

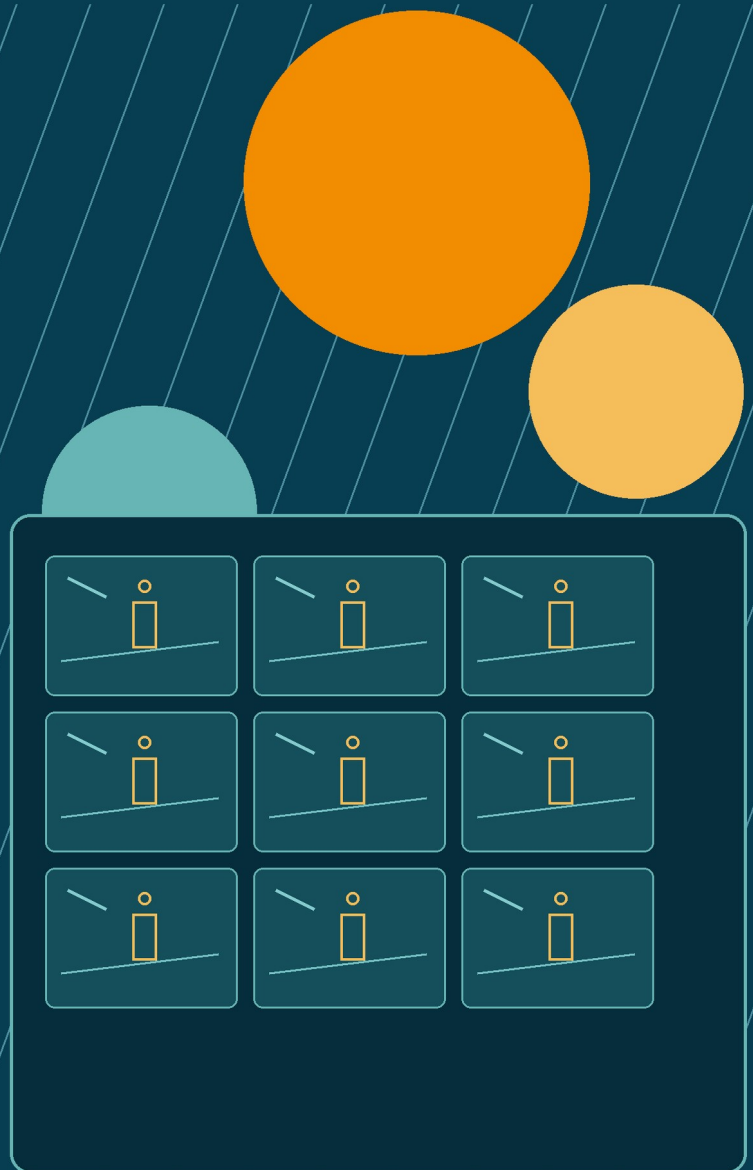
ACTi

Physical Security End-to-End Solution Provider

White Paper | Control Center

CONTROL CENTER

A practical white paper for centralized surveillance, collaborative monitoring, and coordinated incident response



Prepared by ACTi Corporation

Version 1.2 | July 2026

White Paper | Control Center

Contents

1

Executive Summary.....

3

2

About ACTi Corporation.....

4

3

Definition of "Control Center".....

5

4

Core Technical Concepts.....

6

5

High-Value Applications.....

7

6

System Architecture.....

8

7

ACTi Product Portfolio Overview.....

9

8

Related Keywords and Terminology.....

10

Document purpose

This white paper explains the role of a professional security control center and positions ACTi control center capabilities within a complete surveillance and incident-management ecosystem. It is written for system integrators, consultants, end users, security managers, facility teams, operations leaders, and procurement stakeholders.

The structure and visual hierarchy follow the supplied ACTi Standard Cameras white paper, including a full-page cover, consistent section numbering, compact technical tables, practical diagrams, and a grouped terminology chapter. [Reference layout]

1. Executive Summary

A security control center is the operational hub where information from cameras, recorders, analytics, sensors, access control, alarms, and remote sites is transformed into coordinated action. Its purpose is not simply to display many video streams. A well-designed control center helps operators identify priority events, verify what is happening, investigate efficiently, communicate with responders, preserve evidence, and maintain awareness of system health.

