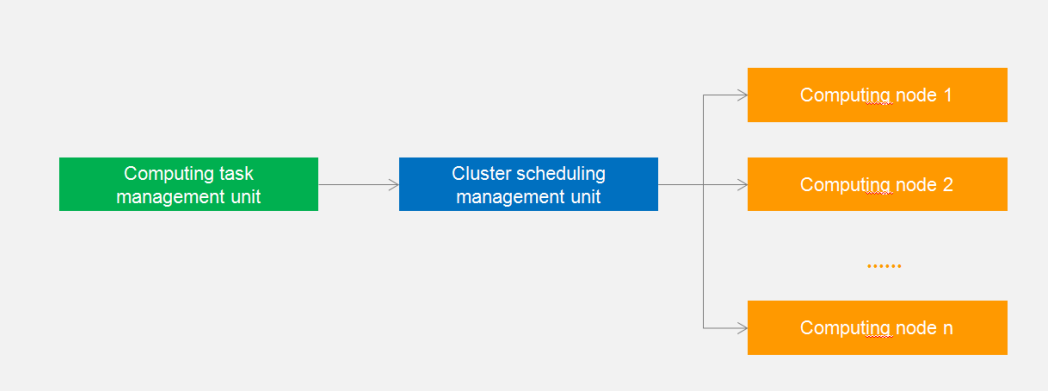
Application Scenario

Increasing growth of data in the surveillance system and the diversity and multi-geographic deployment of data sources pose great demands on the system's computing capacity. In this case, based on the system network, it is necessary to increase computing nodes, support distributed deployment of the computing nodes, and provide an intelligent scheduling module so that the computing tasks can be evenly scheduled in the system, maximizing the

hardware and software resource usage and improving system reliability and performance.

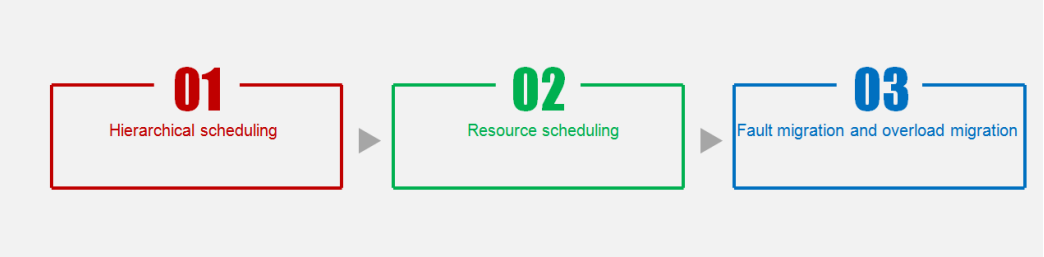
Technical Principle

Figure 17. Distributed intelligent scheduling



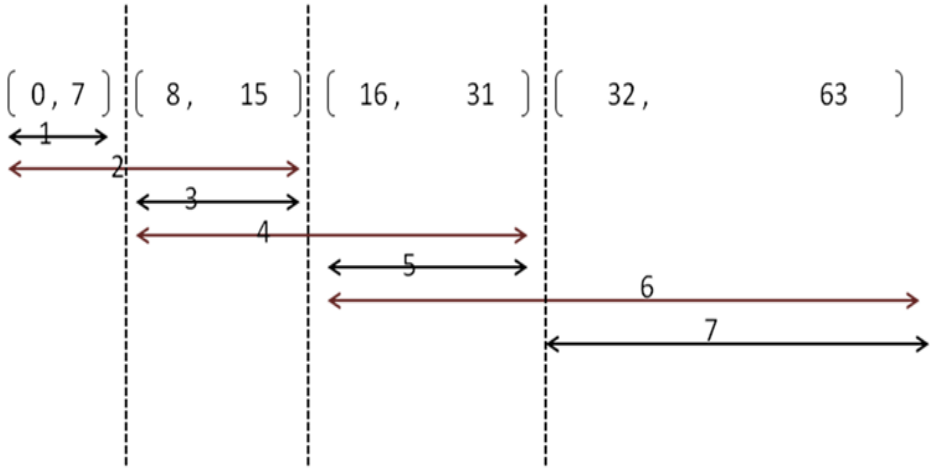
In order to enhance the reliability of the system and make full use of nearby scheduling, the system's computing resources and storage resources are deployed in distributed manner on the upper-layer node and sub-nodes, and are interconnected through a backbone network. Each distributed computing node reports information such as the CPU, memory, storage space, and number of concurrent tasks of the local system to the cluster scheduling management unit. The computing task management unit delivers the intelligent analysis and calculation tasks to computing nodes based on the computing resources reported by each node.

Figure 18. Intelligent scheduling process



- Hierarchical scheduling refers to evenly delivering computing tasks to each computing node based on the hierarchical task thresholds.

Figure 19. Hierarchical scheduling



For example, if the threshold of the first layer is 7, computing tasks are allocated to all computing nodes at the first layer until the number of allocated tasks on each computing node reaches the threshold, which is 7.

When the task quantity of all computing nodes reaches the threshold of layer 1, tasks are allocated to computing nodes at layer 2 ([8,15]) until the task quantity of all computing nodes reaches the threshold of layer 2, which is 15. This rule applies to the hierarchical scheduling for the subsequent layers.

- In resource scheduling, tasks are allocated to computing nodes filtered in hierarchical scheduling and that have the lowest resource consumption based on the reported computing resources such as the CPU, memory, and storage space.
- Fault migration is to record faulty nodes to the blacklist during computing analysis so that the system will not allocate intelligent analysis tasks to the nodes. In overload migration, if the CPU usage of the computing node with the highest CPU usage is higher than that of the computing node with the lowest CPU usage for more than the threshold (for example, 50%) in a window period (for example, 20 heartbeat intervals), the system transfers one task from the computing node with the highest CPU usage to the computing node with the lowest CPU usage.

3.12 Multi-Algorithm Warehouse

Algorithm Plug-in Management

Users can log in to the CSP portal to manage algorithm plug-ins, including uploading, saving, installing, upgrading, uninstalling, querying, and deleting algorithm plug-ins, and managing their validity periods. Users can also enable or disable algorithm plug-ins.

Currently, the following default plug-in types are supported: license plate recognition, non-Chinese license plate recognition (Q-Free), video search, video synopsis, behavior analysis, facial recognition, person search by image, and person and vehicle data structuring.

Management of Multiple Vehicle Recognition Algorithms

The system supports integration of multiple vehicle recognition algorithms, including Huawei's vehicle recognition (license plate recognition + vehicle feature recognition) algorithms and Q-Free's license plate recognition algorithms.

Management of Multiple Facial Recognition Algorithms

The system supports integration of multiple facial recognition algorithms. Before using the facial recognition functions, users need to install the VA algorithms and MCS algorithms for facial recognition, and configure the MCS algorithms. Video Quality Diagnosis

The rapid video surveillance deployment in recent years has seen a growing number of surveillance sites. A large video surveillance system usually connects to hundreds of cameras, even tens of thousands. It is a huge challenge to efficiently manage these cameras to improve security protection efficiency and enhance camera maintenance capabilities.

The industrial video quality diagnosis function is implemented through an independent server, while this function is integrated in the CloudIVS 3000. This saves equipment room footprint, reduces failure points, and decreases total cost of ownership (TCO) for customers.

With the video quality diagnosis function, the CloudIVS 3000 can effectively detect a variety of image exceptions caused by various reasons such as lens blocking and man-made reasons. After detecting an image exception, the CloudIVS 3000 can generate an alarm. This helps maintenance personnel to quickly locate faults and reduce losses caused by image exceptions.

The video quality diagnosis system is an intelligent video fault analysis and warning system that integrates multiple technologies such as image processing, computer vision, computer graphics, and image analysis technologies. The system can analyze collected images and extract valuable object features from the images. Through predefined video quality diagnosis conditions and rules, the system can automatically generate alarms upon detecting image exceptions, such as image noise, stripe interference, image blur, color cast, frame freezing, gain imbalance, and video signal loss.

The CloudIVS 3000 can inspect video quality of cameras across the network and generate alarms when detecting one of the following image exceptions:

- Image brightness abnormality
- Noise interference
- Color cast
- Stripe interference
- Video signal loss
- Frame freezing
- Image shaking
- Image definition abnormality
- Lens blocking

Video quality diagnosis

3.13 Video Surveillance O&M Tool

Users can view and export a variety of statistical reports such as device online rate, device offline rate, SD card fault, disk fault, recording plan execution, recording integrity, packet loss rate, and real-time media information statistical reports.

Users can view various alarms such as SD card fault, camera offline, high camera memory usage, high camera CPU usage, camera temperature, disk fault, system disk RAID degradation, system disk removal, data disk RAID degradation, data disk removal, node CPU overload, node memory overload, and node too-high-temperature, power fault, and fan fault alarms.

Users can also view the CPU, memory, and process counters of physical nodes as well as the CPU and memory counters of containers.

3.14 Cloud-Edge Synergy

Data collaboration

Video viewing: Users in the upper-level domain can use the analysis platform WebUI to view video in lower-level domains level by level.

Alarm and structured data subscription: Users in the upper-level domain can subscribe to face, person, and passing vehicle data as well as face and vehicle alarms from lower-level domains.

Task Collaboration

Alert task: Users in the upper-level domain can create an alert task and deliver the blacklisted person or vehicle image to a lower-level domain. Then the lower-level domain extracts features from the blacklisted person or vehicle image, matches features of persons or vehicles detected in real time with those of the blacklisted person or vehicle, and generates an alarm upon match success. The vehicle library stores structured data, so features do not need to be extracted.

Data search: Users in the upper-level domain upload an image and deliver the image to a lower-level domain for 1:N search. Then the lower-level domain returns the search result to the upper-level domain. The search includes face, person, and passing vehicle search, person search by image, and vehicle search by image. Users in the upper-level domain can view alarms of lower-level domains.

Analysis task delivery: Users in the upper-level domain can create analysis tasks for cameras in lower-level domains. (CloudIVS 3000 V100R019C10 does not support the function.)

Algorithm Collaboration

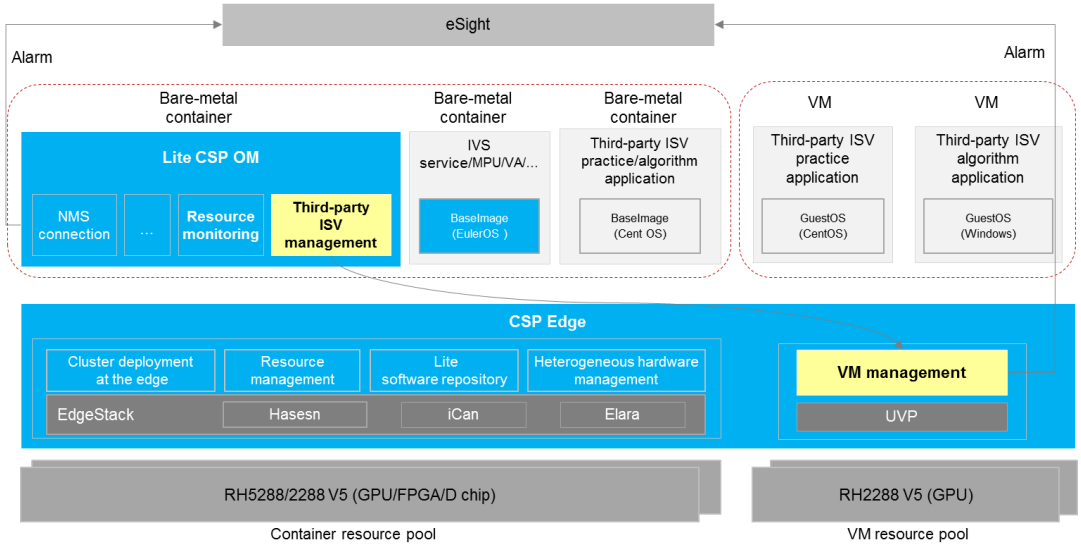
Algorithm plug-in synchronization and update: Users in the lower-level domain can check the local algorithm version in the upper-level domain and download the latest algorithm from the upper-level domain. Users in the upper-level domain can query the status and version of algorithms in lower-level domains.

