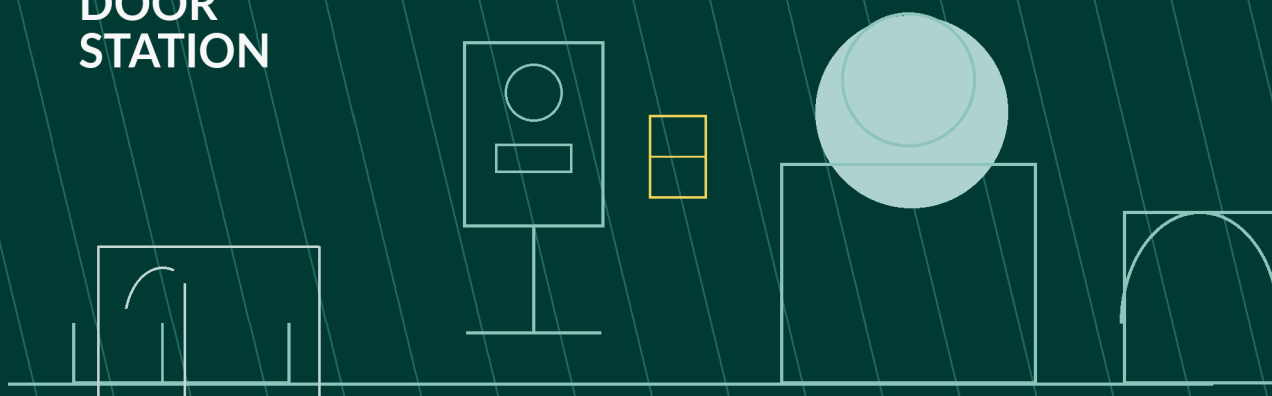


ACTi

Physical Security End-to-End Solution Provider

White Paper | Door Station

DOOR STATION



A practical white paper for designing secure video intercom, access control, and visitor verification systems

Door Station ACTi Corporation

Contents

- 1 Executive Summary
- 2 About ACTi Corporation
- 3 Definition of "Door Station"
- 4 Core Technical Concepts
- 5 High-Value Applications
- 6 System Architecture
- 7 ACTi Product Portfolio Overview
- 8 Related Keywords and Terminology

Document purpose

This white paper explains what a Door Station means in professional physical security, how it supports access control and video intercom workflows, and how it should be specified for entrance management projects.

It is written for system integrators, consultants, security managers, facility managers, procurement teams, and end users that need clear visitor verification, remote communication, access-event recording, and operational evidence at doors, gates, lobbies, reception areas, loading docks, and controlled facilities.

The document references ACTi public product and solution information for Door Station, intercom service, access control, service desk cameras, and ACTi corporate information. It avoids model-specific naming so the content remains usable even as individual part numbers or product generations change.

Reading guide

Use Sections 3 and 4 to define technical requirements, Section 5 to map applications, Section 6 to review the system architecture, and Section 7 to align ACTi product categories with project needs.

1. Executive Summary

A Door Station is a network-connected entrance device that combines video, two-way audio, call initiation, credential input, door-control signaling, event logging, and surveillance-system integration. It transforms a doorway from a simple mechanical access point into a managed security checkpoint where operators can see, speak, verify, unlock, record, search, and respond.

ACTi public information positions Door Station technology around video intercom, camera-based visitor verification, microphone and speaker communication, RFID-based access, touch-button operation, PIR sensing, and face-identification related workflows. ACTi also describes intercom service as a way to combine high-definition video, two-way audio, remote door control, VMS integration, and synchronized evidence recording. [1][2]

For system integrators, Door Station projects create value when proposals address the complete entrance workflow: door hardware, wiring, network, PoE, SIP or intercom routing, credentials, access-control rules, NVR/VMS recording, user permissions, alerts, mobile response, and evidence export. For consultants and end users, the correct specification should define the security objective before selecting the device form factor.