ACTi describes control centers as the preferred approach for large sites and multi-location projects managed from a single room, using individualized workstation screens for focused tasks and collaborative TV walls for shared overview monitoring. ACTi also presents its control center architecture as scalable to very large deployments and able to centralize the management of cameras and network video recorders. [1]

For end users, the value is faster response, consistent procedures, stronger evidence handling, and better visibility across the organization. For system integrators and consultants, the control center creates a structured design framework that connects field devices, network architecture, recording, central management, user permissions, visualization, integration, resilience, and operator ergonomics.

Core message

A control center should be specified as an operational system, not as a room filled with monitors. The design must connect technology, people, process, and resilience so that the right information reaches the right operator at the right time.

Key takeaways

- Central management should unify live view, event handling, maps, playback, evidence export, user control, audit records, and system health.
- Workstation screens support individual duties; TV walls support shared situational awareness and cross-team coordination.
- Event-driven workflows are more effective than expecting operators to watch every camera continuously.
- Network design, time synchronization, cybersecurity, redundancy, storage, and maintenance are part of control center performance.
- Room layout, sightlines, lighting, acoustics, ergonomics, staffing, escalation rules, and standard operating procedures are as important as software features.

Procurement principle

Do not specify a control center only by channel count or number of displays. Specify the required operational outcomes: which sites are managed, which events must be prioritized, how incidents are verified, who may take each action, how evidence is protected, and how the system continues operating during failures.

2. About ACTi Corporation

ACTi Corporation is the writer and publisher of this document. ACTi is a Taiwan-based international company founded in 2003 and serving customers in more than 100 countries. ACTi states that it has more than 20 years of security-industry experience and has been a pioneer in video-based security technology development and innovation. [2]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem covers video surveillance, recording platforms, video management software, workstation and web clients, mobile access, access control, central management, system health management, redundancy, backup, and integration with third-party alarms, intercoms, sensors, IoT devices, and access-control systems. [2]

This end-to-end scope is relevant to control center projects because operational value depends on more than a central application. A complete solution must connect reliable field video, searchable recordings, events and metadata, role-based clients, shared displays, integration, health monitoring, and response procedures.

Why ACTi is relevant to control center projects

ACTi strength	Project relevance
End-to-end system scope	Control centers can be planned with cameras, recorders, management software, clients, access control, alarms, and third-party integration rather than as isolated display systems.
Centralized management direction	ACTi describes central management for large mission-critical projects, multi-site NVR monitoring, workstation applications, and TV wall overview. [1][2]
AI and event workflow	Video analytics and metadata can support incident detection, prioritization, investigation, and decision support instead of relying only on continuous visual observation. [1][2]
Reliability and system health	Redundancy, backup, health monitoring, configuration recovery, and device-status visibility support continuity in critical security operations. [1][2]
Integration readiness	Events and metadata from cameras, sensors, access control, alarms, and external systems can be brought into a common operational workflow. [2]

3. Definition of "Control Center"

A security control center is a centralized operational environment that collects, presents, prioritizes, and manages information from distributed surveillance and security systems. It typically combines central management software, operator workstations, shared display systems, video recording access, maps, event queues, communications, system-health information, and documented response procedures.