Resource Collaboration

Users in lower-level domains can apply for analysis resources from the upper-level domain based on service scenarios. (CloudIVS 3000 V100R019C10 does not support the function.)

3.15 Centralized Management of Containers and VMs

CloudIVS 3000 V100R019C10 allows third-party applications to be deployed on VMs and supports centralized management of containers and VMs through the CSP OM portal.



3.16 GDPR Compliance

In 1995, the EU formulated the Data Protection Directive (Directive 95/46/EC) to protect the personal data of EU citizens. In 2012, the EU announced the Plan of Data Protection Rule Reform and proposed the General Data Protection Regulation (GDPR) draft, which was officially approved on April 14, 2016 and took effect on May 25, 2018.

Impact of GDPR on Huawei

GDPR is a law concerning the processing and flow of a natural person's personal data. GDPR sets out principles for the processing and flow of personal data, regulates the rights, obligations, and accountabilities for violation of GDPR of relevant stakeholders (data subject, data controller, and data processor), and specifies supervisory authorities and empowers them. Huawei entities need to make a lot of changes in terms of external business and internal management both inside and outside of the EU. Otherwise, Huawei may encounter a penalty of up to 20 million EUR or 4% global revenue.

Compliance Requirements Related to CloudIVS

Content that involves privacy in related materials must meet the privacy protection requirements specified in GDRP. The blacklist and redlist that are used for facial recognition or analysis must be stored in encrypted mode. The nationality search function must be removed. Operation logs need to be recorded for commands related to video or image query.

4 Analysis Algorithm Features and Principles

The CloudIVS 3000 provides a wide array of intelligent video analysis services such as license plate recognition, facial recognition, person search by image, video synopsis, video search, and behavior analysis, and constructs a series of rapid, convenient, and easy-to-use intelligent video analysis solutions for customers of different scales.

4.1 License Plate Recognition

CloudIVS3000 can connect to virtual checkpoints, featuring license plate recognition, flexible deployment and on-demand allocation.

4.1.1 Application Scenario

Fast urban development and raised living standards have fueled explosive growth of motor vehicles across major cities. Traffic management and urban security have become two major issues for modern city management. To address these issues, HD cameras can be installed in major city limits, key regions, and roads with heavy vehicle traffic. However, such projects involve huge investments.

Ever-growing Safe City development has fueled fast growth of HD cameras. By optimizing intelligent analysis algorithms, CloudIVS 3000 can extract license plates from video of HD cameras. This helps effectively reduce checkpoint construction costs and maximizes HD video resource usage.

4.1.2 Customer Benefits

Machines are used for vehicle analysis instead of human beings. The system can provide complete images and paths of a vehicle based on the license plate number. This function can effectively reduce human resource costs, shorten the processing duration, and improve case solving efficiency.

Blacklisted vehicle detection: When the system detects a license plate that matches a blacklisted license plate through real-time license plate number comparison, an alarm is triggered. This facilitates rapid vehicle tracking and monitoring and can help police officers capture the target vehicle.

4.1.3 Technical Principle

The license plate recognition technology analyzes and processes vehicle images or video shot by cameras based on the computer vision, digital image processing, and pattern recognition technologies to obtain the license plate number of each vehicle. It can detect and recognize license plates in video images, and no external trigger is required for vehicle and license plate detection. The system integrates multiple algorithms such as license plate locating, license plate character segmentation, and license plate character recognition, featuring high recognition efficiency, high speed, high adaptability, and ease-of-use.

License Plate Recognition System Architecture

The license plate recognition system first obtains required video images with the best quality through the video input management module, locates and tracks the license plate of a driving vehicle through the latest video detection technology, and then automatically extracts the license plate image. Through the accurate license plate

locating, license plate character segmentation, and license plate character recognition modules, the characters of the license plate are segmented and identified automatically and accurately so that the information about all the characters, color, and type of the license plate can be obtained.

The system adopts a highly modularized design, that is, each link of the license plate recognition process is achieved in an independent module. The image processing module includes preprocessing, license plate locating, character segmentation, and character recognition. The **license plate locating**, **character segmentation**, and **character recognition** are the key technologies. The following figure shows the license plate recognition process.

Figure 20. License plate recognition process

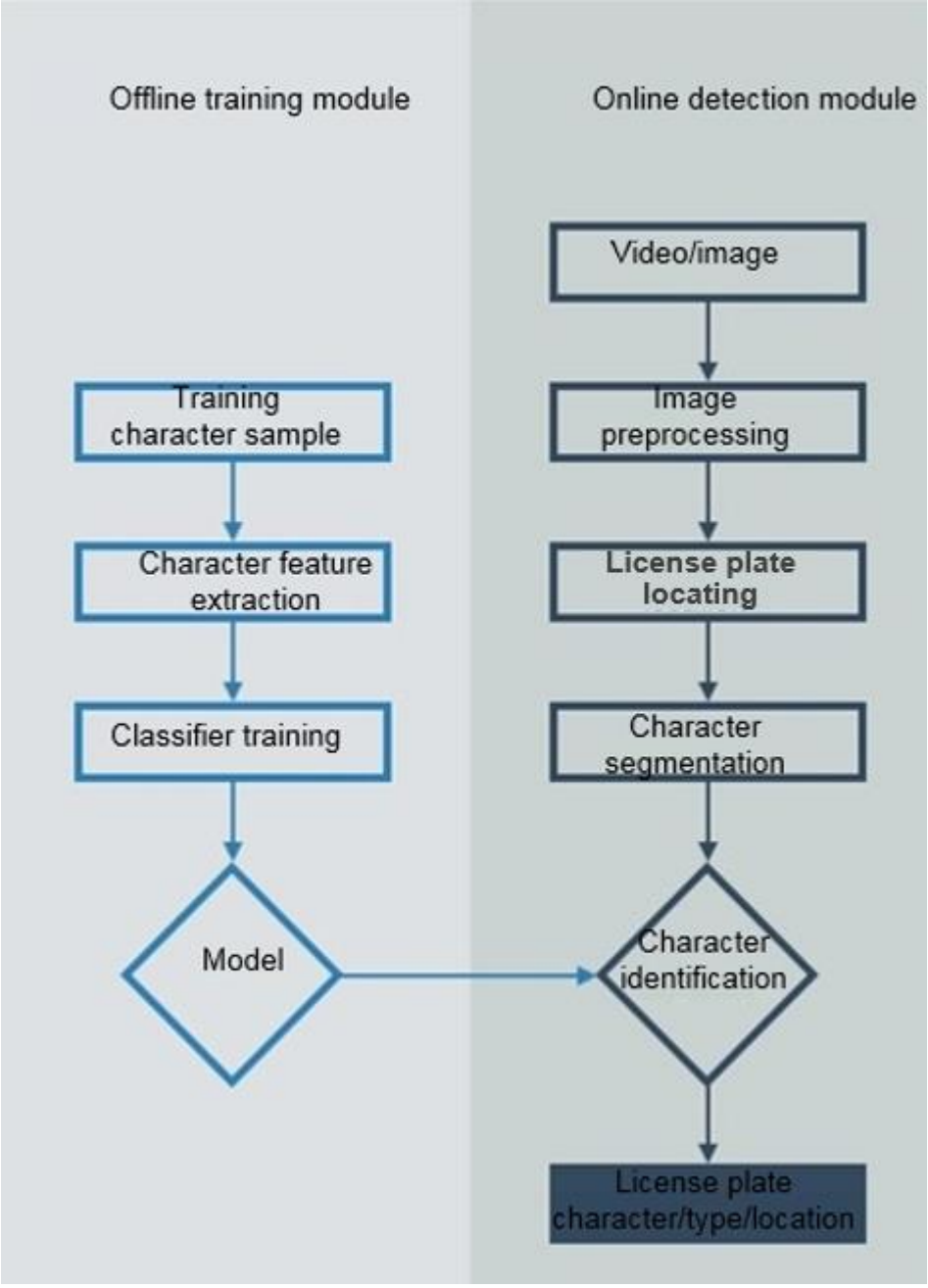


Image preprocessing refers to binarization, edge detection, noise removal, and gray-scale transformation on collected images. Image preprocessing can enhance the object image quality, that is, increasing the contrast of the object and the background image, to facilitate later license plate recognition.

License plate locating refers to locating a license plate in a captured image and extracting the license plate image from the image. License plate locating is the first step of key technologies, that is, the result of license plate locating directly affects character segmentation and recognition.

Tilt correction (optional) refers to detecting the tilt angle of the license plate image and correcting it. Tilted license plate images will result in tilt of characters in license plates, which directly affects license plate character segmentation and recognition. Therefore, the tilted images must be corrected.

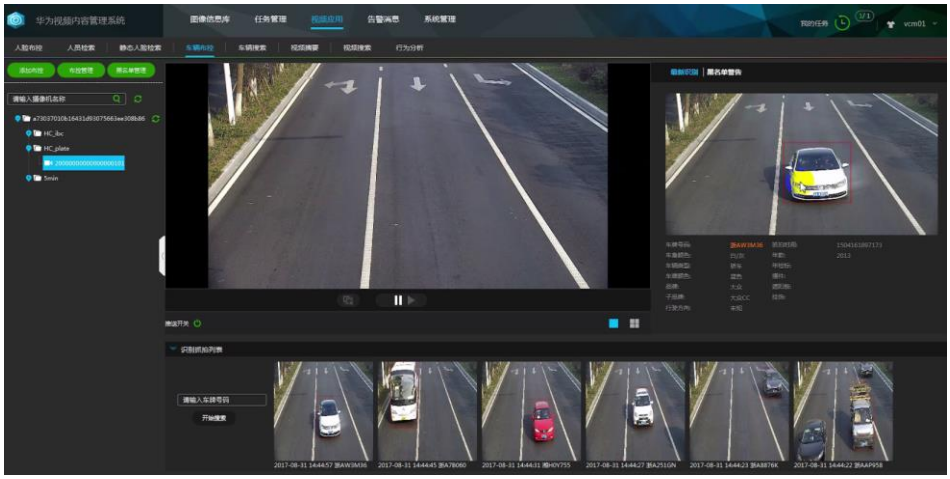
Character segmentation refers to segmenting the extracted license plate image and extracting single characters from the license plate image. Single characters segmented from images are used as input for character recognition, so the accuracy of character segmentation directly affects character recognition.

Character recognition refers to processing segmented characters and recognizing characters in the license plate. License plates in China contain Chinese characters, English letters, and digits, which increases difficulty of character recognition. The accuracy of character recognition directly affects the accuracy of license plate recognition.

