



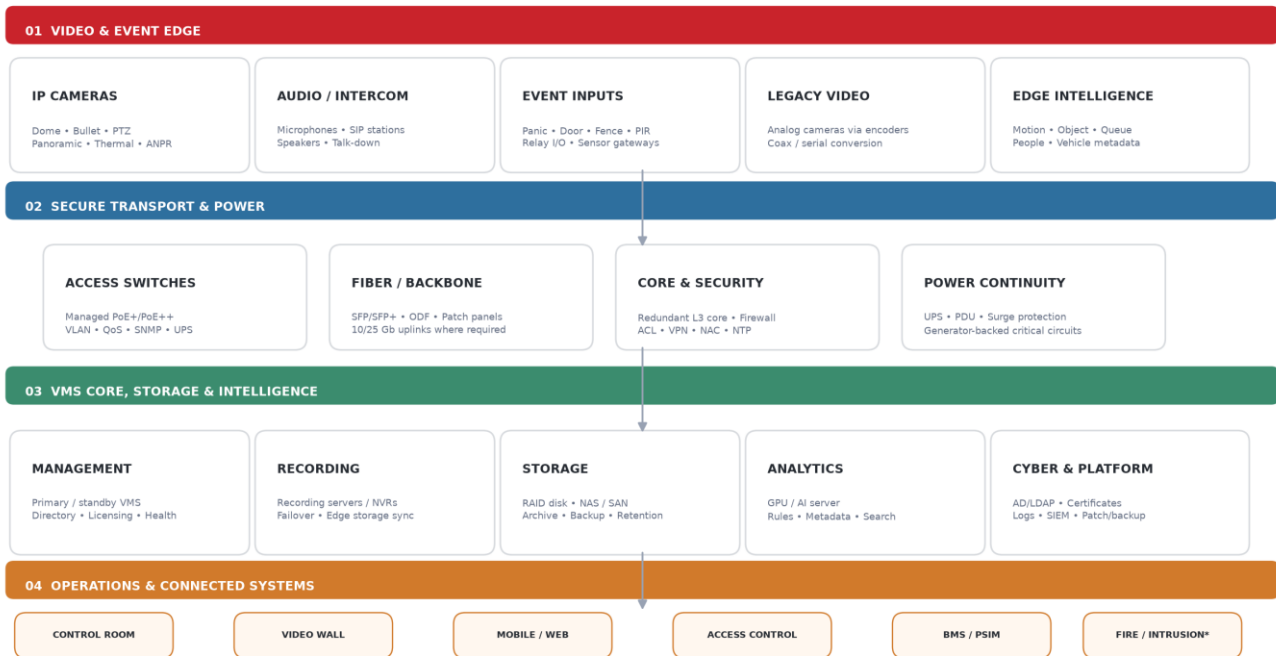
TECHNICAL CONCEPT & EQUIPMENT SCHEDULE

Intelligent Video Management System

Unified video • event intelligence • resilient recording • integrated response

INTELLIGENT VIDEO MANAGEMENT SYSTEM — CONNECTED ARCHITECTURE

Edge devices → resilient network → VMS core → operators, analytics and integrated response



*Fire-alarm integration is supervisory/event-driven only; certified life-safety control remains independent.

Prepared by Scorpions Services

Design, integration, programming, commissioning, training and lifecycle support

Document status	Concept / design basis
Issue date	22 September 2026
Application	Commercial • healthcare • hospitality • campus • industrial • infrastructure

Executive overview



Modern centralized VMS security operations environment.

Scorpions Services proposes an open, scalable and cyber-secure Video Management System (VMS) that unifies live monitoring, resilient recording, intelligent search, alarm verification, evidence management and multi-system integration. The design follows the company profile commitment to intelligent building ecosystems: video is not an isolated CCTV island; it becomes an operational information layer connected to access control, intrusion, intercom, building management, parking, alarms and approved business workflows.

Purpose of this document

This is a manufacturer-neutral technical concept and comprehensive equipment schedule. Final quantities, exact models, lens selections, storage capacity, network bandwidth, retention period, redundancy and compliance options must be confirmed through a site survey, risk assessment, camera-location plan and approved client brief.

Business outcomes

- One command interface for live, recorded and event-driven video across one site or multiple sites.
- Faster incident verification using alarm-linked video, maps, nearby cameras, bookmarks and standard operating procedures.
- High evidential integrity through controlled export, digital signing/watermarking where supported, audit logs and role-based access.
- Resilient service using distributed recording, edge storage, failover, RAID storage, UPS and health monitoring.
- Lower operator workload through metadata search, object classification and carefully tuned analytics.
- Future-ready integration through ONVIF profiles, vendor SDK/API, REST, webhooks, OPC/MQTT middleware, SIP and dry-contact I/O as appropriate.

Scope boundaries

Included in the VMS concept	Design boundary / clarification
Cameras, audio, intercom, encoders, analytics, network, servers, storage, control-room equipment, software, integration and power continuity.	Exact quantities and makes/models are project-specific and are not implied by this concept.
Event receipt from access control, intrusion, BMS, parking, fire alarm and other approved systems.	Certified life-safety, access and equipment-protection logic remains in its dedicated system.
Remote/mobile access for authorized users.	Remote access requires client-approved VPN, MFA, hardening and information-security policy.

Intelligent VMS architecture



Integrated camera, access, intercom and operator environment.

INTELLIGENT VIDEO MANAGEMENT SYSTEM — CONNECTED ARCHITECTURE

Edge devices → resilient network → VMS core → operators, analytics and integrated response

