LYT-X

LYT-X is the core system of the security solution, offering an effective surveillance solution: Smart Lamp Pole Solution and Converged Security & Information Management Solution (CSIM). The software solution enables you to manage and monitor security-related events, data and alerts from a single user interface. LYT-X ensures safer and smarter cities through transforming the ordinary security system into simplified and effective security management.

Doc 4.0

Single monitoring
Single UI / Monitor with standard library of integrations

Automated SOP
Improves response time and resolves incidents faster

Minimizing risk
Identifies true or false alarm with accurate reporting results

Cost effective
Optimise operation costs for automatic detection and resolution with SOP

Facilitates interoperability
Leverages and extends the existing investment

Simplifies situation management
Automated dashboard & standard reports to manage multiple existing systems

Reduces response time
Respond to the incident faster and efficiently

Protects business assets
Able to monitor and track your business assets to prevent risk

The CSIM concept

CSIM software is typically used to collect information from different existing disparate security systems and information systems — video, access control, sensors, video analytics, networks, building systems, cyber — and collate it in one single graphical user interface. A CSIM software system provides five key capabilities to empower personnel to accurately identify and proactively resolve situations.

Connect

Connect physical security system to a single user interface with protocols

Aware

Aware of every alarm event by connecting all network devices into our system

Identify

Identify true or false alarm events with our incident management

Protect

Protect your assets and business with situation awareness and automated SOP

Predict

Predict your assets and resources with our report and dashboard module

Key Features of CSIM

Real-time Data Correlation and Analysis: CSIM platforms are capable of processing vast amounts of data from diverse sources in real-time. This capability ensures that organizations have the most current information at their fingertips, enabling quick decision-making in critical situations.

Comprehensive Situation Management: CSIM excels in providing comprehensive situational awareness. By integrating data from various systems such as video surveillance, access control and cybersecurity networks, it creates a cohesive picture of security-related events.

Enhanced Situational Awareness: With its ability to integrate and visualize data from multiple sources, CSIM provides a global view of security situations. This includes geospatial mapping of incidents and resources, which is crucial for large-scale operations.

Dynamic Response and Resolution Guidance: CSIM platforms not only identify and alert on potential security incidents but also guide operators through the response process. This includes automated workflows and standard operating procedures to ensure effective and consistent handling of incidents.

Scalability and Flexibility: Designed to cater to organizations of various sizes and complexities, CSIM systems are highly scalable. They can adapt to a range of operational needs, from single-site installations to global enterprise networks.

Compliance and Reporting: In addition to operational functionalities, CSIM aids in compliance with various regulatory standards by providing robust reporting and auditing tools. This feature is essential for organizations that need to adhere to strict security regulations.

Integration with Legacy Systems: A significant advantage of CSIM is its ability to integrate with existing security and information systems, protecting prior investments and extending their functionality.

Mobile Accessibility and Remote Management: Reflecting the needs of modern organizations, CSIM solutions often offer mobile applications and remote access capabilities, allowing decision-makers and security personnel to stay informed and react promptly, irrespective of their location.

Platform Architecture

Existing subsystems keep running as they are. LYT-X normalises their events into a single model, applies rules and standard operating procedures, and presents one operating picture to the control room, the field and management.

CONNECTED SUBSYSTEMS

- CCTV, VMS, DVR / NVR
- Access control & IAM
- Fire, intrusion, sensors
- Video analytics & AI
- Network & IT infrastructure
- Cybersecurity tools
- Building management (BMS)
- GIS, GPS & mobile assets

LYT-X CORE PLATFORM

- **Protocol & API connectors**
- **Event normalisation & correlation**
- **Rule engine & alarm prioritisation**
- **Incident management & SOP**
- **E-Map, GIS & virtual matrix**
- **Logging, reporting & analytics**
- **User management & audit trail**
- **High availability & redundancy**

OPERATIONS

- Control room workstations
- Video wall & decoders
- Guided SOP response
- Multi-agency coordination
- Mobile & remote access
- Management dashboards
- Compliance & audit reporting
- Field team notification

Scalable and Modular: Small to large-scale deployments across multi-location, multi-server and multi-system environments.