4.1.4 Function Description

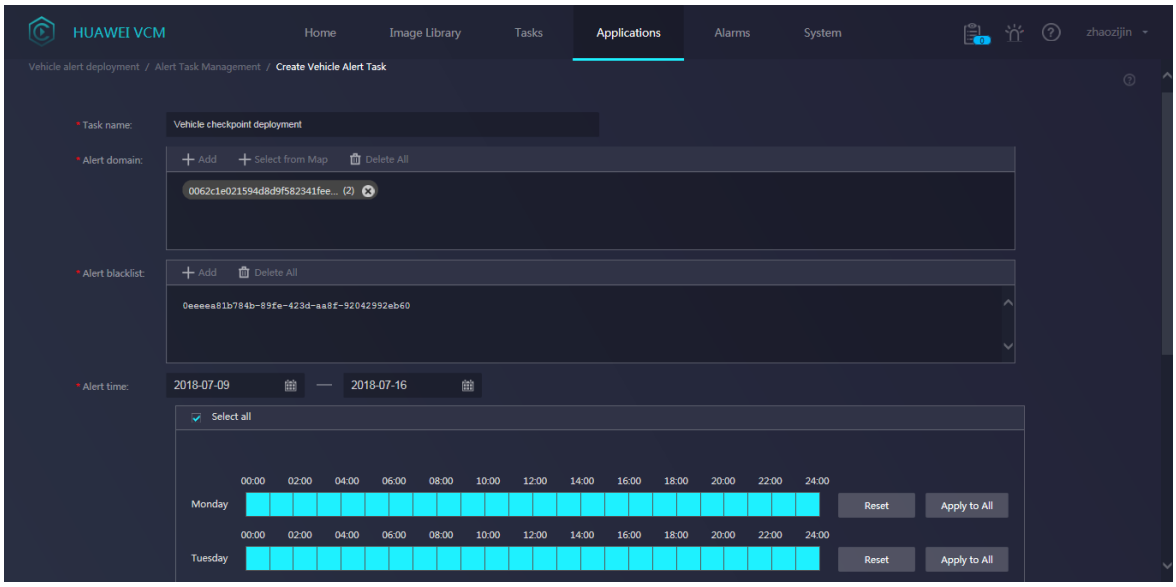
- **License plate recognition**

1. Allows users to add, modify, query, and delete license plates in the license plate library.
2. Supports extraction and identification of the license plate number.
3. Supports license plate recognition based on historical video, virtual checkpoint video, and paths.
4. Allows users to draw a trapezoid region of interest (ROI) on video images to perform license plate recognition.
5. Allows users to draw a polygon (maximum: decagon) ROI on video images to perform license plate recognition.



- **Real-time Blacklist Vehicle Alert**

1. The administrator is able to blacklist license plates. The system shall support uploading blacklisted license plates one by one or in batches. The blacklist license plates information and corresponding vehicle image files shall be provided by Procuring Entity.
2. The administrator is able to add, modify, query and delete blacklisted license plates.
3. The system can generate an alarm when a license plate on real-time video matches blacklisted license plate.
4. Allow the user to search for history alarms.



- **Vehicle Search**

1. Allows users to search for license plates in fuzzy mode.
2. The system supports displaying target vehicle on the GIS map.

4.2 Facial Recognition

The facial recognition function extracts facial features from video and images and then generates a facial feature library. This allows users to search for faces in the facial feature library by face image. Facial recognition also supports detection on human faces in live video through blacklisted face detection and can generate alarms when detecting matched faces.

4.2.1 Application Scenario

The development in economy, science, and technology speeds up urban construction, which concentrates population in urban areas and increases floating population, causing many urban management issues such as traffic control, public safety, key area security, and increasingly prominent cybercrime issues. In Safe City construction, public safety authorities are often unable to find valuable case-related information from large amounts of image data during case investigation. How to accurately obtain the identity information about a target person in a large number of people and make large amounts of video data a reliable weapon for video-based investigation? The facial recognition technology uses computers to analyze face images and compares detected face images with face images in the face image library to check the target's identity. The intelligent video analysis and alarm system based on facial recognition takes snapshots of faces of different objects, such as fugitives, suspects, controlled personnel, and personnel out of control, in key surveillance scenarios such as indoor aisles in airports, stations, and metros, compares the detected faces with face images in the face image library, checks their identities, and generates alarms in real time.

4.2.2 Customer Benefits

Users can search all persons recorded by surveillance cameras based on face images such as ID card photos, in-prison photos, inquiry photos, photos shot by mobile phones, or even surveillance images to quickly find target faces from the pedestrian library containing a large number of face images. This technology can be used in the

following scenarios:

1. When a first-hand clue is obtained (such as face images, which can be the photo on the ID card of a suspect, in-prison photo or inquiry photo of a serial criminal, or the photo shot by a witness's mobile phone), the paths and possible activity area of the suspect can be rapidly located through face search.
2. When full-body shots captured by cameras are found through reverse image search, you can search for face images of the target through the full-body shots and further track the target.
3. Lost children and elderly people can be located and tracked.
4. Users can deploy alert over multiple lists and flexibly control alert deployment policies.

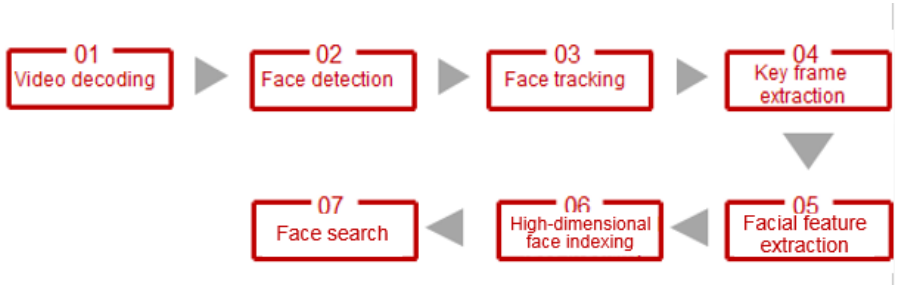
   Redlist: People whose privacy needs to be protected and VIPs can be added to a redlist. The redlist is used for search filtering and cannot return search results, protecting the paths of people in the redlist. The redlist is also used for alert deployment filtering. Even if a person in the redlist exists in the monitored personnel list (blacklist), no alert deployment alarm can be returned. In different scenarios, the filtering function can be configured. You can select only search filtering or alert deployment filtering, or both. The redlist is applied in the following scenario: Important leaders and special personnel cannot be retrieved or monitored.

   Whitelist: Legal personnel and registered personnel can be added to a whitelist, which is used to confirm the validity of personnel identities. The whitelist is applied in the following scenario: Only people in the whitelist can pass the identity authentication gate.

   Blacklist: The blacklist indicates the monitored personnel list. If a person's face image matches the face image of a person in the blacklist, an alarm is generated.

4.2.3 Technical Principle

The process of facial recognition is as follows: video decoding, face detection, face tracking, key frame extraction, facial feature extraction, high-dimensional face indexing, and face search.



Face detection refers to determining whether there is a face in a dynamic scenario and complex background and separating the face.

Face tracking refers to dynamically tracking the target based on the detected face.

Key frame extraction refers to extracting key frames suitable for facial feature extraction according to the face pose and size based on face detection and tracking.

Facial feature extraction refers to extracting the whole and partial high-dimensional features of the face through the in-depth network.

High-dimensional face indexing refers to using hash clusters to create indexes for high-dimensional facial features, improving search performance by more than 10 times.

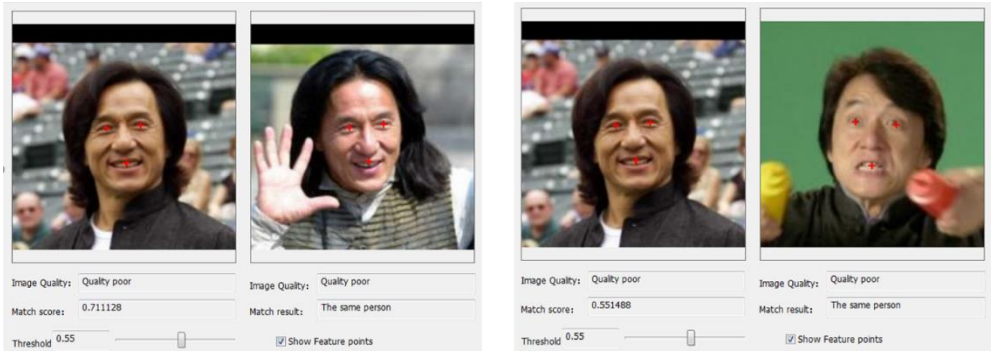
Face search refers to caching facial features in three levels through NVME and IPSAN to improve search efficiency.

Challenges of Facial Recognition

Compared with other biological features (such as fingerprints and irises), faces have the advantages of non-contact, easy to collect, and free of cooperation. However, due to the nature of faces and the influence of external factors, facial recognition is confronted with huge challenges. The same person's different face images can show great differences, mainly due to the face itself and the external environment.

The influence factors of the face itself include facial expressions and age. Because the human face is flexible and non-rigid, the geometric structure of the human face is a three-dimensional surface. The human face of different facial expressions is greatly different in shape, size, and texture structure. As the age increases, the facial skin becomes loose and generates wrinkles, so the age affects the texture of the face image. The following figure shows the face images affected by facial expressions.

Figure 21. Face images affected by facial expressions



External environment factors include illumination, angles, and blocks. The illumination has a significant impact on the imaging quality of the face in visible light. The change of illumination conditions will change the emission of light on the human face, which causes the texture change of the two-dimensional face image. Besides, due to the irregular three-dimensional shape of the face, different illumination conditions produce different shades in two-dimensional face images, leading to losses of some features in the face images. The highlights and shadows caused by the polarized light and side light affect the accuracy of facial analysis and recognition. Moreover, the change of the light environment in different scenarios at different time is often huge, which makes illumination a major challenge in facial recognition. The following figure shows the face images affected by illumination.

Figure 22. Face images affected by illumination

Face angles will seriously affect the appearance in face images. The face is three-dimensional and the image is two-dimensional, so that images captured in different angles give information about the face in different aspects. Due to the three-dimensional surface characteristic of faces, the angles of faces to the camera have a huge influence on two-dimensional images. Different face angles may result in losses of some features in face images. The following figure shows the face images affected by face angles.

Figure 23. Face images affected by face angles

Blocks, such as the hair, glasses, and ornaments, will also affect facial recognition, as shown in the following figure. Besides, image background, imaging parameters, and blood relationship will also cause changes in face images, affecting facial analysis and recognition performance.

Figure 24. Face images affected by blocks

Resolution: a maximum of 150 x 150 pixels and a minimum of 60 x 60 pixels

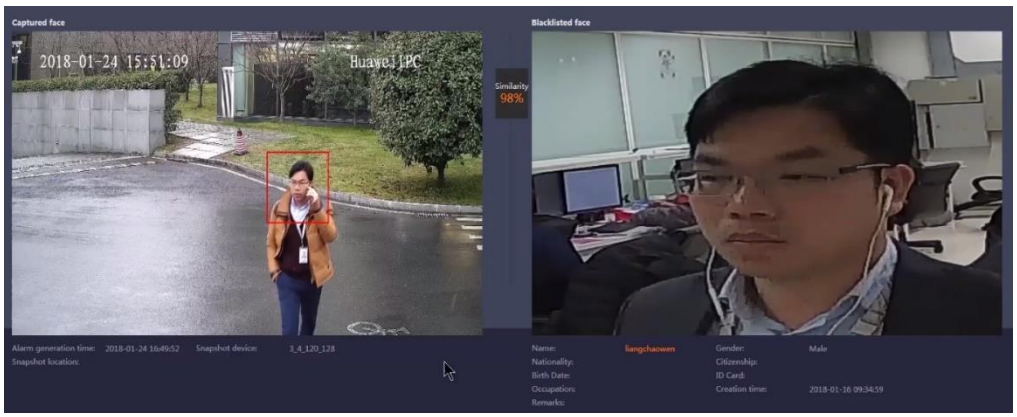
Key Technology Features of Facial Recognition

- Facial recognition can adapt to person checkpoint scenarios through deep learning, the ideal face detection condition is within 15 degrees upward or downward and 30 degrees leftward or rightward, and the ideal resolution is 60 x 60 pixels to 200 x 200 pixels.
- Facial recognition allows users to search for high-dimensional face images in a large scale and returns results within seconds.
- Facial recognition features a low error rate.

