

APPLICATION WHITE PAPER

INDUSTRIAL EDGE NETWORKING FOR MODERN AIRPORTS

*Reference Architecture for Airport Perimeter Security, Airfield Operations,
Remote Apron Monitoring and Connected Infrastructure*

CONNECT / PROTECT / UNDERSTAND



Avcomm Technologies

Industrial Networking for Connected Airport Operations

Contents

This white paper presents a flexible reference architecture for resilient, secure and manageable industrial edge networking across modern airport environments.

CHAPTER 1 • Why Airport Edge Networks Matter

- 1.1 Airports Are Distributed Operational Environments
- 1.2 More Cameras, Higher Resolution and Wider Coverage
- 1.3 Public Operations and Public Safety Depend on Connectivity
- 1.4 Operational Technology Is Moving to Ethernet
- 1.5 Industrial Switches Bring Managed Connectivity to the Edge
- 1.6 Edge Networking Improves Lifecycle Management

CHAPTER 2 • Typical Airport Systems and Edge-Network Applications

- 2.1 Airport Perimeter Security
- 2.2 Video Surveillance and Video-Management Systems
- 2.3 Remote Apron and Aircraft-Stand Monitoring
- 2.4 Airfield Lighting and Visual Guidance
- 2.5 Weather and Environmental Monitoring
- 2.6 Emergency Communications, Intercom and Public Address
- 2.7 Access Control and Airport Gates
- 2.8 Baggage-Handling and Smart Baggage Systems
- 2.9 Airport Utilities and Building Infrastructure
- 2.10 Parking, Roadway and Landside Transportation
- 2.11 Wireless, IoT and Mobile Operations

CHAPTER 3 • Common Airport Network Challenges

- 3.1 Migrating from Fieldbus and Point-to-Point Links
- 3.2 Fiber Distance and Geographic Dispersion
- 3.3 Network Redundancy
- 3.4 Outdoor Cabinets and Limited Installation Space
- 3.5 Harsh Environmental Conditions
- 3.6 From Unmanaged Hubs to Managed Layer 2 and Layer 3 Networks
- 3.7 Visibility and Maintenance
- 3.8 Segmentation and Cybersecurity
- 3.9 Connecting More Devices Without Creating a Flat Network
- 3.10 Integration Creates Value—but Also Responsibility

CHAPTER 4 • Airport Industrial Edge Network Reference Architecture

- 4.1 Architectural Principles
- 4.2 High-Level Reference Architecture
- 4.3 Perimeter Security Edge Node
- 4.4 Remote Apron Monitoring Edge Node
- 4.5 Baggage and Automation Edge Network
- 4.6 Topology Options

CHAPTER 5 • Proven Airport Deployment Experience

- 5.1 Airport Experience Developed Through Asia's Digital Aviation Expansion
- 5.2 From Optical Transceivers to Managed Industrial Ethernet
- 5.3 Airport Perimeter and Airfield Applications

- 5.4 Regional Airports and Cost-Effective Modernization
- 5.5 ATMS: Connecting Networks, Devices and Operational Workflows
- 5.6 Lessons Learned from Airport Deployments

CHAPTER 6 • Modernizing Existing Airport Systems and Preparing for the Future

- 6.1 The Immediate Opportunity Is Modernization
- 6.2 Video-System Modernization
- 6.3 Replacing Standalone Optical Transceivers
- 6.4 Upgrading Unmanaged Field Networks
- 6.5 Adding Network Intelligence at the Edge
- 6.6 Network Visibility as a Primary Design Requirement
- 6.7 Preparing for AI and Data-Driven Operations
- 6.8 An AI-Ready Airport Edge Architecture

CHAPTER 7 • Selecting Industrial Ethernet for Airport Applications

- 7.1 Environmental Requirements
- 7.2 Physical Installation
- 7.3 Port and Bandwidth Planning
- 7.4 Redundancy
- 7.5 Network Management
- 7.6 Cybersecurity
- 7.7 Integration and Interoperability

CHAPTER 8 • Avcomm Airport Edge Networking

- Connect
- Protect
- Understand
- About Avcomm

Executive Summary

Airports are becoming increasingly distributed, connected and data-intensive.

High-definition and thermal cameras are being deployed across perimeter fences, remote aprons, aircraft stands, service roads, gates, parking facilities, utility buildings and other locations far beyond the controlled environment of the terminal data center. At the same time, airports are connecting weather sensors, visual docking guidance systems, airfield lighting controls, emergency communications, access-control equipment, baggage systems, environmental sensors and other operational technologies through Ethernet-based networks.

These systems serve different departments and operational purposes, but they share several infrastructure requirements:

- Reliable communication over long distances;
- Support for geographically dispersed field devices;
- Operation inside outdoor or semi-outdoor cabinets;
- Resistance to heat, cold, humidity, dust, vibration and electrical disturbances;
- Network redundancy and rapid recovery from fiber or equipment failures;
- Secure separation of different airport applications;
- Centralized visibility and maintenance;
- A practical migration path from legacy fieldbus, serial links and optical transceivers to manageable Ethernet infrastructure.

Traditional enterprise switches remain essential in airport data centers, communication rooms and terminal buildings. However, many airport edge locations cannot provide the controlled temperature, space, power quality and maintenance conditions expected by conventional IT equipment.

Industrial Ethernet switches fill this gap.

Installed near cameras, controllers, sensors and operational equipment, industrial switches provide compact DIN-rail connectivity, multiple copper and fiber ports, redundant power inputs, hardened construction and centralized management. VLANs can separate security, operations, communications and maintenance traffic while allowing multiple systems to share a carefully governed physical network.

The purpose of this white paper is not to prescribe one universal network topology. Every airport has its own security program, technology standards, funding requirements, operational priorities and existing infrastructure. Instead, this paper presents a flexible airport edge-network reference architecture that can be adapted to:

- Large international hub airports;
- Medium and regional commercial airports;
- General aviation airports;
- Cargo airports;
- Remote apron and aircraft-stand projects;
- Perimeter modernization programs;
- Existing video-system upgrades;
- New airport developments and terminal expansions.