Open by Design: Web API (JSON, SOAP, RESTful), MQTT, SNMP, SQL, OPC, BACnet, Modbus, POP3, Logfile, SIP, SFTP and Serial Port (RS232, RS485), plus SDKs for custom integration.

Continuous Operation: Failover capability, backup systems and regular data backup for disaster recovery.

HOW AN EVENT TRAVELS THROUGH THE PLATFORM

01
Collect
Devices, analytics and IT systems report events over their native protocol or API.

02
Normalise
Every event is converted to one common model and enriched with location and device context.

03
Decide
Rules correlate related events, filter false alarms and set the priority of the incident.

04
Act
The SOP opens with map, video and contacts; every action is logged for reporting and audit.

SINGLE SITE

One server, one control room, local devices and recorders.

CAMPUS / MULTI-SITE

Multiple sites and servers under one operating picture, with local autonomy retained.

CITY-WIDE

Distributed command centres, multi-agency coordination and redundant core services.

Connect

CSIM, or Converged Security Information Management, is an evolution of PSIM (Physical Security Information Management) systems, integrating not just physical security systems but also cyber and IT security elements. This convergence provides a more holistic approach to organizational security. Here is a list of key integration features for CSIM systems:

Cybersecurity Solutions Integration: Integrating with network security tools like firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and antivirus software to monitor and respond to cyber threats in real-time.

IT Infrastructure Monitoring: Integration with IT infrastructure management tools for monitoring network performance, server health and data storage status.

Physical Security Systems: Similar to PSIM, CSIM integrates with physical security systems such as CCTV, access control, fire alarm, intrusion, visitor, sensors and decoder.

Identity and Access Management (IAM): Integration with IAM systems to ensure that only authorized individuals have access to physical and digital assets.

Building Management Systems (BMS): Including HVAC, lighting and power systems to monitor and manage the physical environment and ensure operational efficiency and safety.

Network Management Systems: Integration with systems that monitor and manage network components like routers, switches and hubs.

Incident Response and Management Systems: Systems that coordinate and manage responses to security incidents, whether physical or digital.

Data Analytics and Business Intelligence Tools: Utilizing advanced analytics tools for predictive analysis, threat detection and decision-making support.

Enterprise Resource Planning (ERP) Systems: Integrating with ERP systems to align security management with broader business processes and objectives.

Communication Systems: Including email, instant messaging and VoIP systems, to ensure seamless communication during security incidents.

Emergency and Public Safety Systems: Integration with external systems like public emergency alerts, weather monitoring and emergency services communication networks.

Compliance and Governance Tools: Tools that help in maintaining compliance with various regulatory standards and corporate governance policies.

Cloud Services and Infrastructure: Integrating with cloud-based services and infrastructure for data storage, processing and analysis.

Mobile Device Management (MDM): Systems to manage and secure mobile devices that access organizational networks and data.

GIS and GPS Technologies: For location tracking and mapping, especially important for organizations with mobile assets or personnel.

Aware

The Aware feature is the cornerstone of any effective security system, providing the foundational capability for comprehensive situational understanding. It is the process of continuously and automatically collecting data from all integrated security and information systems, ensuring that personnel are instantly informed of every event and the real-time status of all devices.

Real-time Data Aggregation: Continuously collects vast amounts of data from all connected sources, including video, access control and IT systems.

Centralized Connectivity: Connects all disparate security systems and network devices into a single, unified graphical user interface.

Comprehensive Device Monitoring: Provides real-time status updates for every network device within the system, detecting any malfunctions or disconnections.

Event and Alarm Consolidation: Gathers all alarm events and alerts from various devices into a single, easy-to-manage dashboard.

Enhanced Situational Visibility: Integrates and visualizes data from multiple sources to create a complete picture of the security landscape.

Integrated System Health Check: Monitors the operational health of all integrated systems, alerting operators to maintenance needs or system failures.

Geospatial Mapping Integration: Displays the location of incidents, devices and personnel on an interactive map for better spatial awareness.