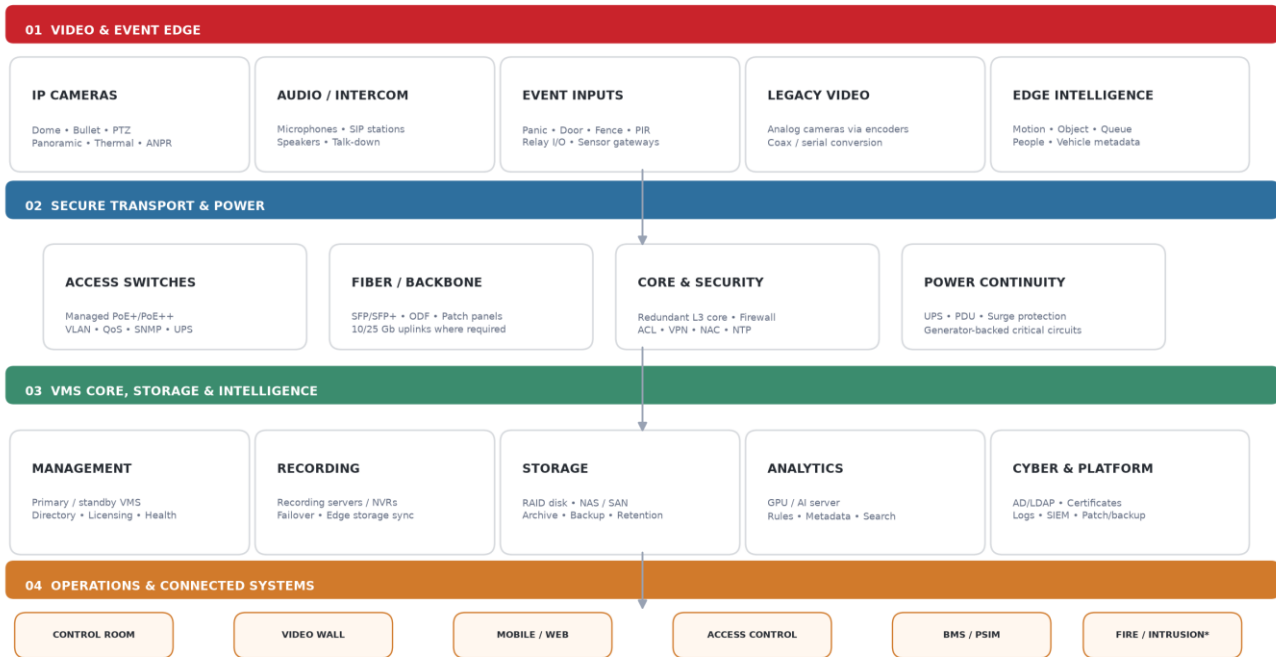


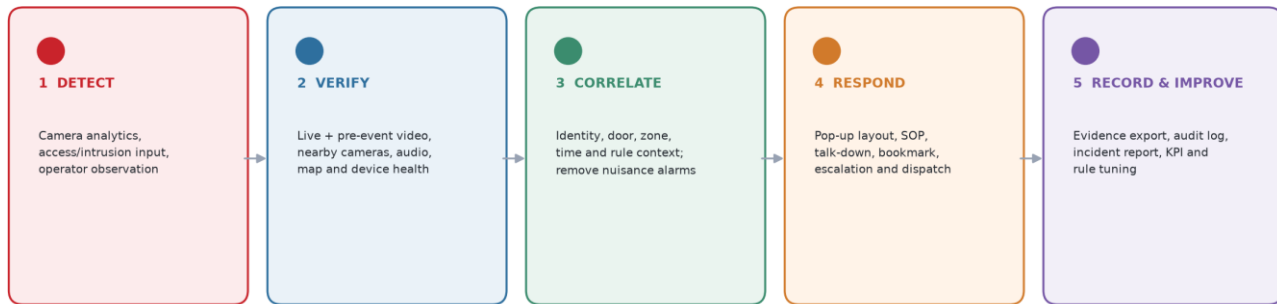
Figure 1 — Logical architecture. The final project may centralize or distribute recording by site, building or security zone. Bandwidth and failure-domain analysis determines where recording servers and storage are located.

Architecture principles

Principle	Design intent
Open edge	Prefer ONVIF-conformant IP devices and verified driver compatibility; retain vendor-native features only where they add measurable value.
Distributed resilience	Keep recording close to cameras where practical; allow cameras to continue edge recording if the server/network path fails.
Separation of duties	Separate camera, management, storage and client traffic logically; restrict administration to approved roles and networks.
Evidence by design	Synchronize time, preserve audit logs, control exports and document chain-of-custody procedures.
Health before failure	Continuously supervise camera tamper, packet loss, storage state, recording gaps, temperature, UPS and switch health.
Scalable licensing	Size licenses and infrastructure for the initial scope plus an agreed growth margin; avoid hidden channel/feature constraints.

INTELLIGENT EVENT-TO-RESPONSE WORKFLOW

Correlate video, analytics and building events—then guide the operator through a controlled response.



Design principle: event-driven video reduces operator workload, while human authorization remains mandatory for consequential actions.

Connected equipment — edge video & field devices



Representative enterprise IP camera families and installation environments.

Equipment	Purpose	Minimum technical detail / selection criteria	VMS connection
Fixed indoor dome camera	General indoor coverage; discreet, vandal-resistant option	4–12 MP; H.265/H.264; WDR ≥120 dB typical; IR as required; microSD; audio/I/O options; IP66/IK10 where exposed	PoE/PoE+ Ethernet; ONVIF Profile S/T/G/M as supported
Fixed outdoor bullet camera	Perimeter, façade, gate, loading/service areas	4–12 MP; motorized varifocal; adaptive IR; defog; heater where needed; IP66/67, IK10; surge protection	PoE/PoE+; fiber media converter for distance/high lightning risk
PTZ camera	Wide-area active tracking and operator response	Optical zoom typically 25–40×; presets/tours; auto-tracking optional; IR; privacy masks; wiper/heater for harsh areas	PoE++ or 24 VAC plus Ethernet/fiber; ONVIF PTZ
Multisensor / panoramic camera	Large halls, intersections, parking and open areas	180°/360° coverage; 8–32 MP aggregate; dewarping; individual streams; edge analytics	PoE+/PoE++; high-bandwidth uplink; VMS client/server dewarping verified
Fisheye camera	Compact 360° indoor overview	6–12 MP; ceiling/wall modes; multiple dewarped views; microSD; privacy masking	PoE; ONVIF; VMS-side or camera-side dewarping
Thermal camera	Perimeter detection, darkness/smoke-prone or temperature-event use	Radiometric only if measurement required; detection lens by range; analytics; optional visible channel	PoE; ONVIF/SDK; alarm metadata to VMS