Core message

Door Stations should be specified as part of a complete entrance management system. Video, audio, credential verification, door status, event metadata, recording, alarm response, remote operation, and maintenance planning all affect whether the system can provide secure access decisions and defensible evidence.

Key takeaways

- Door Station value comes from verified access decisions, not only from installing an intercom device.
- A modern entrance system should combine visual verification, clear communication, credential handling, event logging, and video evidence.
- System design must include door locks, exit buttons, request-to-exit devices, cabling, PoE/network, cybersecurity, recording, and operator workflow.
- Face, card, PIN, mobile, or other credential methods should be selected based on site risk, privacy rules, and operational convenience.
- Integration with NVR/VMS, access control software, CMS, notifications, and mobile clients improves investigation and response continuity.
- Project teams should confirm product availability, integration scope, accessories, regional compliance, and firmware capability before submission.

Procurement principle

Do not specify Door Station only as a device label. Specify the entrance risk, verification method, intercom workflow, door hardware, network topology, recording policy, user permissions, notification rules, maintenance access, and evidence export process together.

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. [6]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem includes IP cameras, recording platforms, VMS, access control, central management, system health management, AI-enabled video technologies, mobile operation, and third-party system integration. [2][3][6]

This broader ecosystem matters for Door Station projects. A front-door device can capture the caller and initiate communication, but the project succeeds only when the full system can verify identity, authorize or deny entry, record the event, notify the correct staff, preserve evidence, and keep every access point manageable across one or many facilities.

Why ACTi is relevant to Door Station projects

ACTi strength	Project relevance
End-to-end system scope	Door Stations can be planned together with IP video, NVR/VMS, access control, CMS, notifications, intercom endpoints, and system health management instead of being treated as isolated devices.
Video as a foundation	ACTi emphasizes video-based security and surveillance technologies; for entrance management, visual verification improves confidence before granting access.
Unified access and video workflow	ACTi access control information references live view, two-way audio intercom, door lock control, event recording, search, playback, export, notifications, and analytics-related access workflows. [3]
Project and compliance fit	ACTi public information references compliance and vertical-market requirements; project teams can align device selection, system software, and documentation with tender needs. [6]

3. Definition of "Door Station"

A Door Station is an entrance-side device used to verify, communicate with, and manage people requesting access at a doorway or gate. In professional security projects, it typically combines a camera, microphone, speaker, call button or touch button, credential reader, input/output interface, event trigger, and network connection.

ACTi describes Door Station as a video door station with intercom, camera, RFID door access, touch button, PIR sensor, and face identification. ACTi intercom-service materials further emphasize high-definition video, two-way audio, remote door control, VMS integration, mobile or remote accessibility, and synchronized recording for audit trails. [1][2]

Project teams should treat Door Station as both a device category and a workflow design topic: who approaches the door, how they call, how operators verify identity, which credential method is accepted, how the lock is triggered, what gets recorded, how events are searched, and how failures are maintained.