Auditable Event Logging: Creates a detailed, searchable log of all events and activities, which is essential for post-incident analysis and compliance.

Cross-System Correlation: Links events from different systems (for example, an access control breach with corresponding video footage) to provide a more detailed context.

Customizable Alerting: Allows users to set specific rules and thresholds for alerts, ensuring that notifications are relevant to their role.

Holistic Environmental Awareness: Combines data from physical security, IT infrastructure and environmental sensors to provide a truly comprehensive overview.

COLLECTED CONTINUOUSLY

Alarm and access events, device and link status, analytics metadata, sensor readings, server and network health.

PRESENTED AS

One unified event list, the live E-Map, a device health panel and a searchable log — in a single user interface.

RETAINED FOR

Post-incident investigation, compliance evidence and trend analysis, under the configured data retention policy.

WHY IT MATTERS

Awareness is what makes every later step possible: an event the system never received cannot be correlated, escalated or reported on. Continuous collection across every connected system is therefore the foundation of the incident record, the audit trail and the dashboard.

Identity

Rule-based analysis in Converged Security Information Management (CSIM) is a crucial feature. It involves setting predefined rules or conditions to trigger specific actions or alerts when those conditions are met. Here is a list of typical rule analysis features in CSIM systems:

Event-Triggered Alerts: Setting rules to trigger alerts when specific events occur, such as unauthorized access, motion detected in restricted areas or system failures.

Conditional Responses: Defining specific responses based on the type and severity of an incident, like locking down an area after a security breach is detected.

Access Control Rules: Implementing rules for access control systems, like restricting access to certain areas during specific times or based on user credentials.

Alarm Prioritization: Setting rules to prioritize alarms based on their type, location or potential impact, ensuring that critical alarms are addressed first.

Automated System Actions: Rules that automatically initiate system actions, such as turning on lights or cameras in response to specific triggers.

Correlation Rules: Creating rules to correlate data from different systems, like linking access control logs with video footage for comprehensive incident analysis.

Maintenance Alerts: Setting up rules for system maintenance alerts, like notifying when cameras are offline or when sensors need calibration.

Escalation Procedures: Defining rules for escalating incidents to higher authorities or external agencies based on predefined criteria.

Time-Based Rules: Implementing rules that are activated during certain times of the day or week, such as adjusting surveillance levels during non-working hours.

Geofencing: Rules that trigger alerts or actions when an asset or person enters or leaves a defined geographical area.

Data Retention Policies: Setting rules for how long data should be stored based on legal or organizational requirements.

Environmental Monitoring Rules: Rules for monitoring environmental conditions, like temperature or smoke levels, and triggering alerts or actions when thresholds are exceeded.

Network Monitoring Rules: Implementing rules for monitoring network traffic and activities, alerting in case of unusual patterns that might indicate cyber threats.

User Activity Monitoring: Rules for monitoring user activities, especially in sensitive or critical systems, to detect potential insider threats or policy violations.

Compliance Enforcement: Rules designed to ensure that operations stay within regulatory and policy guidelines, triggering alerts or actions when compliance is breached.

Protect

Protect is a critical component of Converged Security Information Management (CSIM) systems. It involves a set of features designed to handle and resolve various incidents and emergencies effectively. Here is a detailed list of Protect features typically found in CSIM systems:

Real-Time Monitoring and Alerting: Continuous monitoring of all integrated systems and sensors to detect and alert on incidents in real-time, ensuring immediate awareness.

Incident Detection and Classification: Automatically detecting and classifying incidents based on predefined criteria to determine their nature and severity.

Automated Response Protocols: Activating predefined response actions or protocols based on the type and severity of the incident, ensuring a quick and appropriate response.

Resource Allocation and Dispatch: Efficient management and deployment of resources, including personnel, vehicles and equipment, to handle the situation effectively.

Communication and Collaboration: Facilitating seamless communication among internal security teams, external agencies and stakeholders for coordinated response efforts.

Geospatial Mapping and Tracking: Using GIS (Geographical Information System) to provide real-time mapping and tracking of incidents, resources and personnel.