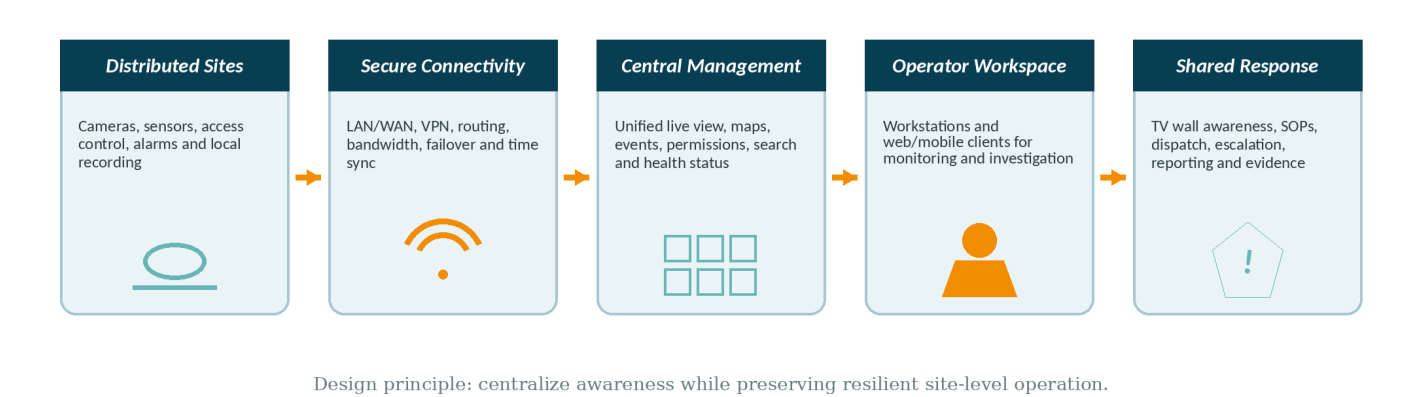
In professional surveillance, a control center may support one large site, a campus, a citywide network, multiple branches, critical infrastructure, transportation facilities, industrial operations, or a combination of local and remote locations. The defining characteristic is coordinated management: separate devices and sites are transformed into a unified operational picture.

Control center vs. related concepts

Term	Meaning	Common misunderstanding
Security control center	Central environment for monitoring, verification, investigation, coordination, evidence, and system oversight.	It is not only a room or video wall; it includes software, network, people, procedures, and resilience.
Central management system	Software layer that aggregates recorders, cameras, events, users, maps, health status, and clients.	Central management does not replace local recording, network design, or operational procedures.
TV wall	Shared multi-display surface used for overview, priority incidents, maps, dashboards, and collaboration.	More screens do not automatically improve awareness; content rules and operator workflow are essential.
Operator workstation	Individual client used for live view, playback, event handling, search, export, configuration, or investigation.	One workstation should not be expected to display every camera continuously.
Security operations center	Broader organizational function that may combine physical security, communications, cyber monitoring, emergency management, and business continuity.	A video control center can be part of a wider operations center, but the scopes are not always identical.

Visual concept

From distributed sites to coordinated response



4. Core Technical Concepts

Control center design should combine surveillance functions, information architecture, cybersecurity, reliability, human factors, and operational governance. The following concepts help project teams compare solutions accurately and avoid a display-centric design that does not support real incident handling.

Concept	Practical meaning
Centralized federation	The management layer aggregates multiple recording servers, sites, cameras, users, events, and status information while preserving local recording and site autonomy.
Event-driven monitoring	Analytics, motion, digital inputs, tampering, audio, access events, device status, and third-party alarms should place priority information in front of the appropriate operator. ACTi lists a wide range of event triggers and automated responses. [1]
Flexible visualization	Operator layouts should support variable grid sizes, priority hot spots, maps, panoramic views, embedded work information, PTZ control, and hardware-assisted decoding where required. [1]
Investigation workflow	Fast search, thumbnails, event filters, bookmarks, instant playback, synchronized multi-channel playback, export, and evidence authenticity improve post-incident work. [1]
Role-based access	User groups, directory integration, customized permissions, account lockout, automatic logout, dual-authentication options, password governance, and audit logs reduce misuse and support accountability. [1]
Cybersecurity architecture	Segmented networks, secure remote access, encrypted recordings, patch and firmware processes, least privilege, logging, and hardened servers protect both live operations and evidence. [1]
Resilience and health	Redundancy, backup, system-health monitoring, configuration recovery, network failover, power protection, and degraded-mode procedures reduce operational interruption. [1]
Human factors	Sightlines, screen size, viewing distance, alert fatigue, acoustics, lighting, seating, shift handover, staffing, and training directly affect response quality.
Interoperability	Control centers often connect access control, alarms, intercoms, maps, sensors, IoT, dispatch, public-address systems, and third-party management platforms. [2]

Specification interpretation

A high channel count does not guarantee a usable control center. Real performance depends on network latency, decoding capacity, storage search speed, alarm prioritization, display rules, operator workload, interface design, and the ability to recover from component or site failures.