The architecture preserves the airport's existing video-management, access-control, emergency-communication and enterprise platforms. Industrial Ethernet is positioned as the resilient edge infrastructure that connects distributed devices to those systems.

CHAPTER 1

Why Airport Edge Networks Matter

1.1 Airports Are Distributed Operational Environments

An airport is not a single building.

It is a geographically distributed operating environment that may include:

- Passenger terminals;
- Runways and taxiways;
- Aircraft aprons and remote stands;
- Perimeter fences and access gates;
- Airfield lighting vaults;
- Baggage-handling facilities;
- Cargo areas;
- Fuel farms;
- Maintenance, repair and overhaul facilities;
- Parking structures and roadways;
- Fire stations;
- Utility plants;
- Weather stations;
- Communications shelters;
- Remote equipment cabinets.

Devices installed across these areas must communicate with airport operations centers, security operations centers, maintenance teams, airline systems and specialized operational platforms.

Many endpoints are located several hundred meters—or several kilometers—from the nearest communication room. Others are installed in areas where constructing a conventional telecommunications room would be impractical or uneconomical.

This creates a distinct airport edge-network requirement.

The edge network must extend managed connectivity from protected airport facilities to remote field locations while preserving availability, security, performance and operational visibility.

1.2 More Cameras, Higher Resolution and Wider Coverage

Airport video surveillance is expanding in both scale and purpose.

Cameras are no longer limited to passenger terminals and security checkpoints. They are increasingly deployed to support:

- Airport perimeter surveillance;
- Restricted-area monitoring;
- Vehicle-gate verification;
- Remote apron observation;
- Aircraft-stand monitoring;
- Ground-service-equipment supervision;
- Service-road monitoring;
- Cargo and baggage security;
- Parking and roadway management;
- Operational incident investigation;
- Wildlife and foreign-object observation;
- Fire and emergency response;
- Construction-area monitoring.

Modern installations increasingly use high-definition, multi-sensor, panoramic, PTZ and thermal cameras. These devices generate significantly more traffic than earlier analog or standard-definition systems.

Unlike terminal cameras, many airfield cameras are installed at widely separated and unattended locations. They may be mounted on:

- Perimeter poles;
- Lighting towers;
- Remote aircraft stands;
- Utility buildings;
- Airfield gates;
- Equipment shelters;
- Roadside cabinets;

- Temporary construction structures.

Consequently, airport video modernization is also a network modernization project.

Adding cameras without evaluating the edge network can produce:

- Oversubscribed uplinks;
- Excessive multicast or broadcast traffic;
- Unstable Power over Ethernet delivery;
- Unmanaged field switches;
- Single points of failure;
- Difficult troubleshooting;
- Inadequate cybersecurity segmentation;
- Limited visibility into remote device status.

The network therefore needs to be planned as part of the video system—not as an incidental accessory.

1.3 Public Operations and Public Safety Depend on Connectivity

Airport networks support both routine operations and safety-related functions.

Examples include:

- Monitoring access to secured and restricted areas;
- Coordinating airport operations and police response;
- Observing remote stands and ground-handling activities;
- Delivering emergency communications;
- Monitoring utilities and environmental conditions;
- Collecting equipment alarms;
- Supporting gate, roadway and parking operations;
- Providing operational awareness during severe weather;
- Preserving video and event records for investigation.

In the United States, airport security requirements are generally risk- and performance-based. Federal regulations and airport security programs define required security outcomes, while individual airports determine how technologies such as fencing, access control, surveillance and intrusion detection will be implemented.

TSA guidance recognizes intrusion-detection technologies as increasingly relevant to airport security and encourages airports to select measures according to risk, airport characteristics and operational conditions.

This approach creates opportunities for flexible architecture, but it also places greater responsibility on the airport and its designers to select infrastructure that is maintainable, defensible and compatible with the airport's existing systems.

1.4 Operational Technology Is Moving to Ethernet

Airport field systems historically used many communication methods:

- Dry contacts;
- Proprietary fieldbus;
- RS-232;
- RS-422;
- RS-485;
- Analog video;
- Dedicated optical transceivers;
- Standalone controller networks;
- Point-to-point fiber links.

These technologies remain in service, and some will continue to be appropriate. However, new airport systems increasingly use Ethernet because it provides:

- Higher bandwidth;
- Standardized interfaces;
- Easier integration;
- Greater device visibility;

- Remote diagnostics;
- Centralized management;
- Flexible physical media;
- Support for IP video and audio;
- A practical foundation for future analytics.

Typical Ethernet-connected airport edge devices include:

- IP cameras;
- Thermal cameras;
- Video encoders;
- Perimeter-intrusion sensors;
- Gate controllers;
- Intercoms and emergency phones;
- Weather sensors;
- Visual docking guidance systems;
- Airfield-lighting interfaces;
- PLCs and remote I/O;
- Environmental monitors;
- Intelligent power systems;
- Baggage-handling controllers;
- Wireless access points;
- Vehicle and asset-tracking gateways;
- Edge-computing devices.

The transition to Ethernet does not mean that every airport system should be placed on one flat network.

Instead, Ethernet provides a common transport technology on which separate business and operational domains can be securely established.

1.5 Industrial Switches Bring Managed Connectivity to the Edge

A field location may need to connect several devices:

Thermal camera

Fixed camera

PTZ camera

Gate controller

Intercom

Perimeter sensor

Cabinet environmental sensor

Wireless or IoT gateway

Installing an individual fiber converter for every device can create a collection of isolated links with limited diagnostic capability. An industrial Ethernet switch consolidates these devices into a managed field node.

A managed industrial switch can provide:

- Multiple Ethernet access ports;
- Fiber uplinks;
- PoE or PoE+;
- Redundant power inputs;
- VLAN segmentation;
- Quality of Service;
- Multicast management;
- Port-level security;
- Network redundancy;
- SNMP monitoring;

- Syslog reporting;
- Link and power alarms;
- Optical-module diagnostics;
- Remote port control.