Equipment	Purpose	Minimum technical detail / selection criteria	VMS connection
ANPR/LPR camera	Vehicle plate capture at controlled lanes	Fast shutter; IR tuned for plates; lane/angle limits; whitelist/blacklist; country library confirmed	PoE; metadata/API; loop/radar trigger optional
Special-environment camera	Marine, corrosive, hygienic, explosion-risk or high-temperature locations	316L stainless, anti-corrosion coating, pressurized/explosion-protected certification, housing/cooling as risk demands	Project-specific power/fiber; certified glands and junction boxes
Camera mount & housing	Correct field of view and environmental protection	Wall/ceiling/pole/parapet mounts; back box; pendant; sunshield; heater/blower; wiper/washer; safety tether	Mechanical attachment plus earth/bonding as required
IR / white-light illuminator	Improve low-light identification without overexposure	Beam angle matched to lens; wavelength 850/940 nm; photocell; power adjustment; IP-rated	PoE++ or local power; optional alarm/control input
Microphone / audio module	Audio verification where legal and approved	Omnidirectional/directional; gain and noise control; privacy/legal signage; balanced input where needed	Camera audio input, IP audio encoder or SIP gateway
IP speaker / horn	Talk-down, warning and automated messages	SIP/ONVIF audio where supported; ambient-noise control; stored clips; indoor/outdoor rating	PoE/PoE+; SIP/VMS plug-in; supervised network
Video encoder	Connect retained analog cameras to IP VMS	1/4/8/16 channels; H.264/H.265 as supported; PTZ serial; alarm I/O; edge storage	BNC input + Ethernet; ONVIF Profile S; RS-485 for legacy PTZ
Video decoder	Decode selected streams for monitor/video wall	Multi-stream hardware decode; layouts; 4K HDMI/DP output; low-latency mode	Ethernet from VMS; HDMI/DP to displays
Edge storage card	Recording continuity during network/server outage	Industrial high-endurance microSD; encrypted/signed file support; capacity by bitrate/outage duration	Installed in camera; edge-storage reconciliation with VMS

Connected equipment — events, identity & integration

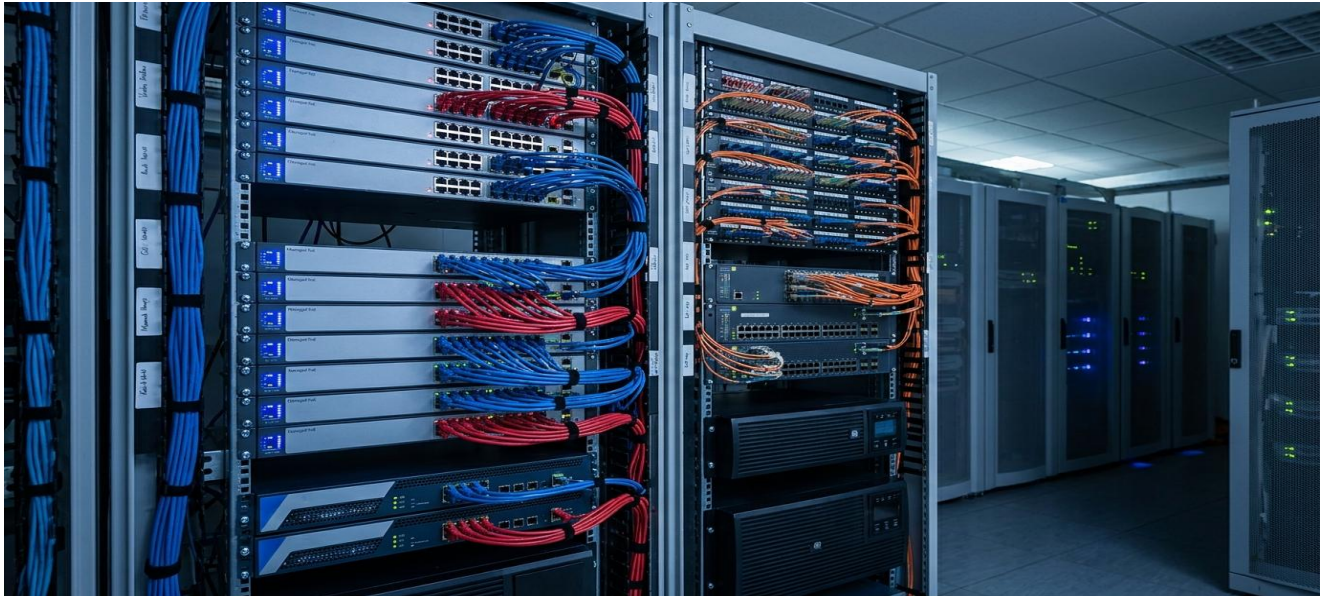


Integrated entrance security with video, access control and intercom.

Equipment / system	Purpose	Design requirement	Connection to VMS
IP video intercom / help point	Two-way voice/video and operator call handling	SIP; HD camera; call button; echo cancellation; relay output; vandal/weather rating	VMS/SIP integration; event opens associated camera and call workflow
Panic / duress button	Immediate security event initiation	Latching/non-latching as approved; supervised input; accessible mounting; tamper	Camera alarm input, network I/O module or intrusion panel integration
Network I/O module	Connect dry contacts and relays	Supervised digital inputs; relay outputs; secure API; PoE; local logic/watchdog	IP driver/API/Modbus gateway as approved

Equipment / system	Purpose	Design requirement	Connection to VMS
Door contact / request-to-exit	Provide door-state context	Installed and supervised by access/intrusion system; held/forced logic remains at source	Access-control event mapped to cameras and VMS rule
PIR / dual-tech detector	Intrusion detection context	Coverage and technology selected by environment; anti-mask where required	Intrusion-panel event or supervised network I/O
Fence / perimeter sensor	Early boundary event	Fiber, microwave, radar or cable sensor; zoned; environmental filtering	Zone event and map location linked to preset cameras
Radar / LiDAR detector	Wide-area tracking and classification	Range/FOV matched to scene; GPS/map calibration; tracks with confidence	Vendor plug-in/API; PTZ cueing subject to verification
Access-control system	Door, credential and identity events	Forced/held door, access denied/granted, anti-passback and alarm events	Certified VMS connector/API; identity display limited by policy
Intrusion alarm panel	Security zone events	Event and zone mapping; arm/disarm visibility if authorized	API/SDK, IP receiver or supervised dry contacts
Fire alarm system	Visual verification support only	Alarm zone/event import; no replacement of certified annunciation or control	Approved read-only gateway/contact; associated camera pop-up
BMS / PSIM platform	Shared alarms, maps and operating context	Bidirectional event exchange only where approved; clear ownership of commands	REST/API, OPC UA, MQTT middleware, webhooks or deep links
Parking / gate system	Vehicle events and evidence	Barrier state, ticket/credential event, lane direction, plate match	API/digital I/O; LPR metadata and transaction link
Elevator interface	Cab/lobby event context	Floor/door/emergency status if vendor supplies approved interface	Read-only event link; safety control remains independent
Active Directory / LDAP	Central user authentication	Groups, least privilege, account lifecycle; service-account controls	LDAPS/Kerberos/SAML/OID C depending on VMS capability
Email/SMS/notification gateway	Route approved alerts	Rate limiting; escalation; delivery logging; secure credentials	SMTP/API; avoid sensitive image delivery unless approved
SIEM / syslog platform	Cyber monitoring and audit consolidation	Admin logins, configuration changes, failures and security events	Syslog/CEF/API over protected management network