Decision Support Systems: Offering data-driven insights and analytics to support decision-making during complex and evolving situations.

Standard Operating Procedure (SOP) Activation: Guiding responders through pre-defined SOPs tailored to specific types of incidents to ensure compliance and effectiveness.

Integration with Public Safety Systems: Connecting with external public safety systems, like fire, police and medical services, for a comprehensive response.

Emergency Notification Systems: Implementing systems to quickly notify and guide occupants in case of emergencies like evacuations or lockdowns.

Multi-agency Coordination: Facilitating coordination and information sharing with multiple agencies for situations that require a joint response.

Post-Incident Analysis and Reporting: Conducting thorough analysis post-incident to assess response effectiveness, gather lessons learned and improve future responses.

Live Video Feeds and Surveillance: Providing live video feeds from surveillance cameras for real-time visual assessment and monitoring of incidents.

Environmental Monitoring: Integrating environmental sensors to detect and respond to hazards like smoke, gas leaks or extreme weather conditions.

Crowd Management and Analysis: Tools for monitoring and managing large crowds, especially in public spaces, to prevent or respond to safety concerns.

Incident Response Flow

Every alarm becomes a tracked incident record. The system displays incident alert progression through four statuses, so operators always see where each case stands and nothing is closed without a documented resolution.

STATUS 01

ToDo

New events, prioritized by time and severity, waiting to be picked up.

STATUS 02

Doing

Incidents actively being resolved under the SOP for that incident type.

STATUS 03

Block

Held while awaiting external assistance from another agency or team.

STATUS 04

Done

Completed and documented, with the summary form and evidence retained.

Detect — devices, sensors and analytics raise an event

Correlate — rules link it to video, access and sensor data

Respond — SOP guides the operator step by step

Review — reports and audit trails close the loop

Automated Incident Creation: A new incident record is generated whenever an alarm or event is triggered, ensuring no critical event is missed.

Classification and Prioritization: Incidents are classified against predefined criteria and assigned a priority level, so operators focus on the most critical events first.

Guided Response: Predefined SOPs provide a form to confirm the incident as genuine or false, contact information for coordination, and a summary form to document the resolution.

Evidence on Screen: The incident name, location and details appear on the E-Map while live or playback video from the nearest camera is shown automatically.

WHAT THE OPERATOR GETS WHEN AN INCIDENT OPENS

Location on the E-Map

The incident and the devices around it, with alarm symbols and camera fields of view.

Video from the nearest camera

Live and playback at the time of the event, with export for evidence.

The SOP for that incident type

Step-by-step actions, true or false alarm confirmation and the resolution form.

Related events

Access records, sensor readings and system events correlated to the same case.

Contacts and channels

Who to notify and how — email, SMS, mobile app, intercom or public address.

A complete audit trail

Every action, timestamp and operator recorded for reporting and investigation.

ESCALATION

When an incident exceeds a defined threshold, time limit or severity, it is escalated automatically to higher authorities or external agencies, and coordination with fire, police or medical services continues inside the same incident record.

Predict

In Converged Security Information Management (CSIM) systems, features related to prediction, reporting and dashboards are essential for proactive security management, analysis and decision-making. Here is a list of these feature functions:

Predictive Feature

Threat Prediction and Analysis: Utilizing advanced algorithms and historical data to predict potential security threats and vulnerabilities.

Behavioral Analysis and Anomaly Detection: Analyzing patterns of behavior to identify anomalies that could indicate security risks.

Predictive Maintenance for Equipment: Forecasting potential maintenance issues in security equipment to prevent failures.

Risk Assessment Tools: Evaluating potential risks and their impacts on organizational security.

Trend Analysis: Analyzing long-term data trends to anticipate future security needs or challenges.

Reporting Features

Customizable Reports: Generating tailored reports to meet the specific needs of different stakeholders.

Incident Reports: Detailed reports of security incidents, including timelines, responses and outcomes.

Compliance Reports: Reports ensuring that the organization is compliant with relevant security regulations and standards.