This makes it possible to connect multiple systems locally while maintaining logical separation.

For example:

VLAN 110 – Video surveillance

VLAN 120 – Perimeter detection

VLAN 130 – Access control

VLAN 140 – Intercom and communications

VLAN 150 – Maintenance and cabinet monitoring

The physical fiber infrastructure may be shared where permitted, while the traffic remains logically separated and governed by airport cybersecurity policy.

1.6 Edge Networking Improves Lifecycle Management

A large airport may have hundreds or thousands of field endpoints. The long-term cost of these systems is not determined only by installation cost. It is also determined by:

- How quickly faults can be located;
- Whether technicians can identify the failed device remotely;
- Whether fiber quality can be monitored;
- Whether PoE delivery can be diagnosed;
- Whether configuration changes are documented;
- Whether spare parts are standardized;
- Whether network events are centrally recorded;
- Whether the airport can expand the system without redesigning it.

An unmanaged network may function on the day it is commissioned but become difficult to maintain as devices are added and systems evolve.

A managed airport edge network provides a foundation for lifecycle management.

CHAPTER 2

Typical Airport Systems and Edge-Network Applications

There is no single universal airport-network design. U.S. airports commonly maintain separate or logically segmented networks for enterprise IT, security, access control, emergency communications, building systems and operational technologies.

Denver International Airport’s published design standards, for example, describe a dedicated Security Access Control Network as well as separate communication architectures for other airport systems. The standards also show that IP cameras may connect through the airport enterprise network or dedicated security infrastructure, depending on their function.

The following systems represent important current and emerging applications for industrial edge networking.

2.1 Airport Perimeter Security

The airport perimeter forms a physical and operational boundary between controlled airport property and surrounding public areas.

A modern perimeter system may include:

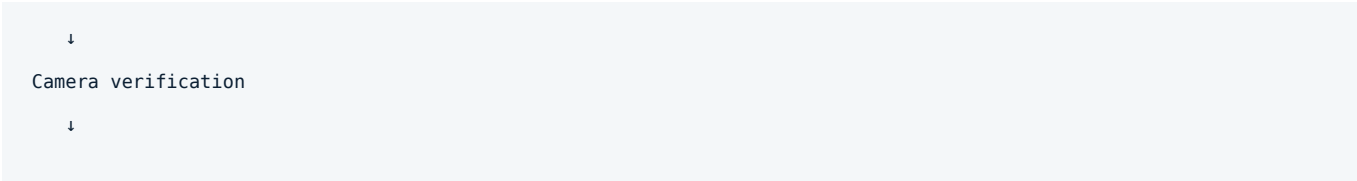
- Security fencing;
- Vehicle and personnel gates;
- Fixed cameras;
- PTZ cameras;
- Thermal cameras;
- Fence-mounted intrusion sensors;
- Fiber-optic sensing;
- Radar or microwave detection;
- Video analytics;
- Lighting;
- Intercoms;
- Access-control readers;
- Cabinet alarms;
- Emergency communications.

The objective is not simply to record video. It is to support a complete event workflow:

Detection



Alarm location



Operator assessment



Dispatch and response

↓

Event recording and review

Industrial Ethernet switches can serve as resilient field aggregation points for groups of perimeter devices.

Depending on airport standards and geography, the network may use:

- Point-to-point fiber;
- Dual-homed star connections;
- A redundant fiber ring;
- A combination of ring and star segments;
- Fiber from individual devices to a centralized communications room.

The correct topology is determined by the airport's available fiber, criticality, physical layout, recovery objectives and cybersecurity policy.

2.2 Video Surveillance and Video-Management Systems

Airport video systems support security, operations, emergency response and investigation.

A U.S. airport project will commonly require new cameras to integrate with an established video-management system rather than operate as an isolated project platform.

Port Authority of New York and New Jersey airport guidelines emphasize integrating new surveillance coverage with the airport's existing security environment and coordinating camera views and operational access with airport security stakeholders.

The edge network must therefore support:

- Airport-approved camera models;
- Required resolution and frame rates;
- VMS integration;
- Video multicast or unicast strategy;
- Defined retention and storage architecture;
- Network bandwidth calculations;
- Camera and switch cybersecurity;
- Time synchronization;
- Event-triggered recording;
- Health monitoring;
- Controlled access to live and recorded video.

The industrial switch does not replace the VMS. It provides the reliable field transport that allows the approved VMS to reach distributed cameras.

2.3 Remote Apron and Aircraft-Stand Monitoring

Remote aprons and aircraft stands are operationally complex areas.

They may involve:

- Aircraft arrival and departure;
- Passenger boarding;
- Baggage loading;
- Cargo handling;
- Catering;
- Refueling;
- Ground-power equipment;
- Pushback tractors;
- Maintenance vehicles;
- Security personnel;

- Ramp-control coordination.

Video and sensor coverage can improve awareness of:

- Stand occupancy;
- Unauthorized personnel or vehicles;
- Ground-service activities;
- Aircraft-door and service-zone events;
- Equipment left within safety areas;
- Delays in ground handling;
- Damage or safety incidents;
- Emergency situations.

Remote apron monitoring may connect:

- Multiple IP cameras;
- PTZ cameras;
- Thermal cameras;
- Visual docking guidance systems;
- Intercoms;
- Environmental sensors;
- Wireless access points;
- Edge analytics;
- Equipment-status gateways.

Because these systems are distributed and often exposed to outdoor conditions, remote aprons are a strong application for compact industrial switches with fiber uplinks and optional PoE.

2.4 Airfield Lighting and Visual Guidance

Airfield systems may include:

- Runway and taxiway lighting;
- Approach lighting;
- Stop bars;
- Guidance signs;
- Lighting-control and monitoring systems;
- Constant-current regulators;
- Field electrical vaults;
- Remote-control cabinets;
- Visual docking guidance systems.