4.2.4 Function Description

- **Face search and match in static mode**

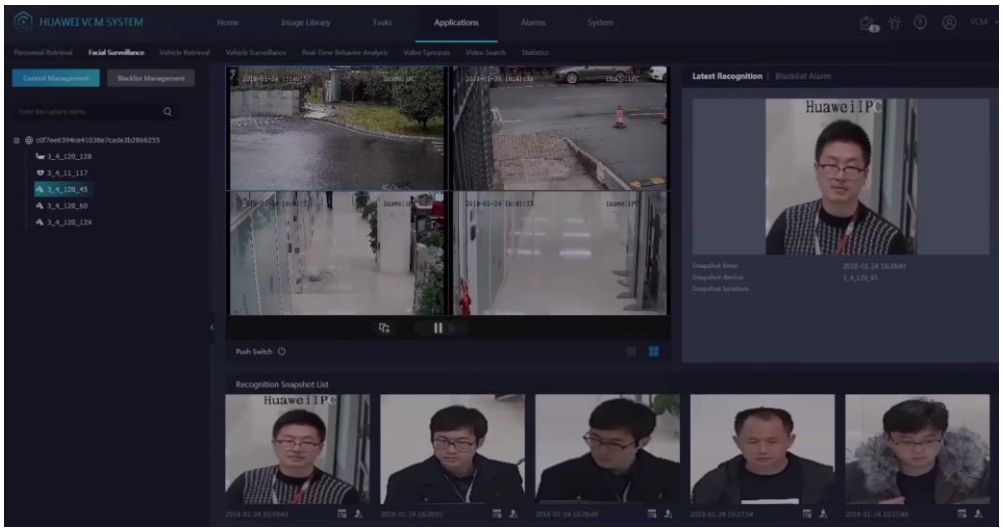
  A face image to be retrieved can be submitted through the platform client. The facial recognition system automatically extracts facial features from the face image, matches the features with all face images in the facial snapshot library or face registration library, and finally displays the match result.



  1:1 identity check: When a user uploads two face images, the system returns the similarity threshold.

  1:n static face image library search: Users can upload a face image to search for face images whose similarity is higher than the specified threshold in a specified static face image library.

- **Blacklisted face detection in real time**



  The surveillance cameras can be used to take snapshots of human faces in real time, and these faces can be recognized and related facial feature information can be stored in the facial feature library.

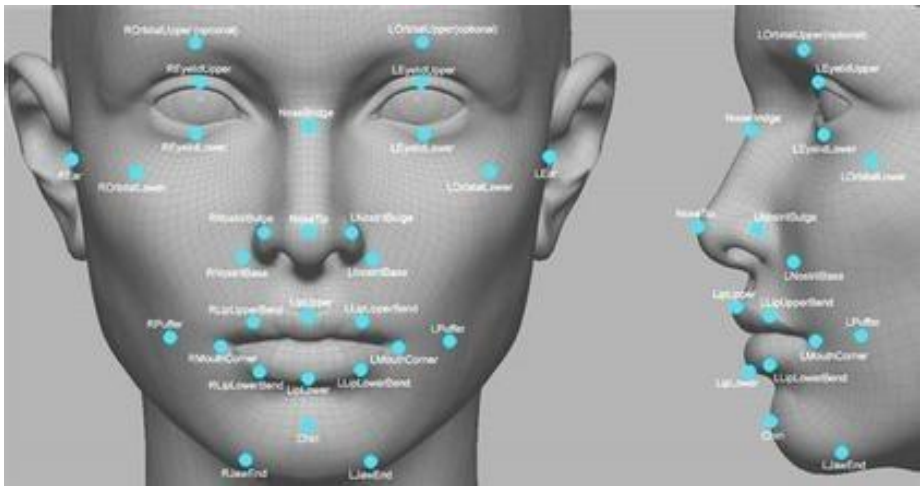
  Users can add monitored personnel such as fugitives, criminals, and terrorists to a blacklist. Then, the system extracts facial features of the blacklisted persons and imports the facial features into the computer database.

  The system analyzes face images in video in real time, compares the detected faces with the blacklisted faces, and generates an alarm when a detected face matches a blacklisted face.

  Users can add, delete, modify, or search for face images in a blacklist and group blacklists.

  Users can search for historical alarms.

- **Face path search**



Face images and facial features that are recognized in real time are stored in the pedestrian library.

The system can perform facial analysis (including real-time face detection, real-time facial feature extraction and importing, and real-time blacklist comparison and indexing) on face images captured by snapshot cameras and live and recorded video shot by person checkpoints. The system can also perform facial analysis on historical video, extract face images and facial features, and import them into the pedestrian library in real time.

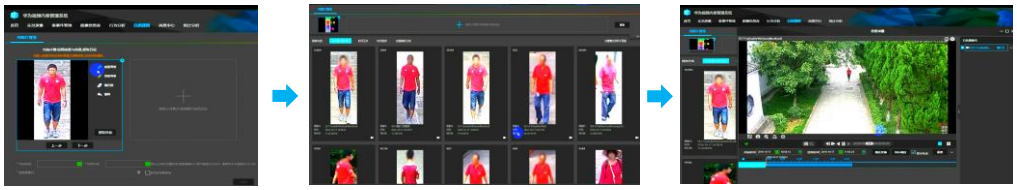
The system supports high-dimensional indexing of facial features and NVME hardware acceleration.

Users can search for faces in the pedestrian library. The search results can be sorted by similarity and time.

Paths of found faces can be displayed.

4.3 Person Search by Image

The reverse image search technology detects objects that pass cameras and extracts their appearance features. The system then imports the object images and feature data into the database and creates indexes to allow users to rapidly search for objects with similar appearance features within the cameras' surveillance area. The search results are sorted by similarity and displayed in snapshot mode, improving efficiency of checking surveillance video.



4.3.1 Application Scenario

Person search by image focuses on solving frequently occurred incidents and violent criminal cases. The person checkpoints are used to monitor the sidewalks, main buildings (enterprises and social institutions such as schools, hospitals, and banks), and entrances and exits of traffic hubs (such as subways and railway stations) in main roads of Safe Cities.

The main targets of the checkpoints are persons and non-motorized vehicles. The system provides personal feature analysis, personal attribute analysis, and face analysis. Users can manually import a full-body shot, box-select the area containing the full-body of the person, set the search period and similarity, and perform search. The search results are displayed in a view based on the level of similarity.

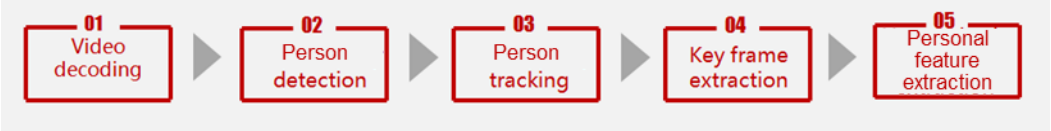
4.3.2 Customer Benefits

Users can search for an object based on full-body shots (from video synopsis, witness-shot photos, and manual check) obtained from first-hand clues and manually confirm the movement paths of the object. Users then can track the object or even obtain clearer photos (face images).

Users can retrieve first-hand image clues in the pedestrian library based on witnesses' structural description.

4.3.3 Technical Principle

Person search by image is implemented through video decoding, person detection, person tracking, key frame extraction, and personal feature extraction.



Person detection: Use the in-depth network to detect walking persons and riders with more than 80 pixels in images.

Person tracking: Use the Kernelized Correlation Filter (KCF) and in-depth features to accurately track objects.

Key frame extraction: Based on person detection and tracking, extract key image frames suitable for feature extraction according to the object posture, size, and moving direction.

Personal feature extraction: Use the in-depth network to extract the whole and partial high-dimensional features of persons.

4.3.4 Function Description

- Allows users to upload one to three images containing specified object features and then search for similar objects in the object library based on the features. The search results are sorted by similarity.
- Extracts and indexes object features from live video, historical video, and uploaded video.
- Extracts and indexes object features from historical video and uploaded video by segment and performs accelerated processing on historical video by segment.
- Allows users to enter personal features (such as head, body, leg, foreground, and background) on clients.
- Supports extraction of personal features, including gender, age, tops color, bottoms color, tops texture, tops style, bottoms style, glasses, hair, holding up an umbrella, wearing a mask, body size, carrying goods, shoulder bag, backpack, holding objects in the front, dragging articles, and riding state.
- Allows users to search the library of images captured by person checkpoints. The input images can be images captured by person checkpoints, uploaded images, or video snapshots.

- The intelligent acceleration on the CPU/GPU heterogeneous platform improves the retrieval performance of reverse image search.
- The system supports high-dimensional feature indexing and NVME acceleration.
- The system supports the person checkpoint scenario and virtual checkpoint scenario. In the person checkpoint scenario, the system aims to associate human bodies with faces, so that the results of reverse image search can be associated with face images. Then, the face images can be used for accurate search to provide data sources for face search.