System Performance Reports: Analysis of the performance and reliability of security systems and infrastructure.

Audit Trails: Comprehensive logs of system and user activities for auditing and investigative purposes.

Dashboard Features

Real-Time Monitoring Dashboards: Providing a real-time overview of security status, alerts and ongoing incidents.

Data Visualization Tools: Visual representations of data, such as graphs, charts and heat maps, for easy interpretation.

Customizable Interfaces: Allowing users to customize their dashboard views based on their roles and needs.

Integrated Data from Various Sources: Displaying consolidated data from physical, cyber and operational security systems.

Actionable Insights: Highlighting key information and insights that require immediate attention or action.

Health and Status Indicators: Provides quick visual indicators for the status and health of all integrated systems and devices, allowing for the real-time monitoring of equipment such as cameras, recording devices, network switches and servers.

Event Logs and Timelines: Displaying timelines and logs of events for tracking and analysis purposes.

Technical Specification

System Architecture

Scalable and Modular Design: Capable of supporting small to large-scale deployments, with the ability to support multi-location, multi-server and multi-system environments — crucial for large-scale and distributed operations.

High Availability and Redundancy: Designed for continuous operation with failover capabilities and backup systems.

Data Handling and Processing

Real-Time Data Processing: Capable of processing large volumes of data in real-time from multiple sources.

Big Data Analytics: Utilizing big data technologies for advanced analytics and predictive modeling.

Database Management: Robust database management systems for storing and retrieving large datasets efficiently.

Integration Capabilities

APIs and SDKs for Custom Integration: Providing APIs (Application Programming Interfaces) and SDKs (Software Development Kits) for custom integrations.

Industry-Standard Protocols: Support for a wide range of industry-standard communication protocols and interfaces including Web API (JSON, SOAP, RESTful), MQTT, SNMP, SQL, OPC, BACnet, Modbus, POP3, Logfile, SIP, SFTP and Serial Port (RS232, RS485) — enabling seamless integration with security devices, automation and IT systems.

CCTV Integration

Brand Compatibility: Ability to interface with different CCTV brands, with support for the common protocols and APIs used by these brands.

Live Streaming: Provides real-time video streaming from connected CCTV cameras, with support for different streaming protocols (e.g. RTSP, HTTP, ONVIF).

Video Playback and Export: The system provides easy retrieval and playback of recorded footage with search functions by camera, date and time, and offers the ability to export video clips in formats like Raw, AVI and MP4, with an option to add password protection and a proprietary viewer to ensure data integrity and prevent modification.

Dynamic Screen Division: Enables the screen to be divided into multiple sections for the simultaneous viewing of different camera feeds, with customizable layouts that also support the synchronized display of both live and recorded footage from the same camera on a single screen for direct comparison.

Layout Templates: Predefined layout templates (e.g. grid views of 4, 9, 16 cameras) for quick selection, with the option for users to create and save custom layout templates based on their specific needs.

Support for Camera Protocols and Standards: Compatibility with ONVIF, RTSP and other camera protocols.

Supported Video Management Systems (VMS) and Recording Devices: Compatible with leading Video Management Systems including Milestone, Axis Camera Station, Axxon, NX and Avigilon, as well as major DVR/NVR brands such as Hikvision, Dahua, UNV, Holowits and Hanwha, ensuring seamless integration across diverse video surveillance infrastructures.

Compatibility and Standards

Integration is achieved through open protocols, vendor SDKs and the platform API — existing equipment stays in place and keeps its own management tools.