Safety-critical airfield-lighting systems should follow their approved control architecture and relevant aviation standards. Industrial Ethernet should not be presented as a replacement for certified safety controls unless it is specifically designed and approved for that function.

However, Ethernet may support:

- Supervisory communication;
- Status monitoring;
- Maintenance diagnostics;
- Environmental monitoring;
- Video observation;
- Connections between control facilities;
- Integration with airport operations platforms.

The network design must distinguish between operational control, supervisory monitoring and general data access.

2.5 Weather and Environmental Monitoring

Airport weather and environmental systems can include:

- Wind sensors;

- Visibility sensors;
- Temperature and humidity;
- Precipitation monitoring;
- Lightning detection;
- Pavement-temperature sensors;
- Runway surface condition monitoring;
- Air-quality sensors;
- Noise-monitoring stations;
- Flood and drainage monitoring.

These devices are frequently installed in remote and exposed locations.

Industrial edge networking can provide:

- Fiber extension;
- Serial-to-Ethernet integration;
- Managed communication;
- Redundant uplinks;
- Remote diagnostics;
- Cabinet power and temperature monitoring.

Weather information may be consumed by multiple systems, but access must be governed so that monitoring or data-distribution functions do not interfere with certified aviation weather systems.

2.6 Emergency Communications, Intercom and Public Address

Airport communications may include:

- Passenger public address;
- Gate announcements;
- Operations announcements;
- Security intercom;
- Emergency telephones;
- Fire-alarm voice evacuation;
- Mass notification;
- Emergency communication systems.

These functions should not automatically be treated as one common system.

Life-safety communication is subject to stricter requirements for:

- Availability;
- Priority;
- Supervision;
- Backup power;
- Amplifier monitoring;
- Fire-code compliance;
- Message zoning;
- Emergency override;
- Testing and commissioning.

Published U.S. airport design guidance commonly requires public-address coverage to be coordinated with security and emergency operations. Port Authority guidelines address public-address and video coverage as integrated elements of airport security planning.

Where IP audio is used, the network may need:

- QoS;
- Multicast control;
- IGMP Snooping;
- IGMP Querier;
- Rapid redundancy;
- Accurate time;

- Network supervision;
- Segmentation from noncritical traffic.

Industrial switches may support the field transport, provided the complete system—including life-safety behavior—complies with the airport's approved design and applicable codes.

2.7 Access Control and Airport Gates

Airport access-control systems may serve:

- Secure doors;
- Air Operations Area gates;
- Vehicle gates;
- Personnel turnstiles;
- Tenant areas;
- Maintenance facilities;
- Utility buildings;
- Remote equipment enclosures.

Field devices may include:

- Card readers;
- Biometric readers;
- Door controllers;
- Gate PLCs;
- Intercoms;
- Cameras;
- License-plate-recognition cameras;
- Loop detectors;
- Traffic signals;
- Gate-status sensors.

At large airports, access control frequently operates over a dedicated security network or tightly controlled segment.

The industrial edge network must support the approved security architecture without introducing unauthorized bridging between airport networks.

2.8 Baggage-Handling and Smart Baggage Systems

Baggage-handling systems are among the most operationally important automation systems in an airport.

A modern baggage environment can include:

- Conveyor control;
- PLCs;
- Motor-control interfaces;
- Barcode readers;
- RFID readers;
- Bag tag printers;
- Explosive-detection interfaces;
- Tracking sensors;
- Diverters;
- Early bag storage;
- Baggage reconciliation;
- Control-room servers;
- Maintenance workstations;
- Video monitoring.

Smart baggage initiatives increase the amount of data generated across the baggage journey.

Industrial Ethernet can support:

- Deterministic and reliable controller communication;

- Segmented automation networks;
- Fiber uplinks between baggage areas;
- Managed multicast;
- Device diagnostics;
- Redundant network paths;
- Integration gateways to baggage-management and airline systems.

Because baggage systems combine operational technology and enterprise data, their architecture should clearly separate:

- Machine control;
- Safety control;
- Supervisory control;
- Tracking data;
- Video;
- Maintenance access;
- Airline and airport interfaces.

2.9 Airport Utilities and Building Infrastructure

Airports operate utility systems similar to those of a small city:

- Electrical distribution;
- Central utility plants;
- Chilled and hot water;
- Water and wastewater;
- Fuel systems;
- Stormwater systems;
- Tunnel ventilation;
- Pump stations;
- Fire-water systems;
- Building automation;
- Elevators and escalators;
- Facility energy management.

Industrial switches can connect controllers and monitoring devices in plant rooms, tunnels, outdoor cabinets and utility buildings.

These applications are often suitable early entry points for industrial Ethernet suppliers because they are operationally important but may be less restricted than core airport security networks.

2.10 Parking, Roadway and Landside Transportation

Airport roadway and parking systems may include:

- Parking guidance;
- License-plate recognition;
- Tolling and revenue control;
- CCTV;
- Dynamic message signs;
- Traffic counters;
- Signal controllers;
- Emergency call stations;
- Shuttle tracking;
- Curbside-management sensors;
- Electric-vehicle charging infrastructure.

These systems are geographically distributed and frequently use outdoor cabinets, making them natural industrial-network applications.

2.11 Wireless, IoT and Mobile Operations

Airports are increasing their use of:

- Wi-Fi;
- Private cellular networks;
- LoRaWAN;
- Vehicle communications;
- Asset tracking;
- Mobile maintenance tools;
- Robotics;
- Drones;
- Temporary construction networks.

Wireless systems still depend on wired backhaul, power and network management.

Industrial switches can provide hardened backhaul for access points, gateways and edge-computing devices deployed outside conventional terminal IT spaces.

CHAPTER 3

Common Airport Network Challenges

3.1 Migrating from Fieldbus and Point-to-Point Links

Many existing airport systems were constructed as independent subsystems.