Procurement warning

Avoid requirements such as “show all cameras at all times.” Instead, define overview views, exception views, event pop-ups, investigation screens, map views, rotation rules, failover behavior, and measurable response procedures.

5. High-Value Applications

Control centers are most valuable where security information is distributed across many cameras, recorders, buildings, sites, or operational teams. ACTi positions the category for large-scale projects and multi-location management from a single room with workstation screens and collaborative TV walls. [1]

Application	Operational value	Typical environments
Multi-site enterprise security	Standardizes monitoring, alarm handling, user access, reporting, and evidence processes across dispersed locations.	Retail chains, offices, banks, campuses, hotels, logistics networks
Critical infrastructure	Combines perimeter, access, process-area, alarm, and equipment-status information for faster verification and escalation.	Utilities, energy, water, communications, data centers
Transportation operations	Coordinates live video, incidents, passenger areas, vehicle movement, restricted zones, and emergency response.	Airports, ports, rail, transit, highways, depots
Industrial and logistics sites	Supports process visibility, worker safety, restricted-area monitoring, loading activity, and remote facility oversight.	Factories, warehouses, distribution centers, plants, yards
Public safety and government	Creates shared situational awareness, controlled evidence workflows, and coordination across agencies or departments.	Municipal facilities, public spaces, correctional sites, government campuses
Large campuses and smart buildings	Unifies buildings, entrances, parking, access control, alarms, visitor areas, and facility operations.	Universities, hospitals, business parks, mixed-use developments

Value by stakeholder

Stakeholder	Main benefit
Control room operator	Prioritized events, consistent layouts, faster verification, synchronized playback, and clearer escalation paths.
Security manager	Common procedures, user accountability, incident reporting, staffing visibility, and measurable response performance.
Facility / operations manager	Shared awareness of safety, access, equipment areas, remote locations, and business-impacting incidents.
System integrator	Structured architecture for combining field devices, recording, central management, clients, displays, networks, integration, and resilience.
Consultant / procurement team	Clearer requirements for scalability, availability, cybersecurity, evidence, operator workflow, room design, training, and acceptance testing.

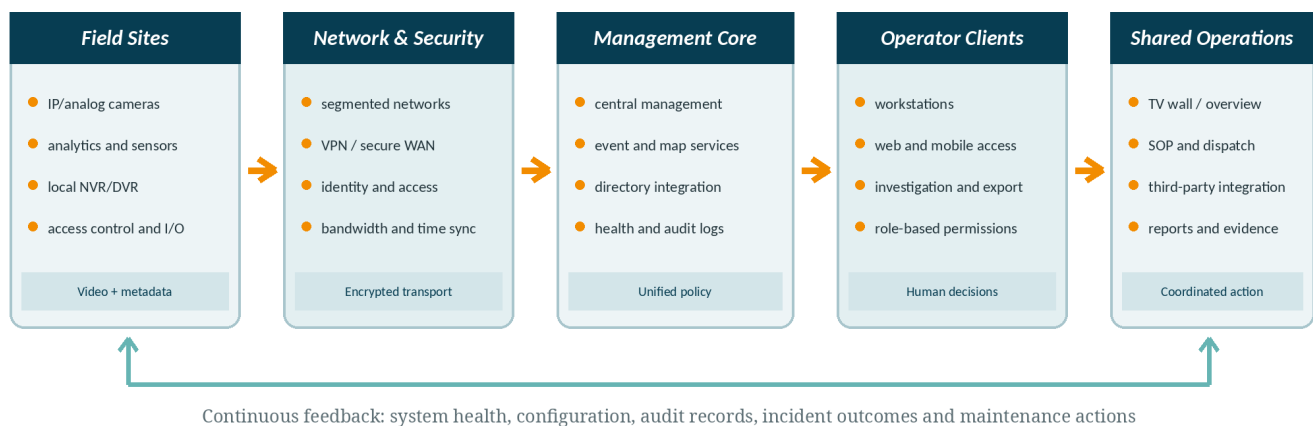
6. System Architecture

A control center should be designed as a layered system. Field devices and local recording protect site-level continuity. Secure networks carry video, metadata, events, and management traffic. The central management core applies common views, policies, maps, user permissions, event rules, search, and health monitoring. Operator clients and shared displays present information according to role and urgency. Integration and response procedures turn verified information into action.