INTEGRATION	PROTOCOLS AND INTERFACES
Web API	JSON, SOAP, RESTful
Messaging & monitoring	MQTT, SNMP, OPC, POP3, Logfile
Building & automation	BACnet, Modbus
Data & file	SQL, SFTP
Voice	SIP
Serial port	RS232, RS485

VIDEO	PROTOCOLS AND CODECS
Camera standards	ONVIF, RTSP, HTTP
Streaming protocols	HLS, RTMP, MPEG-DASH, WebRTC, RTSP, SRT, Microsoft Smooth Streaming
Video codecs	H.264 (AVC), HEVC (H.265), VP8, VP9
Audio codecs	AAC, Opus, G.711, G.722
Export formats	Raw, AVI, MP4 with password protection and proprietary viewer

VIDEO PLATFORMS	SUPPORTED SYSTEMS
Video Management Systems	Milestone XProtect, Axis Camera Station, Axxon, NX, Avigilon, Bosch BVMS, Genetec-class systems via ONVIF / SDK
DVR / NVR brands	Hikvision, Dahua, UNV (Uniview), Holowits, Hanwha Wisenet
Map services	Google Maps, Mapbox, OpenStreetMap, GIS Offline, JPG floor plans

SUBSYSTEMS	TYPICAL INTEGRATION
Access control & IAM	Door control, status and entry/exit logs via API or SDK, linked to the cameras at each door
Fire, intrusion & sensors	Alarm and trouble events over API, Modbus, serial port or log file
Video analytics & AI	Object, face, plate, behaviour and counting metadata via API, MQTT or SDK
Network & IT	SNMP device health, plus Telnet and SSH control of switches from the map interface
Building management	HVAC, lighting and power via BACnet, Modbus or OPC

AI Metadata Integration

Object Detection: Identifies and categorizes objects in the video feed.

Facial Recognition: Recognizes individuals from facial features.

Motion Analysis: Tracks and analyzes movement patterns.

License Plate Recognition: Captures and identifies vehicle plates, with the additional capability to analyze detailed vehicle characteristics.

Crowd Analysis: Estimates crowd size and density.

Behavior Analysis: Detects unusual or suspicious behaviors.

Audio Analysis: Analyzes audio for potential security threats.

People Counting: Automatically counts the number of people passing through a designated area or within a specific view.

Metadata Tagging: Automatically tags footage with AI-generated metadata.

Notifications

Real-Time Alerts: Immediate notification of security incidents, system malfunctions or other critical events based on predefined criteria and thresholds.

Multi-Channel Delivery: Notifications are delivered through multiple channels, including email, SMS, mobile app notifications, intercom systems, public address systems and even through integration with social media platforms.

Popup Notifications: Upon detection of a security event, the system can automatically display a live video feed from the nearest camera to the incident location and automatically display the relevant Standard Operating Procedure (SOP) for that specific type of incident.

Customizable Alert Profiles: Allows for the customization of alert types, priorities and recipient groups. Different stakeholders can receive notifications tailored to their specific roles and responsibilities.

Advanced E-Map and GIS Integration

Multiple Map Formats: The system is capable of handling E-Maps in image formats such as JPG, providing flexibility in the use of custom map images. It supports Geographic Information System (GIS) formatted maps, allowing for detailed and data-rich map presentations. Integration with online mapping services like Google Maps, Mapbox, OpenStreetMap and GIS Offline is available, offering extensive geographical data and familiar navigation tools.

Interactive E-Maps: Electronic maps that allow users to interact, zoom in and out, and get detailed information about specific locations or assets.

Layered Mapping: Offering layered views on the map to display different types of information, such as security zones, camera locations, sensor placements and access control points.

Device Alert Symbols on Maps: The system can display symbols or icons on the map to represent alerts or statuses of various security devices, providing a visual overview of security situations.

Customizable Device Positioning: Users can place icons representing CCTV cameras, recording devices or other security systems on the map, allowing for accurate representation of the physical location of security assets.

Real-Time Location Tracking: Displaying the real-time locations of security assets, personnel, vehicles and other resources on a GIS map for quick situational assessment.

Advanced E-Map and GIS Integration (continued)

Camera Field of View Display: The system is capable of visually representing the field of view for each camera directly on the map interface, providing a clear overview of the surveillance coverage.

Multi-Level Mapping Capabilities: The E-Map functionality supports multi-level maps, useful in complex environments like multi-story buildings or campuses. For instance, clicking on a CCTV camera icon on the map can reveal detailed information about the camera, including its live feed or specific attributes.