A typical legacy arrangement may contain:

```
Camera → Optical transceiver → Fiber → Optical transceiver → Recorder
PLC → Serial converter → Fiber modem → Control room
Intercom → Dedicated copper pair
Sensor → Proprietary fieldbus
```

This architecture can be stable, but it has limitations:

- Each application needs dedicated transmission equipment;
- Bandwidth is difficult to expand;
- Fault location is often manual;
- Devices cannot be centrally inventoried;
- Spare-parts requirements multiply;
- Integration between systems becomes difficult;
- New analytics require additional infrastructure.

Migration to Ethernet allows several services to use a managed communication platform while preserving application-level separation.

A migration strategy may include:

1. Retaining functional legacy devices;
2. Introducing serial or fieldbus gateways where appropriate;
3. Replacing unmanaged optical transceivers with managed industrial switches;
4. Creating VLANs for each operational domain;
5. Establishing redundant fiber paths;
6. Integrating alarms into network-management or IoT platforms;
7. Gradually modernizing field endpoints.

The objective is not to replace every legacy device immediately. It is to build an infrastructure that makes phased modernization possible.

3.2 Fiber Distance and Geographic Dispersion

Copper Ethernet is generally limited to approximately 100 meters per channel under standard structured-cabling design.

Airport field devices may be located much farther away.

Single-mode fiber therefore becomes a fundamental airport edge medium because it provides:

- Long transmission distance;
- Electrical isolation;
- High bandwidth;
- Resistance to electromagnetic interference;
- Support for future expansion.

However, fiber distance alone does not solve the network problem.

The design must also consider:

- Fiber-path diversity;
- Available strand count;
- Patch-panel design;
- Splicing and maintenance;
- Optical power budget;
- SFP temperature rating;
- Connector contamination;
- Fiber-ring failure domains;
- Identification and documentation;
- Expansion capacity.

A managed switch with SFP diagnostics can provide visibility into:

- Transmit power;
- Receive power;
- Module temperature;
- Module voltage;
- Link status.

This allows deteriorating optical conditions to be identified before a complete failure occurs.

3.3 Network Redundancy

A single fiber cut can isolate an entire remote area if the network has only one path.

Possible redundancy strategies include:

Point-to-point with redundant fibers

Each important edge node has two independent uplinks to separate upstream switches.

Dual-homed star

The edge switch connects to two distribution points.

Redundant fiber ring

Field switches form a ring, allowing traffic to use an alternate direction after a link failure.

Parallel or segmented rings

Large geographical areas are divided into smaller rings to reduce fault domains.

Layer 3 routed edge

Routing is extended toward the edge to contain Layer 2 domains and improve scalability.

No topology is universally superior.

A ring may reduce fiber requirements and perform well along a linear perimeter. A dual-homed star may provide clearer failure isolation. A routed architecture may improve segmentation and scalability but require greater design and operational expertise.

The airport should define:

- Required recovery time;
- Maximum affected area;
- Permitted protocols;
- Failure scenarios;
- Maintenance procedures;
- Testing requirements.

Rapid redundancy is especially valuable for video, access control and operational monitoring, but it must be implemented in a way that is compatible with the airport's wider network standards.

3.4 Outdoor Cabinets and Limited Installation Space

Airport field cabinets are rarely equivalent to enterprise communication rooms.

Typical constraints include:

- Limited width and depth;
- Existing power supplies;
- No air conditioning;
- Difficult access;
- Shared space with controllers and electrical devices;
- DIN-rail mounting requirements;
- Restricted ventilation;
- High solar loading;
- Condensation risk;
- Limited maintenance clearances.

Industrial switches are designed for these conditions through features such as:

- Compact form factor;
- DIN-rail mounting;
- Metal enclosure;
- Fanless design;
- Redundant DC power inputs;
- Wide operating temperature;
- Terminal-block power connections;
- Relay alarms;
- Industrial grounding.

Physical design matters as much as port count.

A technically capable switch may still be unsuitable if it cannot fit safely inside the approved cabinet or if its power and thermal requirements exceed available capacity.

3.5 Harsh Environmental Conditions

Airport edge equipment may experience:

- High summer temperatures;
- Freezing conditions;
- Rapid temperature change;
- Humidity and condensation;
- Dust;
- Wind-driven rain entering damaged cabinets;
- Vibration;
- Lightning-induced surges;
- Electrical transients;
- Electromagnetic interference;
- Poor power quality.

The complete system must be engineered—not only the switch.

Important elements include:

- Cabinet ingress protection;
- Proper grounding and bonding;
- Surge-protection devices;
- Fiber isolation;
- Industrial power supplies;
- Redundant power sources;
- Cabinet ventilation or heating;
- Cable separation;

- Shielding strategy;
- Environmental monitoring.

An industrial switch increases tolerance to field conditions, but it does not eliminate the need for correct cabinet and electrical design.

3.6 From Unmanaged Hubs to Managed Layer 2 and Layer 3 Networks

Early field networks often used:

- Ethernet hubs;
- Unmanaged switches;
- Media converters;
- Flat Layer 2 networks.

As airports connect more devices and applications, these approaches become difficult to operate.

Modern edge networks increasingly require:

- VLANs;
- QoS;
- Link aggregation;
- Multicast management;
- Loop prevention;
- Redundancy;
- Access-control lists;
- Layer 3 routing;
- DHCP protection;
- Secure management;
- Central logging.

A key architectural transition is moving selected networking intelligence closer to the edge.

This does not mean that every field switch needs full enterprise routing capability. It means that edge designs should be selected according to the scale and risk of the application.

A simple camera cabinet may require managed Layer 2 switching. A multi-system remote facility may benefit from Layer 3 segmentation and local routing.

3.7 Visibility and Maintenance

A remote node may contain several connected devices. When a camera disappears from the VMS, the actual cause could be:

- Camera failure;
- PoE failure;
- Copper cable damage;
- Switch-port shutdown;
- Fiber loss;
- SFP degradation;
- Switch power failure;
- Cabinet overheating;
- Upstream configuration error.

Without network visibility, a technician may need to travel across the airport simply to determine which component failed.