Connected equipment — network, power & timing

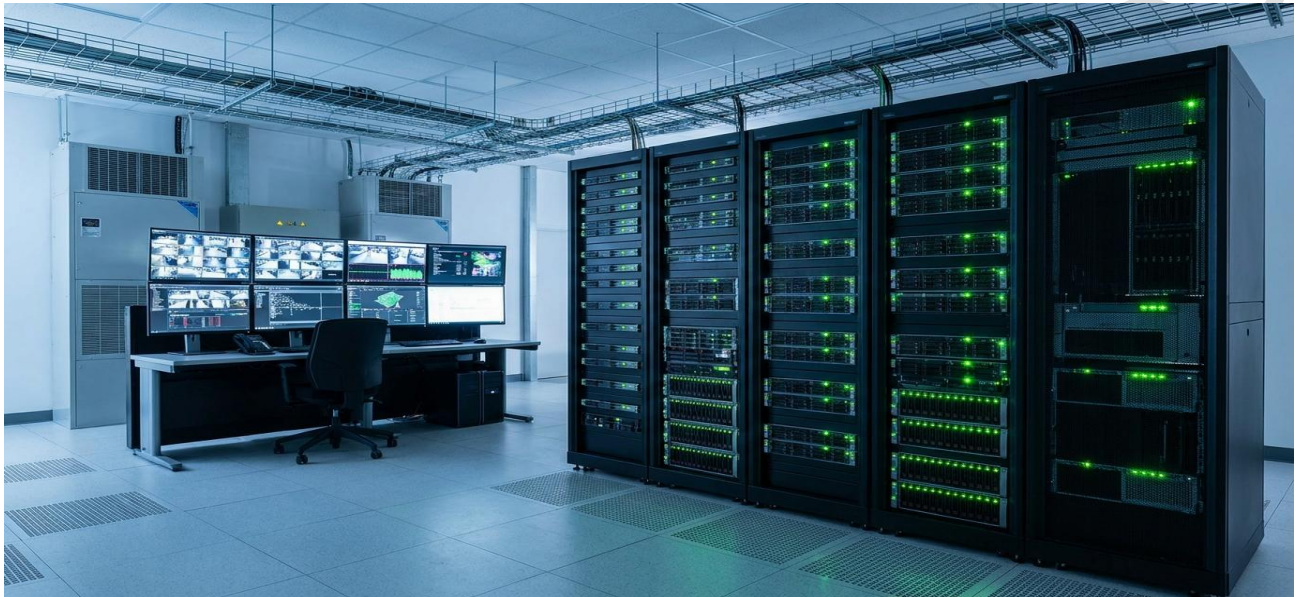


Managed switching, fiber, firewall and resilient rack infrastructure.

Equipment	Function	Detailed requirement	Connection
Managed PoE access switch	Power/connect cameras and field devices	1/2.5 Gb access as required; PoE+/PoE++; per-port budget; VLAN, QoS, LLDP, RSTP/MSTP, SNMPv3; dual uplinks; environmental rating	Camera VLAN to redundant/core uplinks
Layer-3 core/distribution switches	Aggregate buildings and route approved traffic	Stack/MLAG or redundant pair; 10/25/40 Gb as calculated; ACL; multicast controls; redundant PSU/fans	VMS servers, storage, clients and access-switch trunks
Fiber modules & ODF	Long-distance and resilient backbone	Single-mode/multimode selected by distance; matched SFP/SFP+; LC patching; labeled ODF; loss budget	Switch uplinks and remote field cabinets
Industrial field switch	Outdoor/plant/roadside camera aggregation	Extended temperature; DIN rail; redundant DC; surge immunity; IP-rated enclosure	Fiber/copper uplink to distribution network
Firewall / security gateway	Segmentation and controlled remote/integration access	HA pair where required; stateful rules; IPS; VPN; MFA integration; logged policy; throughput sized for video only when video traverses it	Between VMS zones, client IT, remote sites and external services
Router / SD-WAN appliance	Connect remote sites	Dual carrier optional; encrypted tunnels; QoS; path monitoring; bandwidth shaping	Management/event traffic and selected video streams
Wireless bridge / private radio	Hard-to-cable links	Licensed/unlicensed survey; capacity, latency, Fresnel clearance, encryption, failover and weatherproofing	Ethernet bridge; not preferred where fiber is practical
Cat6/Cat6A cabling	Horizontal IP device connection	Permanent link ≤90 m; shielded where EMC demands; certified test; LSZH where required	Camera/device to switch patch panel
Patch panels / cabinets / racks	Organized termination and serviceability	Labeled ports; cable management; ventilation; locks; grounding; spare capacity	Passive infrastructure
Camera power supply	Non-PoE or high-power devices	24 VAC/12/48 VDC as specified; fused outputs; monitored PSU; surge protection	Local device power; status may report to I/O/VMS
Online UPS	Maintain network, servers, storage and operators	Double-conversion; runtime by load; bypass; SNMP card; temperature/battery monitoring; generator compatibility	Power plus SNMP alarms to VMS/BMS/NMS
Rack PDU	Safe monitored power distribution	Metered/switched where required; outlet labeling; dual A/B feeds for dual-PSU equipment	Power monitoring via SNMP optional

Equipment	Function	Detailed requirement	Connection
Surge/lightning protection	Protect exposed copper and power circuits	Coordinated SPD, earth/bonding and local codes; fiber preferred across lightning zones	Installed at building/field boundaries
NTP time source	Consistent evidential timestamps	Redundant NTP; authenticated where supported; GPS/PTP source if required; timezone/DST policy	All cameras, servers, storage, switches and clients

Connected equipment — compute, storage & control room



VMS servers, recording storage and operator infrastructure.