Advanced Search and Expansion Capability: Supports device and location-based search functionality, allowing users to quickly locate specific assets on the map. Additional information and features are accessible via expandable views or dedicated interface pages for detailed exploration.

Annotation and Drawing Tools: The system supports the creation of various annotation and graphic elements including lines, boxes, ellipses, images, text labels, rulers, angles, polylines, memos and line labels, enabling detailed marking and visual explanation on maps or video frames.

GIS and E-Map Interactive: By integrating various control functions directly into the map interface, this feature allows users to perform multiple actions — such as managing computers, viewing live or playback camera feeds, managing I/O, controlling network switches via integrated Telnet and SSH clients, and interacting with the system's API — all from a single, unified interface.

Security and Compliance

Cybersecurity Features: Including encryption, intrusion detection system, firewalls and regular security updates.

Compliance with Industry Standards: Meeting standards such as GDPR, HIPAA or ISO for data privacy and security.

Video Streaming

Live Streaming: Enables real-time broadcasting of video and audio content, often used for events, webinars and live announcements.

On-Demand Streaming: Provides capabilities to store and stream video and audio content to users on demand.

Scalability: Ability to scale the streaming services to accommodate a large number of simultaneous viewers without compromising on quality.

HTTPS Streaming: By supporting streaming over HTTPS, the platform adds an additional layer of security. HTTPS combines HTTP with SSL/TLS encryption, providing a secure channel over which the content is delivered — especially important for sensitive or proprietary content.

Supported Protocols: HLS (HTTP Live Streaming), RTMP (Real-Time Messaging Protocol), MPEG-DASH (Dynamic Adaptive Streaming over HTTP), WebRTC (Web Real-Time Communication), RTSP (Real-Time Streaming Protocol), SRT (Secure Reliable Transport) and Microsoft Smooth Streaming.

Supported Codecs: H.264 (AVC), AAC (Advanced Audio Coding), HEVC (H.265), VP8 & VP9, Opus and G.711, G.722.

Reporting and Analytics

Advanced Reporting Tools: Comprehensive tools for creating custom reports and analytics.

Data Visualization: Tools for visual data representation, including graphs, heat maps and more.

Comprehensive Event Logging: Capturing and logging all system events, user activities and security incidents in detailed logs.

Searchable Logs: Providing powerful search tools to quickly find specific events or activities in the log database.

Pivot Grid Functionality: Utilize interactive pivot grids to summarize and analyze large volumes of historical data from various system logs.

Integrated Data Visualization: Generate dynamic charts and graphs that are directly linked to the data summarized in the pivot grids, enabling clear and actionable insights.

Networking and Connectivity

Robust Networking Capabilities: Supporting LAN, WAN and cloud-based infrastructures.

Remote Access and Mobility: Secure remote access capabilities for mobile devices and off-site management.

User Management

Role-Based Access Control (RBAC): Create user roles with specific permissions, enabling you to assign appropriate access levels to each user.

Password Policies and Security: The system allows for secure password management for each user. This includes features like account lockout after a specified number of failed login attempts, mandatory password change intervals and password expiration policies.

Access Time Restrictions: Define detailed user privileges, such as the right to control image display, search and view recorded footage, and operate PTZ (Pan/Tilt/Zoom) cameras.

Backup and Disaster Recovery

Data Backup Solutions: Regular backup solutions to prevent data loss.

Disaster Recovery Plans: Strategies in place for system recovery in case of major incidents.

Virtual Matrix Monitor Management

Supports dynamic control and switching: Enables operators to control and command the switching of video signals to a video decoder device or video wall, providing flexible display management.

Allows flexible screen layout management: Enabling free-form division and arrangement based on operational needs.

Displays a variety of content: Including live CCTV camera feeds, sequential camera views, grouped camera views (view profiles), GIS maps with device alarm symbols, web applications, video streaming sources and integration with Google Maps or OpenStreetMap.

Provides full control over display window sizing and positioning: Allowing operators to resize or move windows freely.

Virtual Matrix Monitor Management (continued)

Features a Matrix Profile System: With predefined templates that determine how camera feeds, maps and alarm indicators are distributed across monitors; upon profile selection, all defined content is simultaneously presented across designated displays.