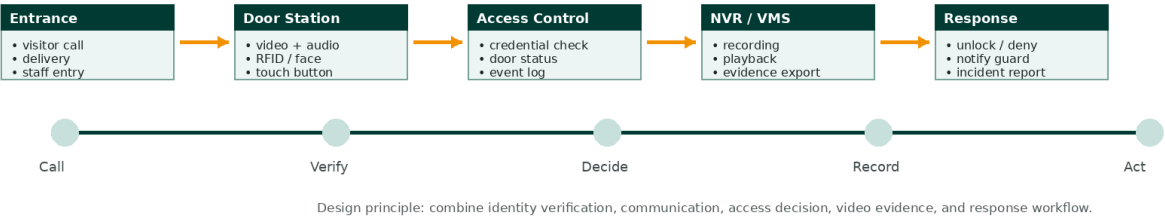
Door Station vs. related concepts

Term	Meaning	Common misunderstanding
Door Station	Network-connected entrance device that combines video, audio, access request, credential input, door-control signaling, and event metadata at a door or gate.	It is not only an intercom button; it should be part of an access, video, and event-recording workflow.
Video intercom	Audio communication combined with live video so staff can visually verify the caller before responding.	Video intercom alone may not include credential management, door status, or access-control rules.
Access control reader	Device used to read card, mobile credential, PIN, biometric, or other identity input.	A reader alone may not provide two-way audio, video, call routing, or evidence recording.
Service desk camera	Compact camera category for counter, desk, or staff-customer interaction monitoring with audio-evidence needs.	It is useful for close interaction evidence but does not replace door lock control or entrance credential handling.
Entrance surveillance camera	Camera viewing a doorway, gate, lobby, or corridor.	General surveillance improves visibility but may not communicate with visitors or control access decisions.

Visual concept

How Door Stations preserve access security and evidence value

From visitor request to verified access, recording, notification, and response



Design note

A Door Station creates value when the system allows operators to verify visitors, speak clearly, trigger door actions, record synchronized evidence, and search events without relying on isolated audio-only communication or manual entrance checks. The complete chain must be planned: entrance survey, mounting height, camera view, audio quality, credential method, door hardware, network path, recording, notification, mobile operation, maintenance access, playback, export, and response.

Practical deployment interpretation

In an office lobby, apartment entrance, warehouse dock, school gate, hospital ward, data center, or industrial facility, the Door Station may face backlight, nighttime operation, noise, vandalism, repeated button use, privacy constraints, high visitor volume, and remote-operation needs. The design should therefore protect both access security and evidence value while keeping operators able to verify, unlock, deny, and report events efficiently.

4. Core Technical Concepts

Door Station selection should begin with the entrance risk and operational workflow. The goal is to provide useful video, reliable audio, correct access decisions, and traceable evidence at the required doorway, distance, lighting condition, credential policy, and response time. The following concepts help teams avoid under-designed specifications.

Concept	Practical meaning
Entrance risk classification	Define who uses the door, what assets are behind it, visitor volume, public exposure, after-hours risk, and required response time.
Video verification	Camera view, resolution, WDR, low-light support, IR illumination, vertical angle, fisheye or wide-angle view, and face visibility determine verification value.
Two-way audio and call flow	Microphone, speaker, noise reduction, echo cancellation, call routing, SIP or platform integration, and mobile response affect user experience.
Credential and identity method	Card, mobile credential, PIN, face identification, visitor QR workflow, or manual approval should match security policy and privacy constraints.
Door I/O and lock control	Digital output, lock feedback, request-to-exit, door contact, emergency release, and fire-safety interlock must be coordinated with local code.
Event logging and evidence	Call, credential attempt, door open, door forced, tamper, failed access, snapshot, audio/video recording, playback, and export must be connected.
Network, power, and cybersecurity	PoE, VLAN, TLS/HTTPS, user permissions, password policy, firmware policy, firewall rules, and remote access protect system integrity.
Maintenance and system health	Remote device status, cable protection, cleaning access, vandal resistance, spare strategy, and support workflow reduce downtime.

Specification interpretation

A Door Station with strong camera and audio specifications can still fail the project if the view is badly angled, the door hardware is incompatible, calls route to the wrong operator, the NVR records the wrong stream, the access server does not log events, or the maintenance team cannot identify device failure quickly. Conversely, a correctly integrated system can improve security, visitor convenience, evidence handling, and operational efficiency at the same time.