Equipment	Role	Full design detail	Connection
VMS management server	System database, configuration, users, device registry and rules	Enterprise server/VM; redundant PSU/NIC; backed-up database; TLS certificates; primary/standby if critical	Management VLAN; directory, clients, recording and integration services
Recording server / NVR	Ingest and record camera streams	CPU/NIC/disk throughput validated for total bitrate; hardware health; RAID/HBA design; failover; no oversubscription	Camera VLAN + storage/management networks
Failover recording server	Automatic/controlled takeover	Capacity for defined failure set; synchronized configuration; tested recovery and return-to-primary	Same protected recording and management networks
Analytics / GPU server	Run central AI/video analytics	Supported GPU; stream/resolution/FPS licensing; queue management; model version control and privacy policy	Receives selected streams/metadata; returns events and classifications
Metadata / search server	Index events and object data	Fast storage; retention aligned to investigation needs; access controls	VMS management and analytics services
Database server	Large-scale configuration/event database when separated	Vendor-supported DB version; HA/backup; maintenance plans; least-privileged service account	Protected server/management VLAN
RAID storage array	Primary high-availability video storage	Enterprise disks; RAID 6/60 typical by design; hot spare; dual controller where needed; rebuild risk considered	DAS, iSCSI, FC or vendor-supported architecture

Equipment	Role	Full design detail	Connection
NAS / SAN	Shared or centralized storage	Throughput/IOPS proven for sustained sequential write and playback; redundant links/controllers	Dedicated storage VLAN/fabric; supported by VMS vendor
Archive / backup appliance	Long-term evidence or configuration backup	Immutable/WORM option if required; encryption; offline/off-site copy; retention and deletion policy	Scheduled VMS archive/export and backup network
Operator workstation	Live view, playback, investigation and export	Business/workstation CPU; supported GPU; 16–32+ GB RAM; dual/quad monitor outputs; hardened OS	Client VLAN to VMS services; USB use controlled
Investigation workstation	High-resolution review and evidence preparation	Higher CPU/GPU; calibrated display; encrypted export path; report tools	Restricted role and evidence network/workflow
Video wall controller	Display multiple layouts and alarms	Redundant PSU/NIC optional; sufficient decode capacity; synchronized outputs; operator control	VMS client/decoder network to display wall
Security monitors / video wall displays	Continuous control-room visualization	Commercial 24/7 panels; narrow bezel as required; brightness/uniformity; burn-in management	HDMI/DP from clients/controller/decoders
PTZ joystick / keypad	Ergonomic camera control	USB/IP; programmable keys; role-controlled priority; durable industrial unit	Operator workstation or VMS network
KVM / console	Secure server maintenance	Rack console or IP KVM with access logging and restricted management	Server rack and out-of-band management
Evidence printer / media station	Incident reports and approved evidence export	Controlled printer; encrypted removable-media process; malware scanning; barcode/seal process if required	Restricted evidence workstation
Mobile/tablet client	Authorized field response	MDM-managed device; VPN/MFA; remote wipe; no local download unless approved	Secure remote access gateway to VMS

VMS software, licenses & functions



Professional operator interface for live monitoring, alarms and investigation.

Software / entitlement	Required capability
Core VMS license	Device/channel registration, live/recorded video, maps, alarms, rules, users, audit and health monitoring
Camera/device channel license	One license per connected video/audio/encoder channel unless enterprise agreement states otherwise
Failover / redundancy license	Management and/or recording failover; confirm automatic takeover limits and recovery behavior
Mobile/web client license	Secure browser and mobile access; validate concurrent-user limits
Video wall license	Shared view control, layouts, alarm takeover and display management
Analytics license	Per-camera/server feature licensing for intrusion, loitering, line crossing, object, queue, occupancy, PPE, smoke/flame concepts or custom AI
LPR/ANPR license	Plate recognition engine, country library, lists, search and parking/transaction integration
Access-control/integration connector	Certified plug-in/API connector plus any middleware and maintenance entitlement
Evidence management module	Case folders, bookmarks, redaction, watermark/signature, audit and controlled sharing
Health monitoring module	Camera/stream/recording/storage/network alarms, dashboards and SLA reports
Map / GIS module	Floor/site maps, camera icons, fields of view, alarm navigation and geospatial layers
Software support & updates	Vendor support, security patches, version upgrades and compatibility assurance for an agreed term

Core operator functions

- Live layouts, sequences, maps, PTZ priority, digital zoom and privacy masking.
- Recorded playback with synchronized multi-camera timeline, thumbnails, bookmarks and incident notes.
- Smart search by time, zone, motion, object class, color/direction or plate where licensed and legally approved.
- Alarm queue with priority, ownership, acknowledgement, escalation, comments and SOP guidance.
- Export with player or standard format, checksum/digital signature where supported, watermark and full audit trail.
- System-health dashboard covering last video, recording status, bitrate, storage days, clock drift, camera tamper and component status.