Integrates seamlessly: With CCTV platform video display systems, supporting pixel-level control with zoom and pan functions via mouse interaction, and independent camera display management for comprehensive situational awareness.

Aggregates and displays multiple data sources: Video, maps, alarms and third-party applications on a unified visual matrix.

Empowers operators: With contextual insights and rapid decision-making capabilities through an interactive, real-time dashboard.

Incident Management

Automated Incident Creation: The system automatically generates a new incident record whenever an alarm or event is triggered, ensuring no critical event is missed.

Incident Classification and Prioritization: Automatically classifies incidents based on predefined criteria and assigns a priority level, allowing operators to focus on the most critical events first.

Guided Response Workflows: The system activates predefined Standard Operating Procedures (SOPs) to guide operators through the response process, providing a form to confirm the incident as a genuine or false alarm, displaying relevant contact information for coordination, and including a summary form to document the resolution.

Evidence and Data Aggregation: Automatically gathers all relevant data, such as live video feeds, event logs, access control records and sensor data, and associates it with the incident for a complete picture.

Integrated Communication Tools: Facilitates seamless communication and collaboration among response teams, stakeholders and external agencies directly within the incident management interface.

Real-time Alert Handling: The system provides a structured process for managing alerts from all integrated systems by displaying the incident's name, location and details on an E-Map, while also automatically showing a live or playback video feed and providing access to recorded footage from the nearest camera at the time of the event.

Incident Status Progression: The system displays incident alert progression through four statuses — ToDo for new events prioritized by time and severity, Doing for incidents actively being resolved, Block when awaiting external assistance, and Done once the incident is completed.

Access Control Integration

Integrated Visuals: Supports the viewing of both live and recorded footage from cameras linked to specific doors, providing visual context for access events.

Real-time Control & Status: Enables real-time control of door status, including the ability to remotely lock and unlock doors. The system also provides a real-time display of the door's status.

Entry/Exit Logging: Provides a detailed log of individuals passing through the door, enhancing security and traceability.

Export Online

Requests for recorded footage rarely arrive through the control room door. Export Online turns that traffic into a governed online service: the public files the request themselves, officers judge it against the recording that actually exists, and nothing leaves the organisation until two separate approvals have been recorded against the case.

Step 1
Filed online
The requester submits date, time, place and purpose, and attaches proof of identity.

Step 2
Matched to footage
An officer locates the cameras and the retained recording that answer the request.

Step 3
Case approved
The grounds for the request are accepted or refused, with the decision noted on the case.

Step 4
Release authorised
A second, separate authorisation is required before the prepared file may leave the system.

Step 5
Handed over
The requester is notified and collects the file through the same online case, under expiry.

For the requester

Self-service intake: A public web form replaces the counter visit — the request, the supporting documents and the contact details all arrive in one submission, correctly formed.

Case reference and progress: Every submission is answered with a reference number the requester can use to follow where the case stands, without telephoning the operations centre.

Collection on notice: When release is authorised the requester is notified and given a time-limited collection window; after it lapses the material is no longer retrievable.

For the officer

One queue, one screen: Incoming requests are worked from a single list — read the request, search the recording by camera, date and time, preview the footage and act, all in the same interface.

Separated authority: Deciding the case and releasing the file are distinct rights that can be held by different people, so no single account can take a request from arrival to handover.

Scoped extraction: Only the segment and cameras the case calls for are cut, in Raw, AVI or MP4, keeping the release proportionate to what was asked.

Complete case record: The request, the attachments, both decisions, the operators involved and the delivery are held together and written to the audit trail for later inspection.

How a released file stays under control

Sealed on export
The clip is written into an encrypted container that carries its own key material; separated from that key the file yields nothing.

Opened under password
Playback runs in the supplied viewer and asks for the password issued with the case, which also keeps the footage from being silently re-edited.

Marked with its origin
The issuing organisation is stamped on the material, so a copy in circulation can still be traced back to the case that released it.