Figure 25. Search by personal feature

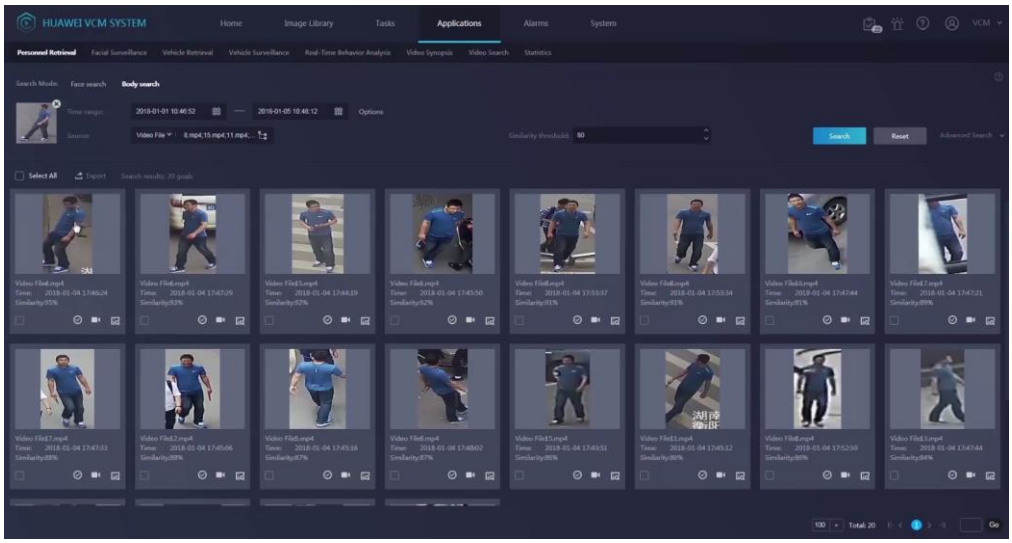


Figure 26. Search by riding status

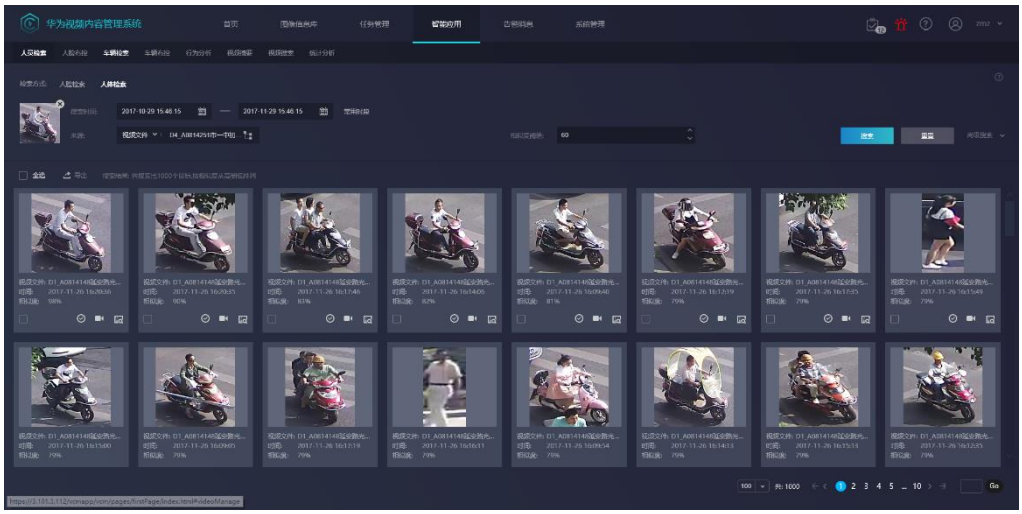


Figure 27. Search by personal attribute

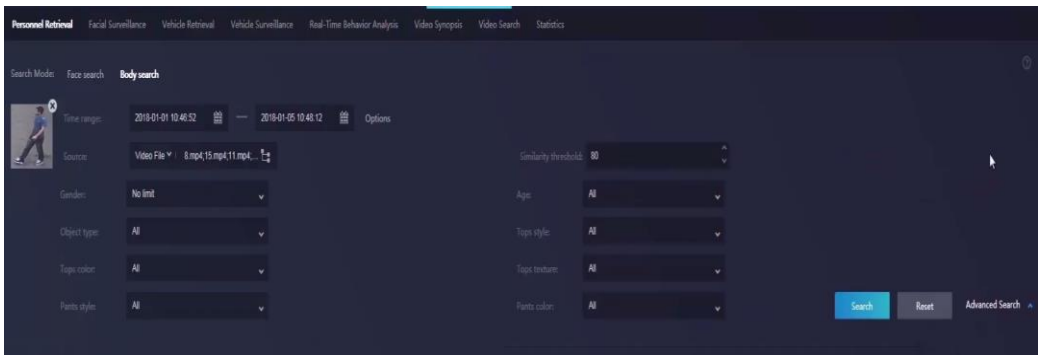
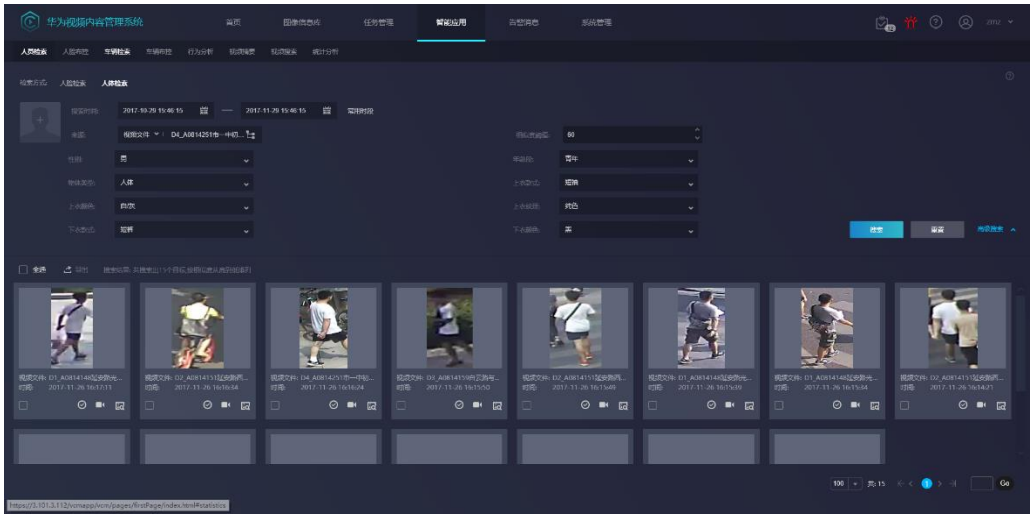


Figure 28. Filtering personal attributes



Virtual checkpoints function as a supplement to person checkpoints. Therefore, virtual checkpoints do not need to be deployed independently. You can reuse common cameras in Safe Cities as virtual checkpoints, which can provide a large amount of data. This aims to obtain first-hand clues of an object using reverse image search regardless of the existence of witnesses, and then obtain continuous paths of the object based on the first-hand clues.

4.4 Video Synopsis

With the video synopsis technology, the system can compress video files of a long period in the time or space dimension to form a valuable video clip. The video clip shows complete video content of the original video file, significantly improving video viewing efficiency.

4.4.1 Application Scenario

After a case occurs, the investigation takes a long time because many cameras are installed around the case occurrence location and the original video amounts to several hundred hours, which is likely to lose the right time of handling the case. With the video synopsis function, the system can compress the original video, delete static unnecessary images, and generate a short video clip. A video feed of one hour long can be compressed to a video

clip of several minutes, sharply enhancing the case investigation efficiency.

4.4.2 Customer Benefits

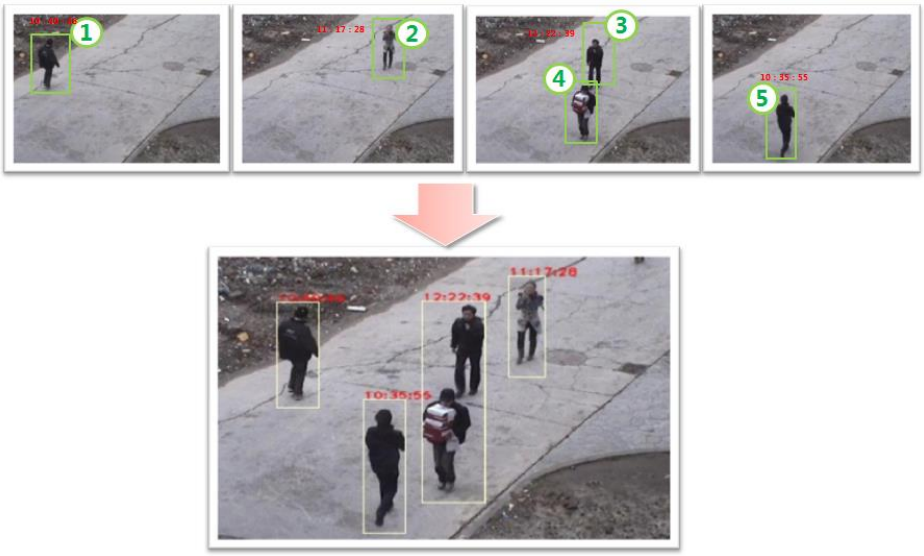
After an incident occurs without any witness or other clues, users can reduce video checking duration and improve video viewing efficiency through video synopsis, efficiently obtaining valuable information and clues from video.

4.4.3 Technical Principle

Through background and foreground object modeling, the CloudIVS 3000 with video synopsis technology can extract moving object paths from a video feed, splice different moving objects into the same background, sort all objects by time, and combine these objects in a new video feed. With the video synopsis technology, a video feed of several hours can be compressed into a short video clip of only several minutes, which records multiple critical events. Investigators can quickly obtain object information in the original video through video synopsis. This greatly shortens the video viewing time and enhances investigators' work efficiency. Investigators can also click an object in a compressed video to view the video where the object initially appears.

For example, as shown in the following figure, some objects appear in the original video at different time points. With the video synopsis technology, these objects can be displayed on the same video image, which greatly enhances video viewing efficiency.

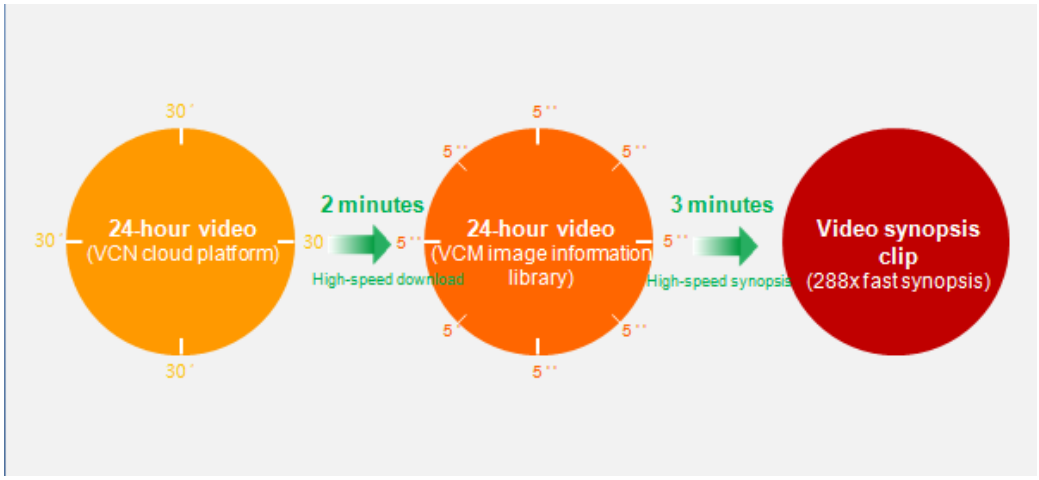
Figure 29. Video synopsis



The video synopsis process mainly consists of two steps. The first step is to create synopsis indexes: The moving object data in the metadata is associated according to certain principles to form synopsis indexes. The second step is to generate the synopsis video: The moving object metadata that meets the requirements and synopsis indexes are combined to generate the optimal trajectory combination of the object and generate the synopsis video through image integration.

In the process of creating synopsis indexes for video synopsis, the algorithm traces moving objects in video images frame by frame, and the number of moving objects is strongly correlated with the processing capability of the algorithm. Not restricted by video surveillance scenarios, Huawei's proprietary video synopsis optimization algorithm can track all moving objects concurrently in a series of images or the entire video, and can complete synopsis on a 5-minute video clip within 3 minutes. The algorithm supports the conditional synopsis mode. It retains all object metadata in the synopsis index analysis phase and temporarily generates combined video clips when clients request video playback. The algorithm supports different synopsis filter criteria without reanalyzing the video. These filter criteria include the direction, area, tripwire, maximum object, and minimum object.

Figure 30. Fast video synopsis



First step of video synopsis:

Divide a 24-hour video file into forty-eight 30-minute video segments. Multiple segments can be simultaneously downloaded to improve video file transmission and download efficiency.

Second step of video synopsis:

Subdivide each 30-minute video segment into six 5-minute video clips and then concurrently compress the clips by six machines in the CloudIVS 3000, which is equivalent to 288 (48 x 6) times compression, sharply increasing the compression efficiency.

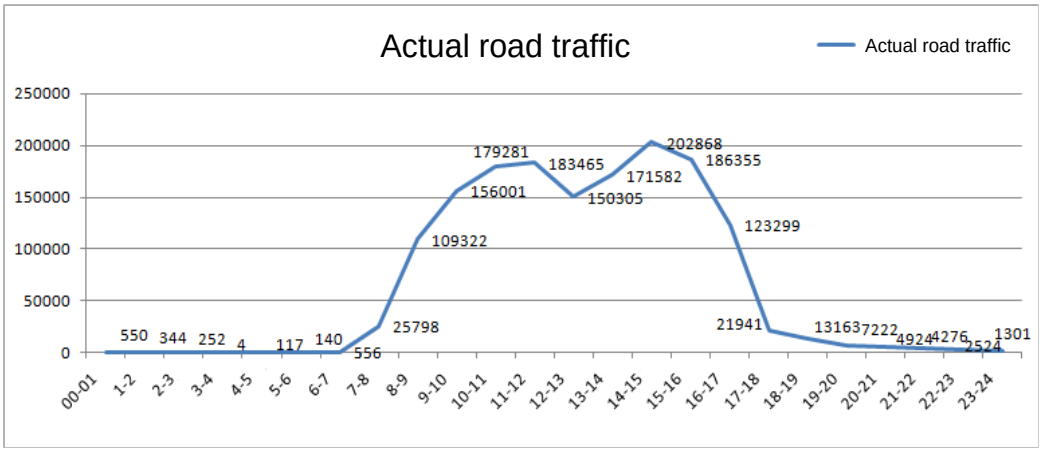
Third step of video synopsis:

Cut off useless still video segments to keep only the segments containing moving objects, sort the segments in time order, and combine the segments to generate a new video clip.