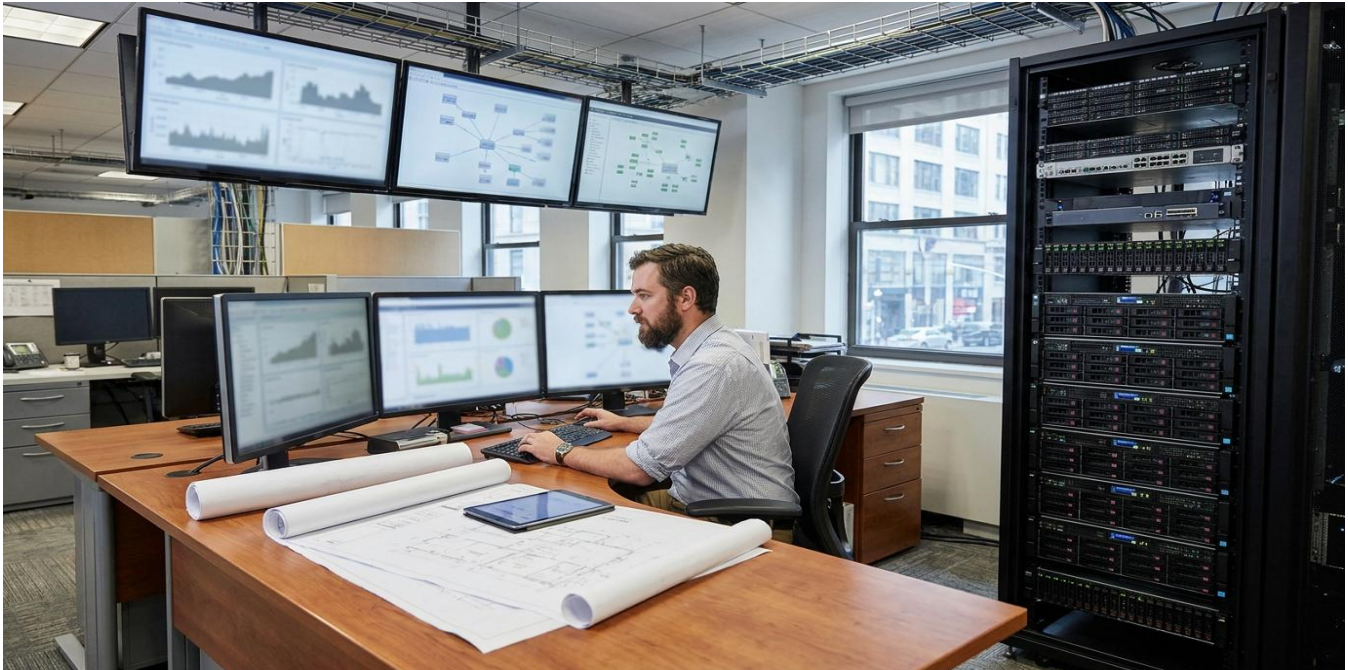
Analytics catalogue and guardrails



AI-assisted detection with mandatory operator verification.

Use case	Typical analytics	Design guardrail
Perimeter	Line crossing, intrusion zone, loitering, wrong-way travel, radar cueing	Tune perspective, target size, dwell time and environmental filters; validate day/night and seasonal conditions.
Building interior	People counting, occupancy, queue, abandoned/removed object, restricted-zone entry	Do not use safety-critical counts without an approved secondary method; document accuracy and exclusions.
Traffic/parking	Vehicle class, stopped vehicle, direction, LPR/ANPR	Control angle, shutter, speed, lighting and legal retention of plate data.
Operations/safety	PPE concept, fall/person-down concept, smoke/flame visual alert	Treat AI as decision support; human verification and certified primary systems remain mandatory.
Investigation	Appearance/object search, face search only if lawful and approved	Complete privacy impact assessment, authorization, bias/accuracy testing and strict retention/access controls.

Sizing basis — bandwidth, storage & retention



Engineering workflow for camera bandwidth, recording and storage capacity.

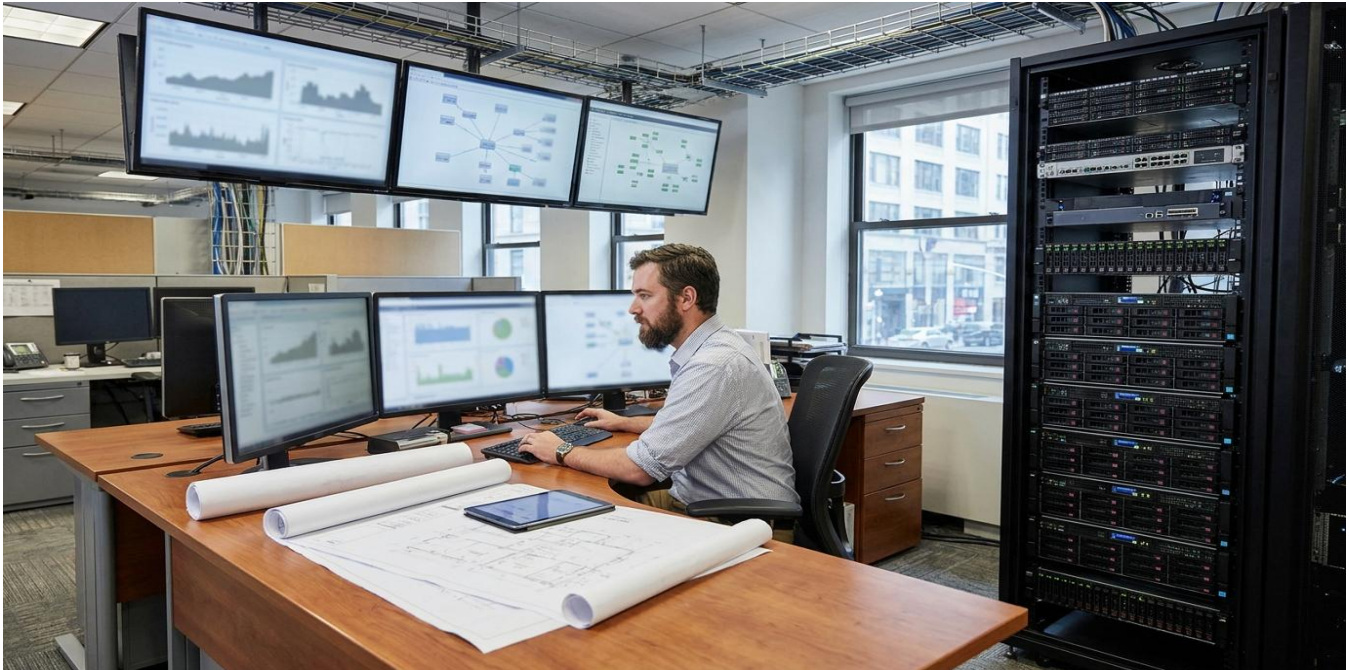
Every camera must have a documented scene objective and operational profile. Storage is calculated from measured/approved average bitrate—not only the camera maximum—and includes overhead, RAID design, failover reserve, rebuild margin and future growth.

Quick engineering formula

Raw storage (TB) $\approx$ total average bitrate (Mb/s) $\times$ 10.8 $\times$ retention days $\div$ 1,000. Apply engineering factors for recording schedule, codec behavior, metadata/audio, filesystem overhead, RAID usable capacity, failover, export reserve and growth. The final vendor sizing tool and performance test remain authoritative.