A managed system should provide:

- Device inventory;
- Topology discovery;
- Link status;
- Port utilization;
- PoE status;

- Optical diagnostics;
- Power alarms;
- Temperature alarms;
- Event logs;
- Configuration backup;
- Firmware records;
- Geographic or map-based device location.

The operational value of industrial Ethernet is therefore not limited to data transmission. It includes faster diagnosis and more efficient maintenance.

3.8 Segmentation and Cybersecurity

The availability of a physical port should never imply unrestricted network access.

Airport edge networks need controlled segmentation between:

- Video;
- Access control;
- emergency communications;
- Baggage automation;
- Building systems;
- Maintenance;
- Wireless infrastructure;
- Enterprise applications.

Relevant controls may include:

- VLANs;
- Layer 3 access-control lists;
- Firewalls;
- 802.1X;
- RADIUS or TACACS+;
- SSH and HTTPS;
- SNMPv3;
- Role-based administration;
- Disabled unused ports;
- Configuration audit;
- Central syslog;
- Firmware and vulnerability management.

The U.S. TSA has emphasized cybersecurity resilience for airport and aircraft operators, including network segmentation, access control, monitoring and incident response.

Network security cannot be added only at the core. Field switches and connected devices must be included in the airport's cybersecurity lifecycle.

3.9 Connecting More Devices Without Creating a Flat Network

As more airport systems use IP, there is a temptation to connect everything to the nearest available switch.

This can create a large, poorly controlled Layer 2 domain.

A better approach is to ask:

- Who owns each device?
- Which system consumes its data?
- Which other systems may access it?
- What traffic must be blocked?
- What is the required availability?
- What happens if the device is compromised?
- Which department manages the switch?
- How is the configuration documented?

A well-designed industrial edge node can connect devices from multiple airport applications, but only when physical sharing is permitted and logical separation is clearly defined.

3.10 Integration Creates Value—but Also Responsibility

Connecting cameras, sensors, gates, intercoms and operational equipment creates opportunities for:

- Unified alarm presentation;
- Video verification;
- Geographic event display;
- Automated workflows;
- Maintenance analytics;
- Asset tracking;
- Operational dashboards;
- AI-assisted diagnostics.

However, integration must not create uncontrolled dependency.

The architecture should preserve:

- System ownership;
- Safety boundaries;
- Cybersecurity zones;
- Authoritative data sources;
- Manual fallback procedures;
- Audit trails;
- Vendor support responsibilities.

The edge network should enable integration without obscuring accountability.

CHAPTER 4

Airport Industrial Edge Network Reference Architecture

4.1 Architectural Principles

The proposed architecture follows seven principles:

8. Preserve existing airport platforms.

The architecture extends the airport’s approved VMS, access-control, emergency-communication and operational systems rather than replacing them unnecessarily.

9. Move hardened connectivity closer to field devices.

Industrial switches are placed in remote cabinets, utility buildings and operational areas where enterprise equipment may not be suitable.

10. Use fiber for distance and electrical isolation.

11. Separate systems logically.

VLANs, routing and security controls prevent the edge network from becoming a flat shared environment.

12. Design redundancy according to operational criticality.

13. Provide centralized visibility.

14. Allow phased modernization.

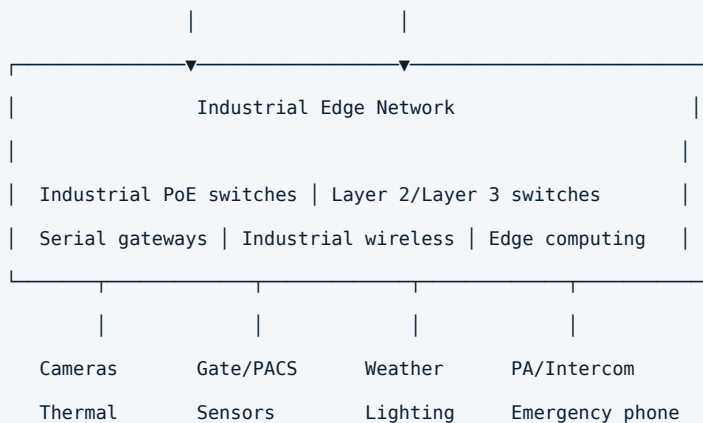
Legacy devices may remain in operation through gateways while new IP devices are added.

4.2 High-Level Reference Architecture





Redundant fiber Point-to-point fiber



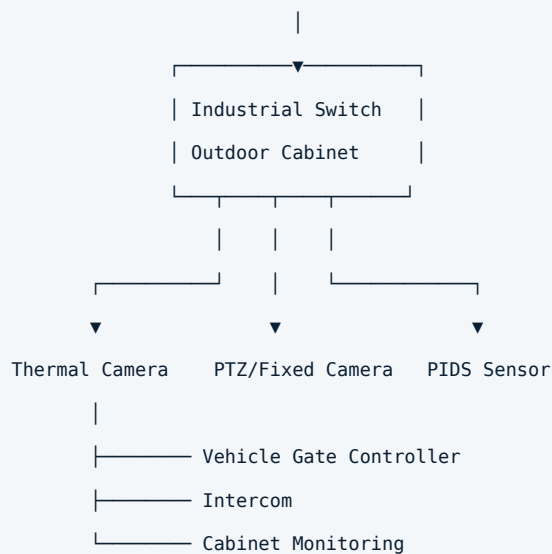
Analytics Controllers Utilities Wireless/IoT