ACTi describes a central management approach that connects many recording servers and cameras, provides individualized workstation use, supports collaborative TV wall monitoring, manages video analytics events, and offers multiple client types. The official control center overview also highlights user management, system health, redundancy, backup, and third-party response actions. [1]

Reference system architecture

Reference control center architecture



Architecture layers

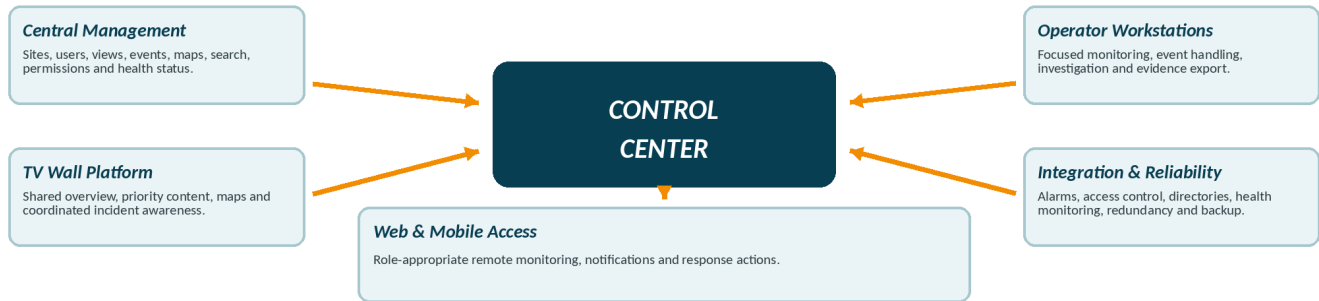
Layer	Role in control center operations
Field and recording	Cameras, encoders, sensors, access devices, alarms, local NVR/DVR, edge analytics, and resilient recording at each site.
Network and security	PoE/access networks, uplinks, WAN/VPN, segmentation, routing, bandwidth, QoS, identity, remote access, firewall rules, and time synchronization.
Management core	Central federation, directory integration, maps, event rules, health status, audit logs, configuration, search services, and integration interfaces.
Operator and display	Workstations, web/mobile clients, decoders, TV wall outputs, ergonomic layouts, hot spots, dashboards, and role-based views.
Response and governance	SOPs, communication, dispatch, access actions, alarm outputs, evidence retention, reporting, maintenance, training, and audit review.

7. ACTi Product Portfolio Overview

ACTi presents control center solutions as an end-to-end combination of central management, operator workstations, TV wall systems, client applications, event management, analytics integration, user control, system health, redundancy, backup, and third-party integration. The portfolio should be selected by role and system function rather than by a single appliance or model number. [1][2]

Portfolio building blocks

Control center portfolio building blocks



Category	Where it fits	Use-case fit
Central management platform	Core software or server layer that aggregates multiple recording systems, cameras, users, events, maps, search, and status.	Multi-site monitoring, large channel counts, common policies, unified investigation, and centralized administration.
Operator workstation client	Full-featured individual interface for monitoring, playback, event handling, export, configuration, and investigation.	Dedicated security operators, investigators, supervisors, and technical administrators.
TV wall platform	Multi-output visualization for collaborative overview and priority content.	Shared awareness, emergency coordination, maps, dashboards, high-priority incidents, and executive overview.
Web and mobile clients	Remote or lightweight access suited to role, device, network, and security policy.	Supervisors, remote guards, mobile response teams, facility managers, and after-hours verification.
Video decoder / local display	Mouse-free or keyboard-free display endpoint for controlled video output.	Guard posts, reception, local overview, simple display-only stations, and selected TV wall endpoints.
Health, redundancy, and backup services	Supporting functions that monitor critical devices and preserve service or recordings during faults.	Mission-critical deployments, remote sites, high-availability operations, and formal maintenance programs.
Integration interfaces	Connections to access control, alarms, intercom, digital I/O, sensors, IoT, maps, directories, and third-party management systems.	Unified verification, automated response, cross-system investigation, and operational dashboards.