Input	Project decision required
Camera count by type	Resolution, lens/FOV, identification objective, FPS, codec, WDR, audio and analytics.
Recording mode	Continuous, motion/event, dual stream, pre/post alarm and edge recording duration.
Retention	Days by camera/security class; incident/legal hold and archive rules.
Playback load	Simultaneous users, cameras per user, export workload and investigation peaks.
Availability	Permitted outage, recording failover set, server/storage redundancy and disaster recovery.
Growth	Recommended spare ports, rack/power/cooling, storage and license margin agreed with client.

Illustrative calculation — not a quotation



Storage and network sizing must be validated against the final camera profiles.

Parameter	Illustrative value
100 cameras × 4 Mb/s average	400 Mb/s aggregate recording bitrate
Raw daily video	≈ 4.32 TB/day before engineering factors
30-day raw requirement	≈ 129.6 TB before RAID/overhead/reserve/growth
Design action	Validate actual bitrates by scene, codec, FPS and analytics; then select usable storage and write throughput with vendor approval.

Camera selection method

- Define the surveillance objective: detect, observe, recognize or identify—then select pixel density and lens accordingly.
- Confirm mounting height, target distance, lighting, backlight, motion speed, weather, vandalism and privacy zones.
- Produce a camera schedule with unique ID, location, scene purpose, model, lens, mount, IP address, switch/port, power class, recording profile and retention class.
- Validate representative scenes through a proof of concept before mass procurement.

Cybersecurity, privacy & evidence integrity



Protected VMS infrastructure with monitored, segmented network services.

Control domain	Required controls
Identity	Named accounts, RBAC, least privilege, MFA for remote/admin access, AD/LDAP integration, periodic access review and controlled service accounts.
Device hardening	Change defaults; disable unused services/discovery; signed firmware where supported; HTTPS/TLS; certificates; secure SNMP; lock local reset/SD access where practical.
Network segmentation	Separate camera, server/storage, client and management zones; deny-by-default ACL/firewall rules; dedicated admin path; controlled internet access.
Patch & vulnerability	Asset inventory, supported firmware/software matrix, risk-based patching, maintenance window, backup and rollback plan.
Logging & monitoring	Audit log retention; failed login/configuration alarms; syslog/SIEM export; clock-drift monitoring; alert ownership.
Remote support	Client-approved VPN, MFA, time-limited authorization, session logging and no unmanaged remote desktop exposure.
Privacy	Purpose limitation, camera signage, privacy masks, audio authorization, restricted sensitive areas, data minimization and approved retention/deletion.
Evidence	Synchronized time, chain-of-custody form, role-controlled export, checksum/signature, tamper-evident storage and documented legal hold.
Backup & recovery	Encrypted configuration/database backups, offline/off-site copy, restoration test and documented recovery objectives.

Recommended logical zones

Zone	Permitted traffic concept
Camera/edge zone	Cameras to approved recording/management/NTP/DNS destinations only; no direct user or internet access.
Server/storage zone	Recording, management, database and storage flows restricted to required ports; dedicated storage network if used.
Client/control-room zone	Operator clients to VMS services; no direct camera administration for ordinary operators.
Management zone	Privileged jump host, monitoring, backup and device administration; MFA and full audit.
Integration/DMZ zone	API gateway/middleware for BMS, access, remote sites or cloud service; rate-limited and monitored.

Control-room design & operating concept



Ergonomic security control room with video wall and PTZ operator controls.

Element	Design requirement
Operator positions	Ergonomic desk, sightlines, task and ambient lighting, cable management, acoustic control and 24/7-rated furniture where applicable.
Display layout	Primary alarm/incident display, supporting live views, maps and health dashboard; avoid excessive simultaneous streams.
Alarm handling	Priority classes, audible/visual indication, ownership, acknowledgement target, escalation timer and written SOP.
PTZ governance	Role priority, lock/takeover rules, preset naming, privacy areas and audit of manual control.
Evidence process	Incident number, bookmark, export authorization, media labeling, checksum, handover receipt and retention/legal hold.
Business continuity	Spare operator client, failover layouts, local emergency contact list, UPS runtime and degraded-mode procedure.

Typical intelligent event sequence

- 1. A perimeter analytic, access-denied event or panic button creates a time-stamped alarm.
- 2. The VMS presents the alarm camera, pre-event buffer, nearby cameras, map and source-system details.
- 3. The operator verifies the event, follows the on-screen SOP and may select a PTZ preset or initiate approved talk-down.
- 4. The platform records acknowledgement, actions, comments, escalation and linked system events.
- 5. The incident is bookmarked/exported under controlled permissions; a case record and performance metrics are retained.

Naming convention example

SITE-BUILDING-FLOOR-ZONE-TYPE-NUMBER → BEI-HQ-L02-EAST-DOME-014. Apply the same ID to drawings, VMS, switch port, patch panel, cable label, camera schedule and maintenance records.

Testing, commissioning & handover



Field testing, camera adjustment and integrated VMS commissioning.

Stage	Acceptance evidence
Design review	Approved camera plan, risk coverage, lens/FOV, network, storage, cybersecurity, integration matrix and responsibility schedule.
Installation inspection	Mounting, field of view, weather sealing, labels, cable test, grounding, cabinet/rack condition and asset serials.
Point-to-point test	Every stream, audio path, I/O, preset, event, map icon, clock, recording profile and health alarm verified.
Image-quality test	Day/night scenes; backlight; target motion; focus; IR reflection; privacy masks; recognition/identification objective documented.
Recording/retrieval test	Continuous/event recording, edge recovery, playback, synchronized cameras, export, signature/checksum and retention behavior.
Resilience test	Server/service restart, failed recorder, uplink loss, storage alarm, UPS event, failover and return-to-normal procedures.
Cybersecurity test	Accounts/roles, MFA, disabled defaults, ports/services, certificates, firmware baseline, logging and backup/restore.
Integration test	Each source event, alarm priority, camera association, SOP, acknowledgement and round-trip status where approved.

Stage	Acceptance evidence
Performance test	Sustained ingest, simultaneous clients/playback/export, storage utilization, CPU/GPU/NIC and packet-loss checks.
Training & acceptance	Operator, investigator and administrator training; scenario drills; punch list; client sign-off.