Video synopsis compression rate:

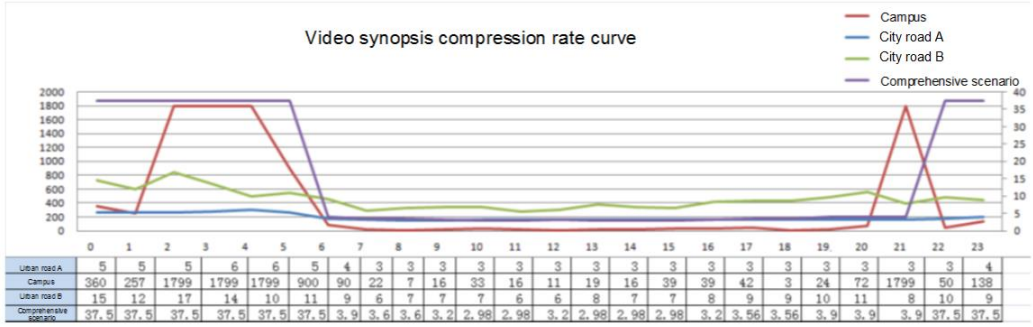
The following figure shows the change of road traffic in a city. It can be seen that there are traffic peaks in the morning and afternoon. The traffic before 07:00 and after 18:00 is relatively low.

Figure 31. Road traffic changes



The following figure shows the video compression rate at different time periods. Compared with the road traffic, the compression rate of the synopsis generally keeps in a relatively stable range of about 3. When the traffic is decreased to a certain extent, there will be a big jump in the compression rate of video synopsis.

Figure 32. Video synopsis compression rate changes by time



The traffic indicated by the red curve is relatively small, as shown in Figure 33. Except for commuting hours, the number of passing vehicles is very small, and there may be no car or no pedestrian in the early morning.

The traffic in city road A indicated by the blue curve is relatively stable, as shown in Figure 34. The traffic in daytime is relatively large, and cars continue passing by at night.

The traffic in city road B indicated by the purple curve is small, as shown in Figure 35. There are few cars passing by in the whole day, but occasionally, cars pass by at night.

Figure 33. Traffic in the campus

Figure 34. Traffic in city road A

Figure 35. Traffic in city road B

4.4.4 Function Description

- Allows users to play original and compressed video in comparative or associated manner.
- Supports video synopsis by specific criteria, such as direction, area (ROI), tripwire, maximum object, and minimum object.
- Supports common and fast video synopsis. The fast synopsis allows the system to segment a video feed, concurrently process multiple video segments, and use the hardware feature to optimize the synopsis.

4.5 Video Search

With video search technology, users can quickly and accurately locate key information in a large amount of video data by multiple search criteria, for example, space, time, object behavior, and object type.

4.5.1 Application Scenario

When a case occurs, it takes a lot of time and energy for the police to discover clues in video feeds. Also, it is easy to miss some clues. Therefore, the video search function can be used in the following scenarios:

- With feature search, the system can distinguish pedestrians from vehicles and support further filtering by certain criteria such as the vehicle color and clothes color.
- The system automatically displays paths of moving objects in video images and detects suspicious objects based on their moving paths.

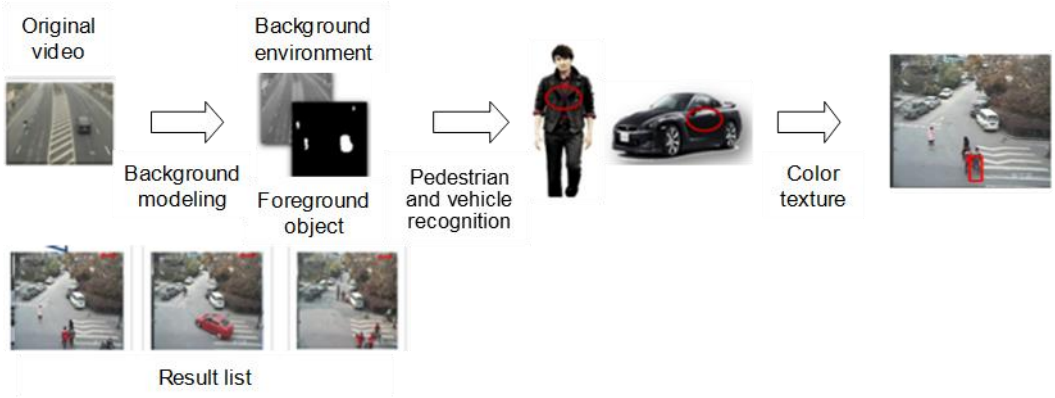
4.5.2 Customer Benefits

Users can quickly search for desired objects by object behavior, enhancing case cracking efficiency.

4.5.3 Technical Principle

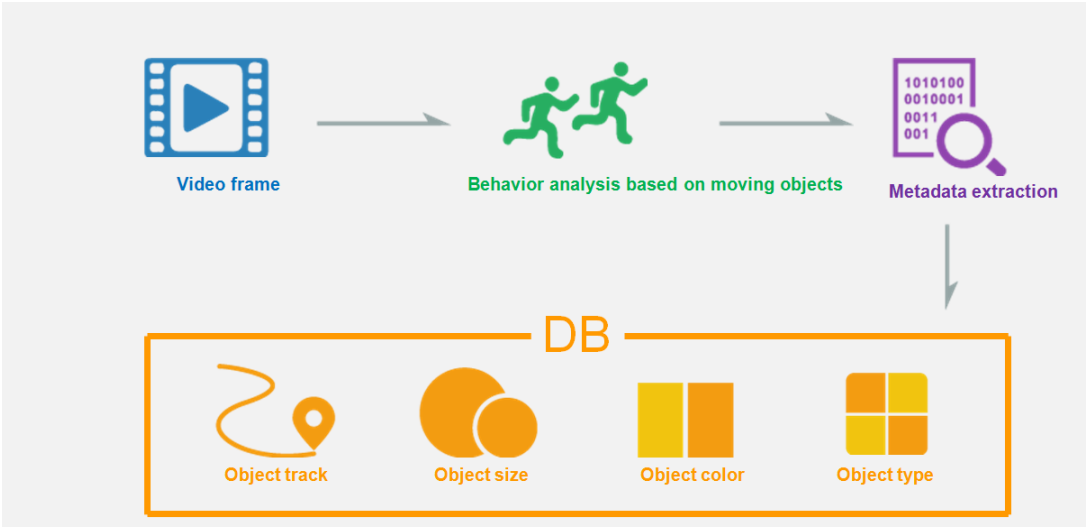
With video search, CloudIVS 3000 can intelligently analyze unstructured original video data, extract moving object features (such as the object color, size, and path) from the video through background and foreground modeling, and construct a structured database for objects. Then, investigators can quickly find wanted objects by specifying search criteria, including the object type (pedestrian, vehicle, or article), area where the object appears, moving direction, and object color. The objects that are found can be displayed in video thumbnails. Investigators can also click an object in synopsis video to view the original video where the object first appears. This helps improve investigators' work efficiency.

Figure 36. Video search



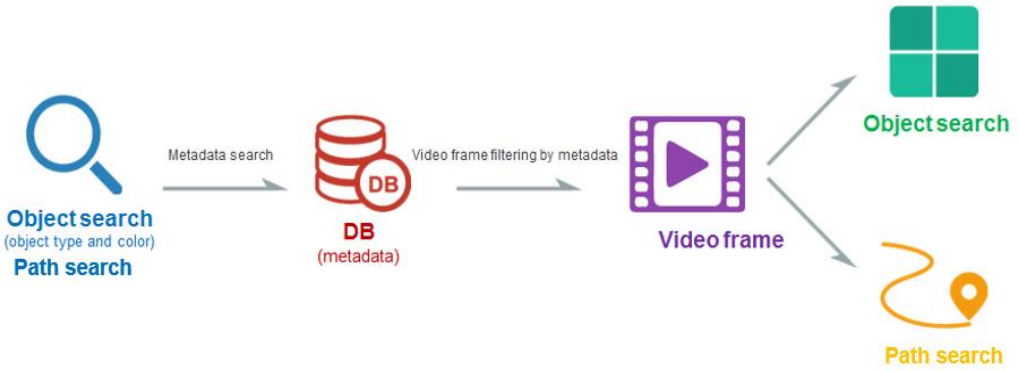
The video search process can be divided into metadata extraction and video search handling.

Figure 37. Process of extracting metadata for video search



- Process video frames based on behavior analysis of moving objects, and extract the background image and object metadata information of the image through background modeling, foreground extraction, and object tracking.
- Object metadata includes object trajectory, object size (resolution), object color (black, gray, white, red, yellow, green, blue, or unknown), and object type (pedestrian, vehicle, or unknown).
- Store the object metadata to the database metadata table. The metadata table contains the video file ID, object ID, size, type, color, trajectory, start time, and end time.

Figure 38. Video search process



- There are two types of video search: object search and path search. The object search requires criteria input, such as the object type (pedestrian, vehicle, or article), object color (black, gray, white, red, yellow, green, or blue), object size, object area, and excluded area. The system searches the metadata table based on the criteria and returns the required metadata.
- According to the result of metadata search and object trajectory information (indicated by a binary sequence of x, y, width, height, and time), the system obtains the timestamp of the trajectory midpoint, extracts the corresponding frames in the video file, and takes screenshots.
- For object search, the system frames and marks the object, takes a screenshot, and stores it.
- For path search, the system introduces the object trajectory recorded in the metadata table to the frames, takes a screenshot, and stores it.

4.5.4 Function Description

- Extracts object frames from video files and classifies them by pedestrian and vehicle. Then, users can query video files by pedestrian or vehicle.
- Supports fuzzy match to colors of objects that appear in video based on the user-defined color and sorts the results by color similarity.
- Allows users to set a detection area on the video. Then, the system can automatically detect moving objects entering this area.
- Allows users to set a non-detection area on the video. Then, the system will ignore objects entering this area.
- Allows users to set a tripwire along a moving direction on the video. Then, the system automatically generates an alarm when detecting a vehicle or pedestrian that crosses the tripwire from the specified direction.
- Tracks moving objects in the video and marks their paths. Then, users can quickly find suspicious objects through their paths.
- Allows users to quickly and accurately search for suspicious objects by multiple search criteria, for example, object type (pedestrian, vehicle, or article), area, moving direction, and object color.

- Supports multi-file search.

4.6 Behavior Analysis

The CloudIVS 3000 supports behavior analysis on live video and generates alarms when detecting abnormal behavior. The CloudIVS 3000 supports the following behavior analysis on live video: tripwire detection, intrusion detection, removed object detection, abandoned object detection, direction detection, loitering detection, crowd density detection, head counting, abnormal speed detection, and route detection.

4.6.1 Application Scenario

- **Tripwire detection**

  An alarm is generated immediately when an object crosses a predefined tripwire from a specified direction so that losses can be effectively and promptly prevented.

- **Intrusion detection**

  An alarm is generated immediately when an object enters a specified surveillance area so that losses can be effectively and promptly prevented.

- **Removed object detection**

  An alarm is generated immediately when a precious object is removed from a specified surveillance area so that losses can be effectively and promptly prevented.

- **Abandoned object detection**

  An alarm is generated immediately when an object is abandoned in a specified surveillance area so that losses can be effectively and promptly prevented.

- **Direction detection**

  An alarm is generated immediately when an object moves along the specified direction so that losses can be effectively and promptly prevented.

- **Loitering detection**

  An alarm is generated immediately when an object is loitering in a specified surveillance area for a specified time so that losses can be effectively and promptly prevented.

- **Crowd density detection**

  An alarm is generated immediately when the crowd density in a specified surveillance area exceeds the preset threshold so that losses can be effectively and promptly prevented.

- **Head counting**

  Crowd traffic in places such as a supermarket, market, or shopping mall, can be calculated. Analysis on the regular pattern and trend of the crowd helps users improve security measures.

  When the head counting function is adopted, the system automatically calculates the number of people in a surveillance area, effectively reducing errors in manual counting and human resource costs.

- **Abnormal speed detection**

  An alarm is generated when an object moves at a speed higher than or lower than a specified threshold.

- **Route detection**

  Through route detection, users can quickly find objects that move in a specified route.

4.6.2 Customer Benefits

The CloudIVS 3000 automatically detects key information in video feeds, reducing labor costs and improving

detection efficiency.