Portfolio-level capabilities to confirm

- Number of sites, recording servers, cameras, users, concurrent clients, displays, and simultaneous streams.
- Live-view layout, decoding performance, map functions, event pop-ups, investigation tools, export formats, and evidence verification.
- Analytics event support, alarm response actions, notifications, audio, PTZ, digital output, and third-party integrations.
- Directory services, user groups, permissions, audit logging, password policies, secure communications, encryption, and patch management.
- Redundancy, backup, system health, configuration recovery, power and network failover, and maintenance access.
- Latest regional availability, licensing, datasheets, release notes, compatibility lists, and project quotation documents.

8. Related Keywords and Terminology

The following reference groups collect common terms related to security control centers, central management, video walls, operator workflows, incident response, system integration, resilience, and project procurement.

Core topic keywords

security control center, surveillance control center, video control center, command center, monitoring center, central monitoring room, security operations center, physical security operations center, centralized surveillance, multi-site surveillance, large-scale video management, mission-critical security monitoring

Central management keywords

central management system, multi-NVR management, multi-site video management, federated video surveillance, unified security management, centralized camera management, user and role management, event management, map-based monitoring, system health monitoring, audit logging, directory integration

Operator and display keywords

security workstation, operator workstation, control room workstation, video wall, TV wall, multi-monitor surveillance, collaborative monitoring, priority video display, alarm hot spot, flexible video grid, panoramic dewarping, PTZ joystick control, control room ergonomics

Event and investigation keywords

video analytics event, alarm verification, incident detection, event pop-up, automated response, thumbnail search, event search, instant playback, synchronized playback, evidence export, video bookmark, authentic evidence, incident reconstruction, forensic video review

Integration keywords

access control integration, alarm integration, intercom integration, sensor integration, IoT integration, digital input output, map integration, third-party VMS integration, SCADA video integration, emergency communication, dispatch integration, public address integration

Reliability and cybersecurity keywords

N+1 redundancy, system failover, recording backup, configuration backup, system health management, device status monitoring, network segmentation, VPN surveillance, encrypted video evidence, role-based access control, account lockout, audit trail, secure remote access, time synchronization

Application keywords

airport control center, seaport control center, transit operations center, campus security center, retail monitoring center, industrial security control room, logistics monitoring center, utility security operations, city surveillance center, data center security monitoring, hospital security control room

Procurement and project keywords

control center design, control room requirements, surveillance command center architecture, video wall design, operator workstation specification, control center acceptance testing, control room staffing, alarm response SOP, multi-site surveillance specification, control center cybersecurity, control center redundancy, ACTi control center white paper

Common question phrases

what is a security control center, how to design a surveillance control room, central management system vs VMS, how many monitors should a control room have, how to reduce alarm fatigue, how to manage multiple NVR servers, how to design a video wall, how to secure a surveillance control center, how to test control center failover

Source notes

This white paper is based on ACTi public source pages and established video surveillance system-design practices. Product details, software functions, licensing, compatibility, and regional availability should always be reconfirmed against the latest ACTi documentation before formal project commitment.

Ref.	Source
[1]	ACTi Corporation, “Control Center,” official product category page. URL: https://www.acti.com/products/control-center . Accessed: July 21, 2026.
[2]	ACTi Corporation, “About ACTi,” official corporate page. URL: https://www.acti.com/corporate/about . Accessed: July 21, 2026.
[Reference layout]	ACTi Corporation, “ACTi Standard Cameras White Paper,” user-supplied PDF used only as the structure and layout reference for this document.

Revision note: This document is a marketing and technical education white paper. It is not a regulatory certification, safety standard, room construction drawing, cybersecurity assessment, or final project design. Validate workflow, network, resilience, room layout, staffing, permissions, and incident procedures in the target environment before deployment.

Prepared by ACTi Corporation

For control center projects, confirm architecture, capacity, clients, display requirements, event workflows, integrations, cybersecurity, redundancy, licensing, and regional availability with your ACTi sales contact or authorized system integrator.