Capability matrix

Entrance challenge to Door Station capability matrix

Translate entry-point risk into device, system, and operations requirements

Site challenge	What can go wrong	Capabilities to specify	Operational output
Blind visitor verification	Voice-only approval enables impersonation	Wide-angle video, two-way audio, call event	Visual confirmation
Noisy entrances	Poor audio causes slow or wrong decisions	Noise reduction, echo control, clear speaker	Clear communication
Unauthorized entry	Door forced, tailgating, invalid credential	RFID/face/PIR, door status, tamper events	Immediate alarm
Fragmented evidence	Separate systems lose context	NVR/VMS recording, event metadata, export	Searchable audit trail

How to use this matrix

Use the matrix during site survey and proposal design. Each entrance problem should be translated into a device requirement, system integration requirement, recording requirement, access-control rule, notification rule, and maintenance requirement. This reduces the risk of installing an attractive door device while leaving the system unable to preserve or use the captured evidence.

For tender writing, define the entrance type first. Then specify the Door Station form factor, camera view, audio performance, credential method, door I/O, lock integration, network security, recording platform, event search, notification workflow, remote operation, and report export requirements.

5. High-Value Applications

Door Stations are most valuable where communication, visual verification, and access authorization overlap. ACTi public materials connect Door Station and intercom workflows with entry points, remote door control, access control, VMS integration, recording, events, search, playback, export, and notifications. [1][2][3]

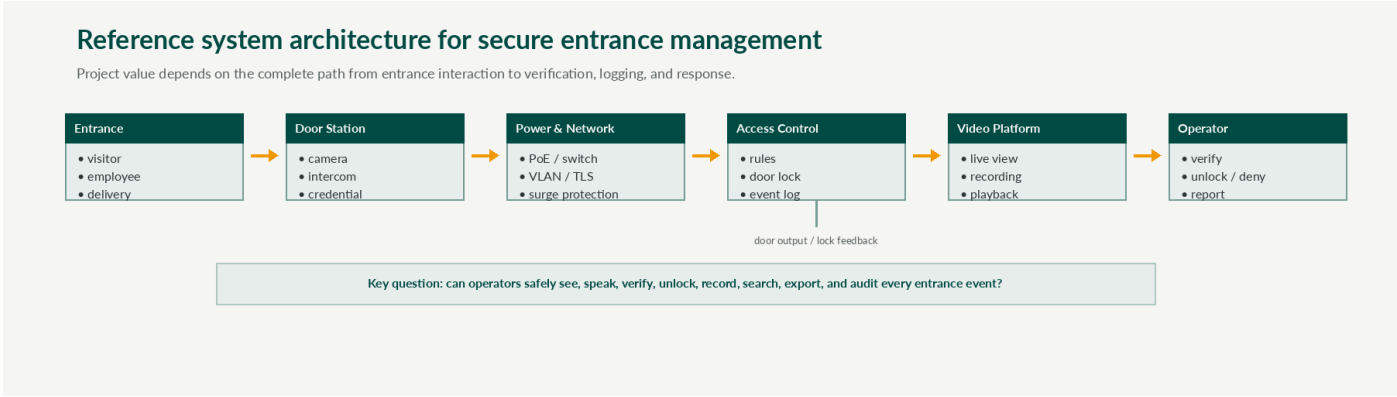
Application	Operational value	Typical locations
Corporate offices and reception areas	Verify visitors, deliveries, contractors, and employees before allowing access; preserve synchronized audio/video evidence for disputes or incidents.	Main entrances, lobbies, reception desks, executive floors, meeting areas
Residential buildings	Allow residents, guards, or managers to communicate with visitors and remotely grant access while maintaining an event trail.	Apartments, condominiums, gated communities, building entrances
Schools and campuses	Control entry during school hours, visitor check-in, after-hours access, and emergency response while keeping events searchable.	School gates, administrative entrances, dormitories, campus buildings
Healthcare facilities	Improve controlled access to wards, pharmacies, labs, staff-only areas, and after-hours entrances while supporting compliance evidence.	Hospitals, clinics, nursing homes, laboratories
Warehouses and logistics	Handle driver check-in, dock access, vendor verification, and gate control without requiring staff to be physically present at every entrance.	Loading docks, warehouse gates, truck entrances, guard booths
Industrial and critical facilities	Support remote verification at restricted doors, perimeter gates, control rooms, and high-value zones with video, audio, and event records.	Factories, utilities, data centers, plants, equipment rooms