Both 24/7 surveillance and time-based surveillance are available to meet a variety of surveillance requirements and mitigate potential losses during shift changes.

Surveillance personnel need to view live video only when alarms are triggered. Therefore, the number of cameras that a surveillance person can manage increases dramatically, which helps reduce labor costs.

4.6.3 Technical Principle

- **Tripwire detection**

  The CloudIVS 3000 automatically generates an alarm when anything crosses a tripwire from a specified direction in a video surveillance area. When surveillance personnel find an object moving in the wrong direction on the video image, they can assign personnel to the site to handle the situation, preventing crises.

- **Intrusion detection**

  The CloudIVS 3000 automatically generates an alarm when an object enters a specified surveillance area. When surveillance personnel find an object that enters a specified surveillance area on the video image, they can assign personnel to the site to handle the situation, preventing losses.

- **Removed object detection**

  The CloudIVS 3000 automatically generates an alarm when an object is removed from a specified surveillance area. When surveillance personnel find an object that is removed from the surveillance area on the video image, they can assign personnel to the site to handle the situation, preventing valuable objects from being stolen.

- **Abandoned object detection**

  The CloudIVS 3000 automatically generates an alarm when an object is abandoned in a specified surveillance area. When surveillance personnel find an object that is abandoned in the surveillance area on the video image, they can judge the object impact and assign personnel to the site to handle the situation, maintaining public interests and personnel security.

- **Direction detection**

  The CloudIVS 3000 automatically generates an alarm when an object moves along the specified direction. When surveillance personnel find an object moving in the wrong direction on the video image, they can assign personnel to the site to handle the situation, preventing crises.

- **Loitering detection**

  The CloudIVS 3000 automatically generates an alarm when an object is loitering in a specified surveillance area. When surveillance personnel find that the loitering duration of an object exceeds the specified threshold in the surveillance area on the video image, they can assign personnel to the site to handle the situation, which effectively prevents crises.

- **Crowd density detection**

  The CloudIVS 3000 automatically generates an alarm when the crowd density in a specified surveillance area exceeds a preset threshold. When this alarm occurs, surveillance personnel can view on-site video and assign related personnel to the site to handle the alarm.

- **Head counting**

  The CloudIVS 3000 calculates the number of people in a specified surveillance area and analyzes the regular pattern and trend of the crowd, helping users to improve security measures.

- **Abnormal speed detection**

  The CloudIVS 3000 automatically generates an alarm when an object moves at a speed higher than or lower than a specified threshold. This function applies to street order maintenance.

- **Route detection**

The CloudIVS 3000 detects vehicles that illegally make a U-turn on the road to maintain the traffic order.

4.6.4 Function Description

- **Tripwire detection**

  The CloudIVS 3000 generates an alarm when anything crosses a tripwire from the specified direction in a specified surveillance area.

Figure 39. Tripwire detection

Tripwire detection provides the following functions:

1. Detects and distinguishes multiple objects that cross tripwires and generates alarms simultaneously.
2. Allows users to stretch the tripwire direction and automatically generates an alarm only when any crosses the tripwire from the specified direction.

- **Intrusion detection**

  The CloudIVS 3000 automatically generates an alarm when an object enters a specified surveillance area.

Figure 40. Intrusion detection

Intrusion detection provides the following functions:

1. Allows users to specify the shape (polygon) of a surveillance area.
   2. Allows users to set multiple surveillance areas.
2. Detects and distinguishes multiple objects that suddenly move to a specified surveillance area and generates an alarm.
3. Displays alarm information including the alarm type, occurrence time, duration, and object paths.

- **Removed object detection**

  The CloudIVS 3000 automatically generates an alarm when an object is removed from a specified surveillance area.

Figure 41. Removed object detection

Removed object detection provides the following functions:

1. Allows users to specify the shape (polygon) of a surveillance area.
2. Detects and distinguishes multiple objects that have been removed from a specified surveillance area and generates alarms simultaneously.
3. Allows users to set the time length (5s to 60s) when an object is removable. If an object has been removed for a time length longer than the preset value, the system generates an alarm.
4. Displays alarm information including the alarm type, alarm occurrence time, and object location.

- **Abandoned object detection**

  The CloudIVS 3000 automatically generates an alarm when an object is abandoned in a specified surveillance area.

Figure 42. Abandoned object detection

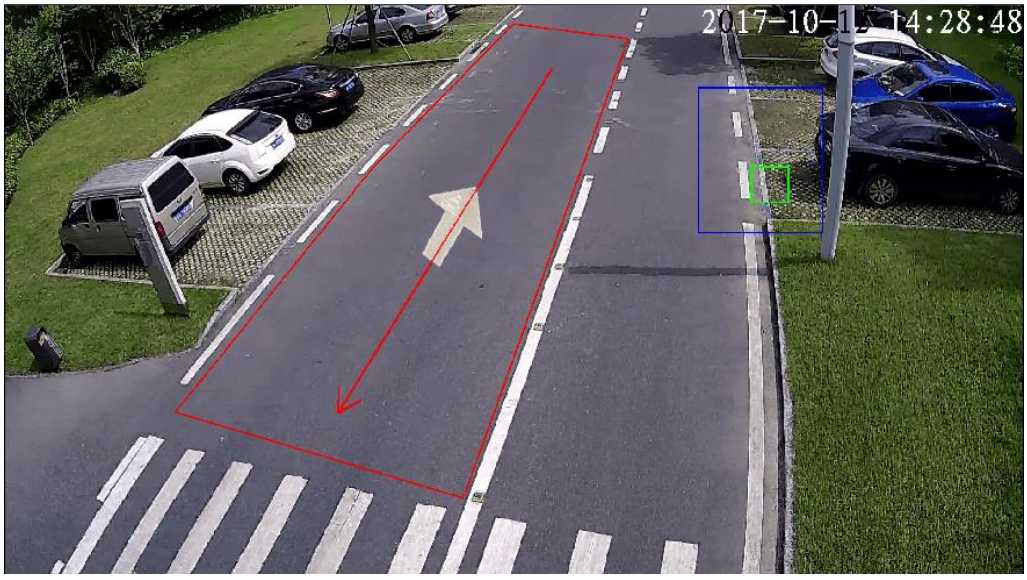
Abandoned object detection provides the following functions:

1. Allows users to specify the shape (polygon) of a surveillance area.
2. Detects and distinguishes multiple objects that are abandoned in a specified surveillance area. When the abandoned object has a color similar to the background color (which can be distinguished by naked eyes), the system can effectively identify and track it.
3. Allows users to specify an object abandoned duration (5s to 60s). When the duration has elapsed, the CloudIVS 3000 generates an alarm.
4. Displays alarm information including the alarm type, alarm occurrence time, and object location.

- **Direction detection**

  The CloudIVS 3000 automatically generates an alarm when an object moves in the wrong direction in a specified surveillance area.

Figure 43. Direction detection



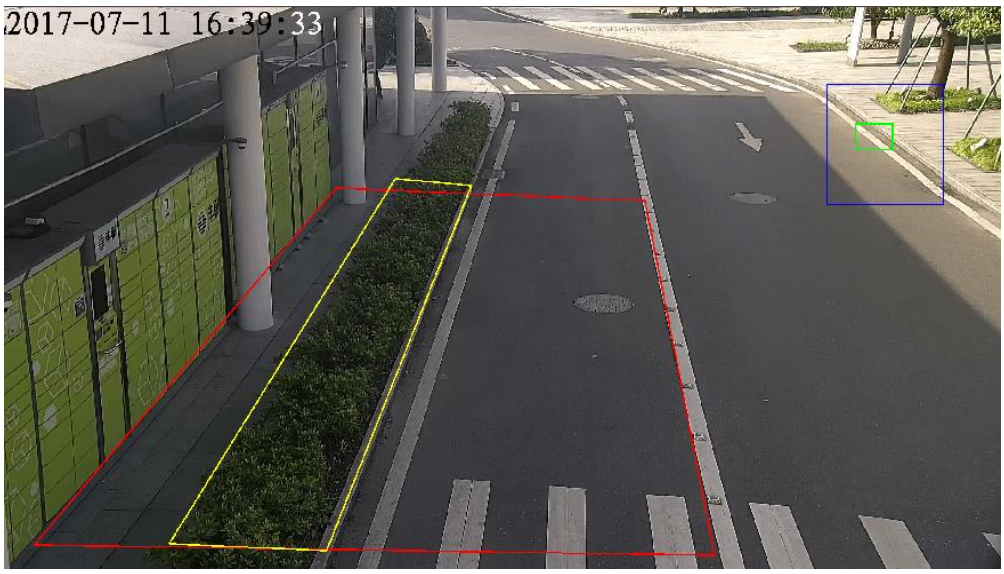
Direction detection provides the following functions:

1. Identifies all objects moving in the wrong direction in a specified surveillance area and generates alarms.
2. Accurately tracks an object whose color is similar to the background color.
3. Displays alarm information including the alarm type, alarm occurrence time, and object location.

- **Loitering detection**

  The CloudIVS 3000 automatically generates an alarm when a person is loitering in a specified surveillance area for a specified period of time.

Figure 44. Loitering detection



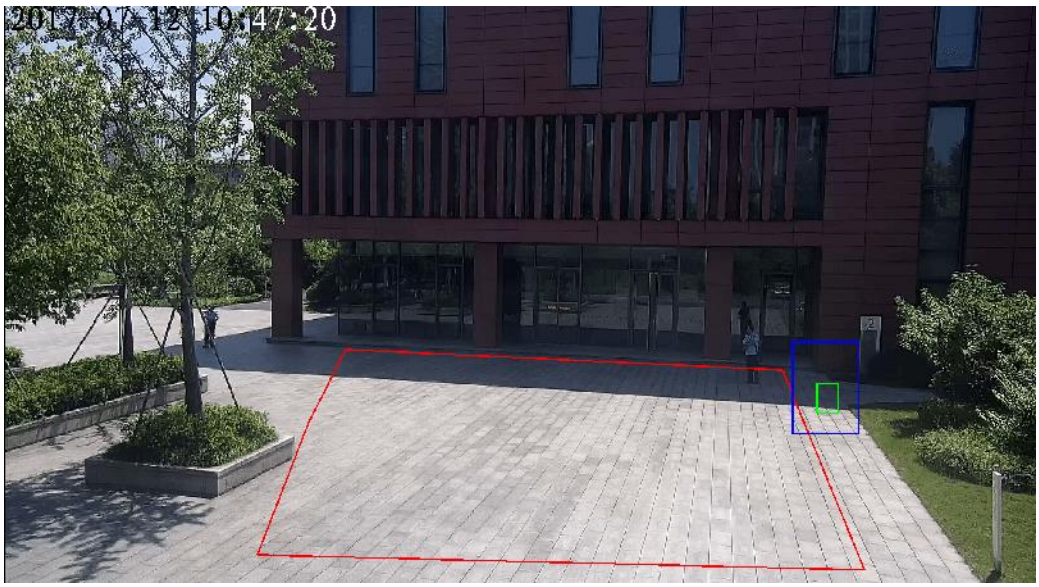
Loitering detection provides the following functions:

1. Allows users to specify the shape (polygon) of a surveillance area. Only objects that enter the surveillance area can trigger alarms.
2. Allows users to specify an acceptable loitering duration (5s to 30s). When the loitering duration has elapsed, the CloudIVS 3000 generates an alarm.
3. Displays alarm information including the alarm type, occurrence time, object paths, and object marks.

- **Crowd density detection**

  The CloudIVS 3000 automatically generates an alarm when the crowd density in a specified surveillance area keeps above the preset threshold in a specified period (5s to 60s).