4.3 Perimeter Security Edge Node

Airport Security Network



Redundant single-mode fiber



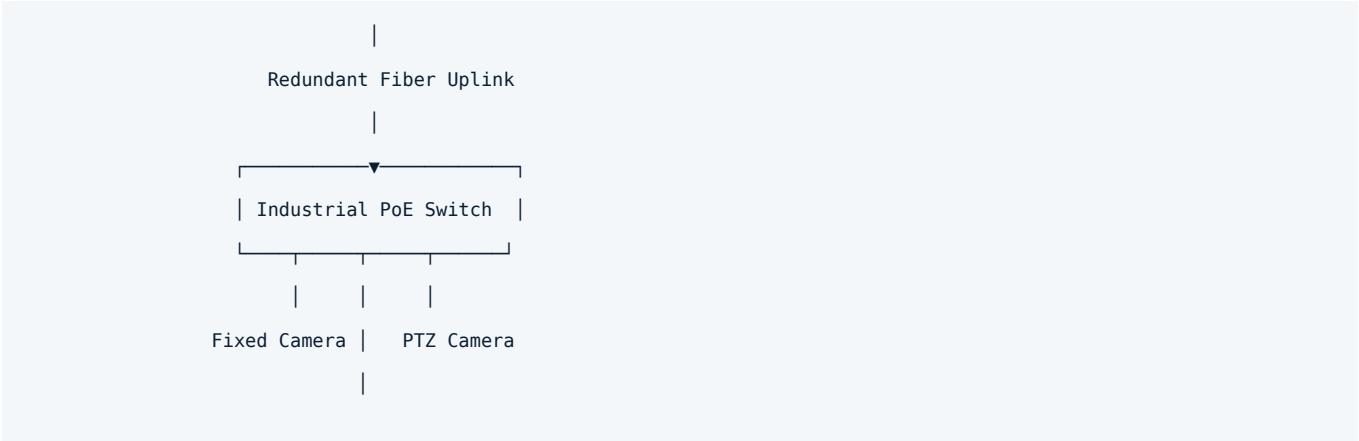
Recommended considerations:

- Two independent power inputs where practical;
- PoE budget calculated under low-temperature startup conditions;

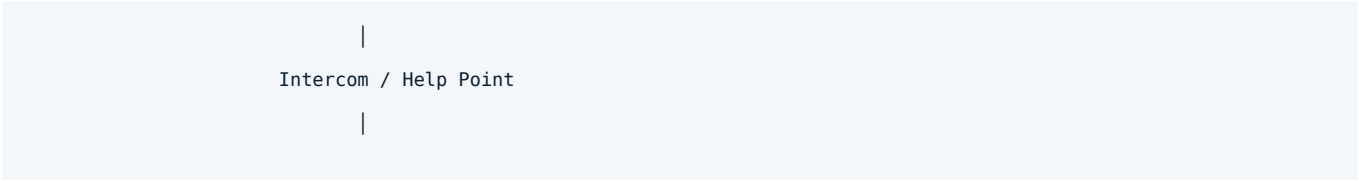
- Single-mode SFPs rated for the cabinet environment;
- VLAN separation between video, intrusion detection and maintenance;
- Rapid recovery after fiber failure;
- Central SNMP and syslog;
- Cabinet-open and temperature alarms;
- Disabled unused ports;
- Secure local and remote administration.

4.4 Remote Apron Monitoring Edge Node

Airport Operations Network



VDG/Stand Interface



Wireless Access Point



Edge Analytics Device

The remote apron design should consider:

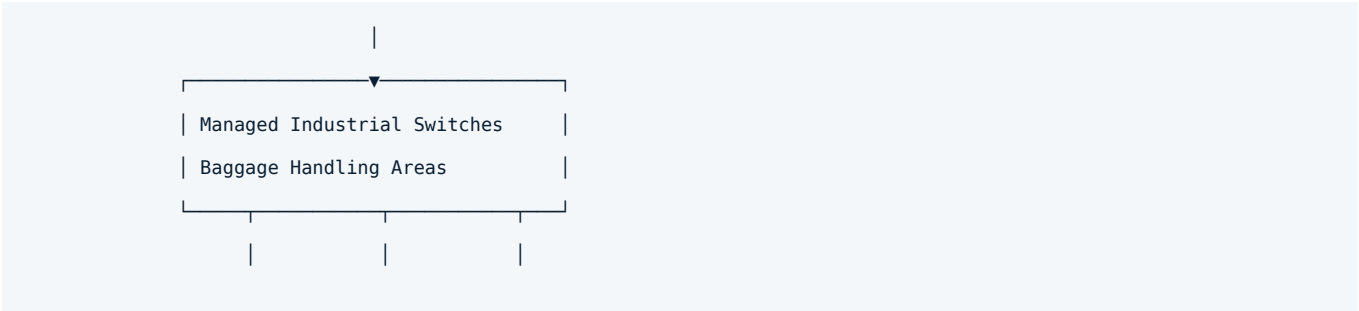
- Expected simultaneous video streams;
- Camera bitrate under low-light and high-motion conditions;
- PoE budget;
- Stand expansion;
- Local cabinet power;
- Fiber-path diversity;
- Whether analytics run centrally or at the edge;
- Interfaces to VMS and airport operations platforms.

4.5 Baggage and Automation Edge Network

Airport Operational Technology Core



Redundant Distribution



PLC Barcode/RFID HMI



Remote I/O Tracking gateway



Motor-control interface

Key design requirements may include:

- Segmentation between controls and business systems;
- Redundancy appropriate to baggage operational requirements;
- Multicast and QoS control;
- Controlled engineering access;
- Configuration backup;
- Time synchronization;
- Compatibility with approved PLC and controller protocols.

4.6 Topology Options

Option A: Redundant fiber ring

Best suited to:

- Linear perimeter routes;
- Tunnels;
- Service roads;
- Distributed lighting or utility nodes;
- Environments with limited available fiber.

Advantages:

- Efficient fiber utilization;
- Alternate path after a link failure;
- Natural alignment with perimeter geography.

Considerations:

- Failure-domain size;
- Ring protocol compatibility;
- Recovery time;
- Maximum nodes;
- Maintenance practices.

Option B: Dual-homed star

Best suited to:

- Critical facilities;
- Locations with fiber-path diversity;
- Airports preferring centralized Layer 2 or Layer 3 design.

Advantages:

- Clear failure isolation;
- Independent uplinks;
- Flexible routing and segmentation.