Handover package

- Approved as-built camera layouts, topology, rack elevations, IP/VLAN plan and cable/port schedules.
- Camera/device register, warranty details, licenses, firmware/software baseline and approved configuration backups.
- VMS administration manual, operator SOPs, alarm matrix, integration matrix and evidence-export procedure.
- Storage/bandwidth calculations, test sheets, image-quality snapshots, failover records and cybersecurity checklist.
- Training attendance, spare-parts list, preventive-maintenance plan, escalation contacts and service-level agreement.

Preventive maintenance & lifecycle support



Preventive camera maintenance and field system-health inspection.

Frequency	Typical tasks
Continuous / daily	Automated health alarms; recording gaps; camera offline/tamper; storage capacity; server/UPS/switch condition; operator shift review.
Monthly	Sample playback/export; lens/housing inspection; event-rule review; failed-login and audit review; backup completion.
Quarterly	Clean exposed cameras; verify focus/IR/night images; UPS and cabinet checks; integration event sampling; capacity/growth report.
Semiannual	Firmware/software risk review; failover test; restore test; user/role recertification; analytics retuning for scene changes.
Annual	Full representative acceptance retest, storage/retention verification, cybersecurity assessment, asset/warranty review and lifecycle plan.

Recommended spares

- At least one spare of each critical camera family or an agreed percentage by type.
- Spare SFPs, PoE switch or field switch for critical sites, power supplies, disks matched to array policy, patch cords and surge devices.
- Preconfigured replacement procedure with license transfer, firmware baseline, naming/IP template and restoration test.

Scorpions Services delivery scope

Project stage	Scorpions Services role
Survey & risk assessment	Stakeholder workshop, scene objectives, existing-system audit, network/power survey and integration discovery.
Engineering	Camera plan, coverage/FOV, equipment schedule, bandwidth/storage, network, rack, power and cybersecurity design.
Supply & installation	Approved equipment, cabling coordination, mounting, racks, servers, storage, operator room and labeling.
Programming & integration	VMS configuration, users, maps, alarms, analytics, SOPs, dashboards and third-party interfaces.
Commissioning	Point-to-point, scenario, image-quality, recording, resilience, cybersecurity and integrated-system testing.
Training & handover	Role-based training, as-builts, backups, manuals, test records, spares and acceptance.
After-sales support	Preventive/corrective maintenance, remote support, patching, health reporting, upgrades and lifecycle planning.

Project-specific information required



Joint site survey for camera locations, coverage and network requirements.

- Site plans, floor plans, risk assessment, operational hours, security concept and priority zones.
- Camera counts/locations or permission to conduct a joint camera-location survey.
- Required retention by camera class, legal/privacy rules, audio policy and evidence workflow.
- Existing camera makes/models, licenses, cabling, network switches, fiber, racks, servers, storage and UPS.

- Client IT standards: IP/VLAN, directory, certificates, NTP, remote access, monitoring, backup, patching and cybersecurity approvals.
- Connected-system details: access control, intrusion, fire, BMS/PSIM, intercom, parking, gates, elevators and notification systems.
- Availability targets, failover scope, disaster recovery, growth horizon and maintenance/service-level expectations.

Quantity take-off worksheet

#	Item	Qty	Unit	Remarks
1	Indoor fixed dome cameras	TBC	TBC	Survey / design confirmation required
2	Outdoor fixed bullet cameras	TBC	TBC	Survey / design confirmation required
3	PTZ cameras	TBC	TBC	Survey / design confirmation required
4	Panoramic/multisensor cameras	TBC	TBC	Survey / design confirmation required
5	Thermal cameras	TBC	TBC	Survey / design confirmation required
6	ANPR/LPR cameras	TBC	TBC	Survey / design confirmation required
7	Special-environment cameras	TBC	TBC	Survey / design confirmation required
8	Intercom/help points	TBC	TBC	Survey / design confirmation required
9	IP speakers/microphones	TBC	TBC	Survey / design confirmation required
10	Encoders/decoders	TBC	TBC	Survey / design confirmation required
11	Managed PoE access switches	TBC	TBC	Survey / design confirmation required
12	Core/distribution switches	TBC	TBC	Survey / design confirmation required
13	Fiber modules/ODF	TBC	TBC	Survey / design confirmation required
14	Firewalls/routers	TBC	TBC	Survey / design confirmation required
15	Racks/cabinets/patch panels	TBC	TBC	Survey / design confirmation required
16	UPS/PDU/surge protection	TBC	TBC	Survey / design confirmation required
17	VMS management servers	TBC	TBC	Survey / design confirmation required
18	Recording/failover servers	TBC	TBC	Survey / design confirmation required
19	Analytics/GPU servers	TBC	TBC	Survey / design confirmation required
20	Primary usable storage (TB)	TBC	TBC	Survey / design confirmation required
21	Archive/backup storage (TB)	TBC	TBC	Survey / design confirmation required
22	Operator/investigation workstations	TBC	TBC	Survey / design confirmation required
23	Control-room monitors/video wall	TBC	TBC	Survey / design confirmation required
24	Software channel/integration/analytics licenses	TBC	TBC	Survey / design confirmation required

Assumptions, exclusions & approval notes



Stakeholder review of project boundaries, design and approvals.

- This concept is brand-neutral and does not nominate exact makes or models. Products must be selected from client/consultant-approved manufacturers and verified on the VMS compatibility list.
- Camera performance depends on scene geometry, lighting, mounting and configuration. Datasheet resolution alone does not guarantee identification quality.
- Analytics accuracy is probabilistic and environment-dependent. It must be validated for each scene and cannot replace certified life-safety or human decision-making.
- Network switching, fiber paths, electrical circuits, cooling, rack space and civil works are included only when explicitly stated in the commercial scope.
- Third-party integrations may require vendor licenses, API access, gateways, engineering support, certificates or maintenance agreements.
- All privacy, audio recording, biometric/face-processing, plate-data and retention requirements must be approved by the client and relevant authority before activation.
- Final design must comply with applicable local law, consultant specifications, authority requirements and adopted standards, with project-specific testing and documentation.

Recommended next step

Conduct a joint technical workshop and site survey. Scorpions Services will then issue the project camera schedule, coverage drawings, integration matrix, network topology, storage/bandwidth calculation, cybersecurity plan, bill of quantities and detailed technical/commercial offer.

Contact



Scorpions Services remote support and lifecycle assistance.