Figure 45. Crowd density detection



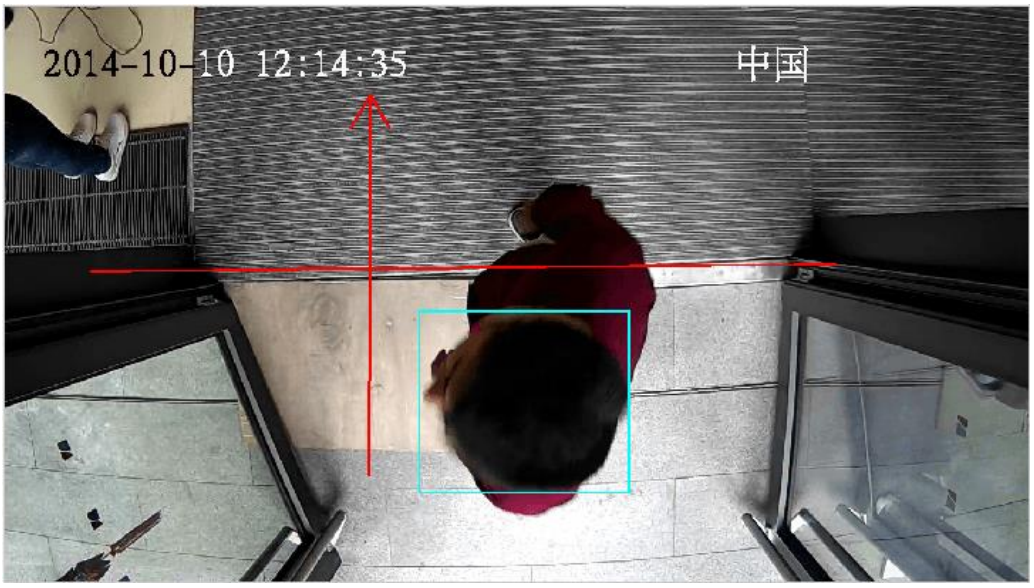
Crowd density detection provides the following functions:

1. Allows users to specify the shape (quadrangle or polygon) of a surveillance area.
2. Allows users to set the threshold for the crowd density detection alarm. When the crowd density in a specified surveillance area exceeds the preset threshold, the VCM generates an alarm and provides the real-time crowd density.

- **Head counting**

  The CloudIVS 3000 automatically counts the total number of persons that enter and exit a specified surveillance area.

Figure 46. Head counting



Head counting provides the following functions:

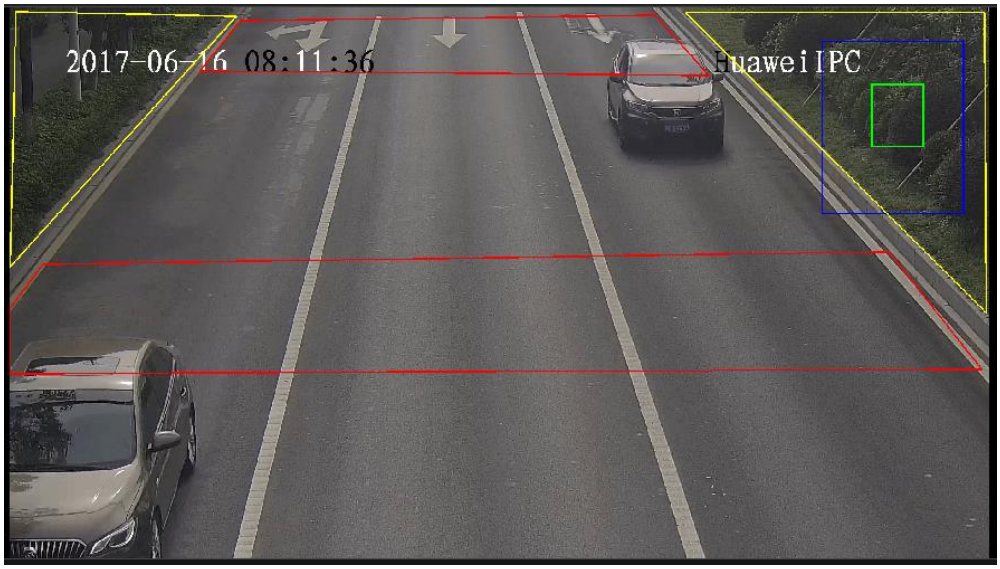
1. Automatically collects statistics on the number of people entering or leaving a specified surveillance area.

2. Allows users to specify the direction (unidirectional or bidirectional) of population flows to count.
3. Collects statistics, including the number of people entering and leaving a specified surveillance area and statistical time.

- **Abnormal speed detection**

  The CloudIVS 3000 automatically generates an alarm when an object is moving at a speed higher than or lower than a specified threshold.

Figure 47. Abnormal speed detection



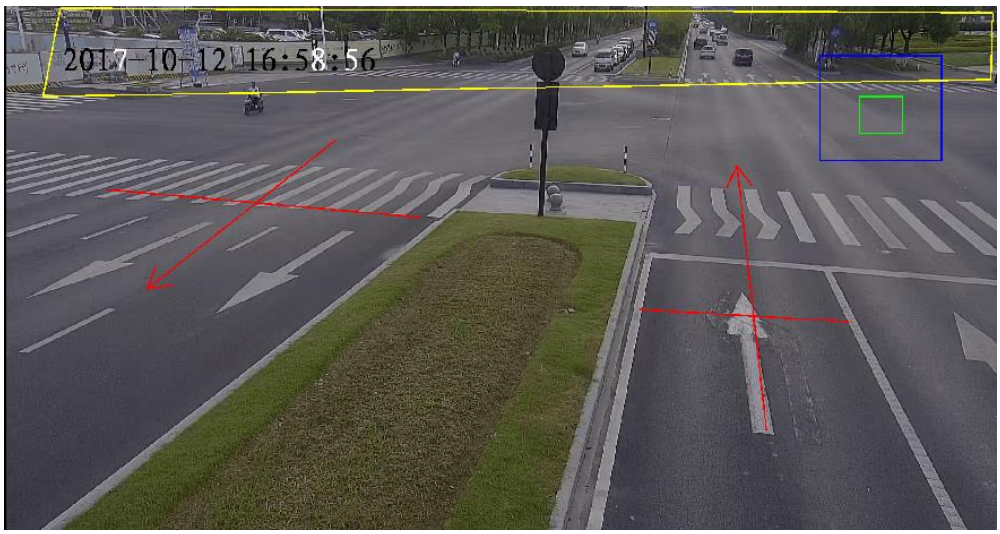
Abnormal speed detection provides the following functions:

1. Allows users to set two target areas in a surveillance area, an over-speed threshold (1s to 50s), and a low-speed threshold (1s to 100s). When the duration for an object to pass the two target areas is lower than the over-speed threshold or higher than the low-speed threshold, the CloudIVS 3000 generates an alarm. Users can only set the allowed time interval for an object to pass the two target areas. Therefore, users need to calculate the corresponding speeds based on the distance between the two areas and the detected time interval.
2. Displays alarm information including the alarm type, alarm occurrence time, and object location.

- **Route detection**

  The CloudIVS 3000 automatically generates an alarm when the movement path (marked with multiple lines) of an object meets the predefined route detection rule.

Figure 48. Route detection



Route detection provides the following function:

Allows users to set a maximum of two tripwires (including directions). A tripwire and a specified direction can form a route. If an object moves in the specified route, an alarm is generated.

5 Sensitive Feature Disclaimers

In response to Customer's explicit request, Huawei makes commercially reasonable efforts to provide the facial recognition and reverse image search features ("Features"). The Features are used to recognize human faces that pass a specified surveillance area, generate alarms upon detecting a blacklisted human face, and search for required images by uploading full-body shots. Huawei will not enable or use the Features without customer's authorization, or acquire any information about Customer's usage or maintenance of the Features. Customer and its authorized parties shall, as required by applicable laws and regulations, provide the users, governmental bodies, and any other third parties with necessary information, and obtain and reserve all necessary consents, licenses, and authorizations, when using and maintaining the Features. Applicable laws and regulations, user agreements, terms of use, privacy policy or statement, any other lawful agreements ("Agreements"), and publicly or targeted statements ("Statements") shall not be violated. Huawei provides the Features for Customer as per Customer's warrants to Huawei that Customer will use and maintain the Features as permitted by applicable laws and regulations, Agreements, and Statements. Huawei will not bear any legal obligations or liabilities, including but not limited to, claims, liabilities, obligations, costs, expenses, penalties, injunctions, judgments, that are not caused by Huawei's misconduct when Customer and its authorized parties are using and maintaining the Features.

In the event that any governmental body adopts laws and regulations, or Customer signs agreements with third

parties or makes statements, which materially affects the legitimacy of the Features wholly or partially, or the provision of the Features, Huawei reserves its rights to, at its sole discretion, terminate the provision of the Features without any liability to the extent permitted by law.

6 Appendix A References

《IVS V100R019C00轻量云系统架构设计说明书（v0.1,2018-06-30）》

《CloudIVS V100R019C00 系统架构设计》

《CloudIVS V100R019C00 轻量云规格清单》

《华为VCN3000系列技术白皮书 V1.6（C20171211）》

《CloudVCN V100R003 技术白皮书 V1.1（C20180301）》

《华为 CloudVCM V100R003C00 技术白皮书 V1.2（C20180523）》

《CloudIVS V100R019C10版本安全性设计说明书》

《IVS V100R019C10 CloudIVS 3000规格清单》

7 Appendix B Acronyms and Abbreviations

英文缩写	英文全称
CU	Client Unit
DAS	Direct Attached Storage
DCG	Device Connection Gateway
DVS	Digital Video Server
DVR	Digital Video Recorder
GOP	Group of Pictures
IP	Internet Protocol
IPC	IP Camera
IP SAN	IP storage area network
IVS	Intelligent Video Surveillance
MC	Mobile Client
MDU	Media Distribution Unit
MRU	Media Record Unit
MTU	Media Transcoding Unit
MU	Media Unit
NAS	Network-Attached Storage
NVR	Network Video Recorder

NTP	Network Time Protocol
OMU	Operation Maintenance Unit
ONVIF	Open Network Video Interface Forum
PAG	Peripheral Access Gateway
PC	Personal Computer
PCG	Platform Connection Gateway
PU	Peripheral Unit
SMU	Service Manage Unit
SCU	Sevice Control Unit
SDK	Software Development Kit
CMU	Cluster Manage Unit
MAU_QD	Media Analysis Unit-Video Quality Diagnosis
DDB	Distributed DataBase
DFS	Distributed File System
DPC	Data Process Center
SBI	Search By Image
SE	Searching Engine
FE	Feature Extraction
PR	Pedestrian Recognition
MCS	Media Content Search
MCSS	Media Content Storage Server
VA	Video Analytics

VA-OA	VA-Object Analyser
VA-OD	VA-Object Dector
VCM	Video Content Management
VCN	Video Cloud Node
ROI	Region Of Interest
RONI	Region Of Non Interest
SAN	Storage Area Network
IP	Internet Protocol
IPSAN	SAN Over IP
NAS	Network Attached Storage
NVR	Network Video Recorder
VMU	VideoManagement Unit
MPU	Media Process Unit
IVS	Intelligent Video Surveillance system
MU	Media Unit
IMGU	Image Unit
DCG	Device Connection Gateway
OMU	Operation Maintenance Unit
CU	Client Unit
PU	Peripheral Unit
PCG	Platform Connection Gateway
CMU	Cluster Management Unit

SMU	Service Management Unit
MAU_QD	Media Analysis Unit_Video Quality Diagnosis
SCU	Service Control Unit
MP	Media Process
VA	Video Analytics
TS	Text Search
Alarm Server	VCM Alarm Server VCM
GIS	Geographic Information System
MSU	Media Storage Unit
MAU	Media Analytics Unit
SEM	Service Engine Management
SEM_Agent	Service Engin Management Agent
MongoDB	NOSQL Database
GPU	Graphics Processing Unit
CPU	Central Processing Unit
SSD	Solid State Drive
DDR4	Double-Data-Rate Fourth Generation SDRAM
SDRAM	Synchronous Dynamic Random Access Memory
RAID	Redundant Array of Independent Disks
PCI-E	PCI Express