Value by stakeholder

Stakeholder	Main benefit
System integrator	Stronger differentiation when proposals connect Door Station hardware, access control, VMS/NVR, notifications, door hardware, and maintenance workflow.
Consultant	Clearer specification language for entrance risk, verification method, door I/O, credential policy, event logging, and evidence export.
Security manager / operator	Faster visual confirmation, clearer communication, more consistent response, and searchable incident history.
Procurement team	A more defensible buying decision based on application fit, lifecycle cost, integration scope, compliance readiness, and support risk.

6. System Architecture

Door Station projects should be designed as system architecture. The entrance device provides the field interaction point, but the full solution must preserve operational value through mounting, power, network, credential rules, door hardware, recording, live viewing, playback, search, export, notification, system health monitoring, and maintenance workflow. If any layer is under-designed, the project may lose evidential value or create avoidable response delays.



Architecture layers

Layer	Role in Door Station surveillance and access control
Field layer	Entrance location, mounting height, camera angle, microphone/speaker performance, credential input, PIR, tamper, door contact, lock wiring, and visitor ergonomics.
Network layer	PoE, switching, VLANs, latency, HTTPS/TLS, remote access, firewall rules, time synchronization, surge protection, and cyber controls.
Access-control layer	User database, credential rules, schedules, door groups, unlock logic, anti-passback policy, face or card workflows, and access-event metadata.
Recording layer	NVR or VMS storage, codec, bit rate, frame rate, retention period, snapshot capture, synchronized audio/video, playback, and export workflow.
Management layer	Client software, web access, CMS, mobile client, user permissions, event review, multi-site monitoring, notification policy, and system health management.
Response layer	Operator SOP, visitor approval, guard dispatch, emergency opening, maintenance ticketing, escalation, incident reporting, evidence export, and audit trail.

Architecture warning

A Door Station system can still underperform if the camera angle is wrong, audio is unclear, the credential workflow is incomplete, the lock wiring is unsuitable, the network drops, the recorder uses the wrong profile, or health alarms are not acted upon.

7. ACTi Product Portfolio Overview

ACTi positions Door Station and intercom-related solutions around entrance verification, access control, video recording, event management, and centralized operation. Public ACTi materials describe video intercom, high-definition video, two-way audio, remote door control, VMS integration, access-control events, notifications, search, playback, export, and device/system management. [1][2][3][4]

Portfolio categories

Category	Where it fits	Use-case fit
Outdoor video Door Stations	Entrances where visitors, employees, or deliveries need to call, be seen, speak, and request access from outside.	Main doors, gates, lobbies, loading docks, campus entrances
Indoor intercom stations	Interior locations where staff or residents answer calls, view visitors, and communicate with entrance-side devices.	Reception desks, security rooms, apartments, nursing stations
Access control readers and controllers	Credential validation and door hardware control where access policy must be enforced and logged.	Staff doors, restricted rooms, turnstiles, gates, equipment rooms
NVR/VMS and CMS platforms	Recording, live view, playback, investigation, multi-site monitoring, and video evidence management.	Control rooms, security operations, multi-building deployments
Notifications and mobile operation	Remote response when operators are away from a fixed workstation or when alerts must reach guards quickly.	After-hours entry, remote sites, small facilities, distributed campuses

Portfolio-level capabilities to confirm

- Required entrance type, outdoor/indoor installation, mounting height, viewing angle, audio environment, vandal-resistance need, and weather exposure.
 - Required credential method, door lock type, digital input/output, emergency release behavior, visitor management policy, and privacy requirements.
 - Recorder/VMS compatibility, bit rate, codec, retention, synchronized audio/video recording, playback, evidence export, CMS, remote access, and health monitoring.
 - Cybersecurity and compliance requirements such as secure transmission, account control, firmware policy, procurement restrictions, and regional availability.
 - Accessory compatibility, cabling, PoE budget, bracket or wall-box needs, installation space, maintenance access, and service response workflow.
- Project note**
Product availability, detailed specifications, compliance status, integration scope, accessory compatibility, recorder compatibility, and regional part numbers should be confirmed from the latest ACTi product pages, datasheets, release notes, installation guides, and quotation documents before project submission.

8. Related Keywords and Terminology

The following keyword reference groups collect common terms related to Door Station, video intercom, access control, entrance security, system architecture, and project procurement.

Core topic keywords

door station, video door station, IP door station, smart door station, network door station, entrance intercom, video intercom, access control intercom, visitor verification system, secure entrance management

Device and hardware keywords

touch button, call button, microphone, speaker, wide-angle camera, fisheye door camera, PIR sensor, RFID reader, door contact, digital input output, door lock relay, tamper detection, vandal-resistant enclosure

Access control keywords

RFID access control, face identification, credential verification, card access, mobile credential, visitor access, door unlock, request to exit, access event log, failed access attempt, door forced open, lock status

Video and audio keywords

high-definition video intercom, two-way audio, noise reduction, echo cancellation, low-light entrance camera, WDR entrance camera, IR illumination, visual verification, synchronized audio video recording

Software and integration keywords

access control server, VMS integration, NVR recording, CMS monitoring, SIP intercom, mobile client response, event notification, pop-up video verification, playback, search, evidence export, audit trail

Application keywords

office entrance security, residential video intercom, school visitor management, hospital access control, warehouse gate intercom, data center entrance control, loading dock visitor verification, lobby security system

Cybersecurity and reliability keywords

HTTPS, TLS, secure account management, firmware policy, VLAN, PoE switch, time synchronization, system health management, device status monitoring, uptime planning, maintenance workflow

Procurement and project keywords

door station specification, video intercom selection guide, access control camera white paper, camera for system integrators, camera for consultants, camera for end users, entrance security solution, ACTi Door Station

Common question phrases

what is a Door Station, when do I need a video Door Station, what is the difference between a Door Station and a video intercom, how to specify Door Stations for office entrances, how to integrate Door Stations with access control, how to record Door Station audio and video, how to manage visitor verification remotely, what Door Station features are important for schools, how to design entrance security for warehouses, how to connect a Door Station to door locks, how to search access events with video evidence, how to export entrance incident evidence, how to manage Door Station cybersecurity, how to monitor Door Station health remotely

Source notes

Ref.	Source
[1]	ACTi Corporation, "Door Station," official product category page. Accessed: June 29, 2026.
[2]	ACTi Corporation, "Intercom Service," official application page. Accessed: June 29, 2026.
[3]	ACTi Corporation, "Access Control," official product category page. Accessed: June 29, 2026.
[4]	ACTi Corporation, "Access Control Solution," official solution page. Accessed: June 29, 2026.
[5]	ACTi Corporation, "Service Desk Cameras," official product category page. Accessed: June 29, 2026.
[6]	ACTi Corporation, "About ACTi," official corporate page. Accessed: June 29, 2026.

Revision note

This document is a marketing and technical education white paper. It is not a regulatory certification, electrical design, life-safety design, fire-code interpretation, privacy assessment, or final project design. Always validate door hardware, lock power, emergency egress, fire-safety requirements, privacy rules, cybersecurity policy, field of view, lighting, audio environment, recording settings, storage, VMS control, access-control rules, system health monitoring, maintenance access, and operator workflow in the target scene before deployment.

Prepared by ACTi Corporation

For Door Station projects, confirm form factor selection, access-control requirements, door hardware, materials, lighting, recording platform, compliance requirements, mounting accessories, and regional availability with your ACTi sales contact or authorized system integrator.

sales@acti.com | www.acti.com