Considerations:

- Greater fiber requirements;
- Distribution-switch capacity;
- Duct and pathway availability.

Option C: Point-to-point fiber

Best suited to:

- Individual high-value cameras;
- Isolated gates;
- Small facilities;
- Projects requiring simple operational ownership.

Advantages:

- Simple topology;
- Limited shared failure impact.

Considerations:

- Fiber consumption;
- Additional transceivers;
- Limited local aggregation.

Option D: Routed industrial edge

Best suited to:

- Large multi-system remote facilities;
- Campuses with many VLANs;
- Projects requiring smaller broadcast domains.

Advantages:

- Improved scalability;
- Better fault containment;
- Policy enforcement closer to devices.

Considerations:

- Greater configuration complexity;
- Need for routing governance;
- Coordination with airport IT.

CHAPTER 5

Proven Airport Deployment Experience

5.1 Airport Experience Developed Through Asia's Digital Aviation Expansion

Over the past two decades, Asia has experienced one of the world's most intensive periods of airport development, terminal expansion and infrastructure modernization.

Many major Asian airports were newly constructed, significantly expanded or digitally upgraded during a period when IP communications, high-definition video, industrial Ethernet, centralized management and data-driven operations had already become practical technologies.

As a result, these airports were able to incorporate more digital systems into their original designs and subsequent expansion programs.

The objective was not only to accommodate increasing passenger traffic. Modern airport development also needed to support:

- Growing baggage and cargo volumes;
- Larger and more distributed airfield facilities;
- More aircraft stands and ground-service operations;
- Expanded retail, hospitality and commercial facilities;
- More extensive perimeter and video coverage;
- Higher public-safety and security expectations;
- Greater operational visibility;
- Faster coordination between airport departments;
- More connected equipment and field devices;
- Long-term expansion without interrupting airport operations.

This period of development created a demanding environment for airport technology providers.

Airport owners, design institutes and system integrators needed to connect an increasing number of cameras, controllers, communication devices, sensors and operational systems across large geographical areas. These devices were often installed far from terminal communication rooms, in outdoor cabinets, utility facilities, tunnels, remote aprons and other locations where conventional enterprise-networking equipment was not always suitable.

Industrial Ethernet became an important part of this transformation.

It provided a practical way to replace isolated point-to-point transmission links with managed, redundant and scalable network infrastructure. Multiple airport systems could be connected through fiber networks while remaining logically separated, centrally monitored and easier to maintain.

Avcomm's Participation in Airport Digitalization

Avcomm developed its airport experience during this period of rapid digital expansion.

Since its early airport deployments, Avcomm industrial-networking products and solutions have been applied in approximately 20 large and regional airport projects.

These projects have included applications such as:

- Airport perimeter surveillance;
- Airfield video transmission;
- Remote apron and remote aircraft-stand monitoring;
- Airport access and gate connectivity;
- Emergency telephone communication;
- Public-address and operational communication interfaces;
- Airport tunnel and service-road systems;
- Environmental and operational sensing;
- Distributed field cabinets;

- Redundant fiber networks;
- Network and equipment monitoring;
- Integration of field devices with airport operational platforms.

Avcomm's airport record includes both large international airports and regional airports.

Large airports require network infrastructure capable of supporting extensive geographical coverage, continuous operation, multiple contractors, large numbers of connected devices and complex coordination between security, operations, maintenance and information-technology teams.

Regional airports face a different challenge. They often need comparable reliability and visibility with fewer communication rooms, smaller maintenance teams and more limited project budgets.

Working across both environments has allowed Avcomm to develop solutions that can scale from a small number of remote field nodes to multi-area airport networks.

Experience Beyond Product Supply

Avcomm's airport experience is not limited to supplying industrial switches.

The company has participated in the practical application of industrial Ethernet across the airport edge, including:

- Evaluating field-device communication requirements;
- Selecting appropriate copper and fiber interfaces;
- Designing redundant fiber-ring and point-to-point architectures;
- Connecting multiple devices within remote field cabinets;
- Separating different airport applications through VLANs;
- Monitoring network, optical-link and equipment status;
- Supporting phased migration from optical transceivers and unmanaged networks;
- Integrating network and field-device alarms into operational platforms;
- Supporting long-term maintenance and system expansion.

This experience has provided Avcomm with a practical understanding of how airport field networks perform after commissioning—not only how they appear in design documents.

Learning Across Aviation Markets

The commercial aviation industry developed earlier in the United States than in many Asian countries.

U.S. airports accumulated decades of practical experience in airport safety, airfield operations, passenger processing, emergency response and infrastructure maintenance. Many Asian airport owners, planners and design organizations studied international practices, including those developed in the United States, when planning new airports and major expansion programs.

However, Asian airports did not simply reproduce earlier airport designs.

Because many projects were developed or extensively modernized during the digital era, they had an opportunity to combine established airport-operating principles with newer technologies such as:

- IP video surveillance;
- Industrial Ethernet;
- Centralized network management;
- Digital access control;
- Smart baggage systems;
- Integrated operational databases;
- IoT sensors;
- Video analytics;
- Automated equipment monitoring;
- Digital-twin and AI-oriented platforms.

This created a valuable body of implementation experience.

The aviation industry can now learn in both directions.

Asian airports continue to benefit from the operational maturity and safety practices developed by established U.S. airports. At the same time, airport owners, engineering consultants and system providers in the United States can

evaluate digital systems and implementation approaches that have already been deployed at scale in newer and recently expanded Asian airports.

Relevance to Airport Modernization

Many U.S. airports are now upgrading systems that were originally constructed in different technology generations.

These modernization programs may involve:

- Replacing analog or early-generation IP cameras;
- Expanding perimeter and remote-apron coverage;
- Upgrading unmanaged field switches;
- Replacing standalone optical transceivers;
- Increasing fiber-network capacity;
- Introducing network redundancy;
- Improving cybersecurity segmentation;
- Connecting previously isolated operational systems;
- Providing centralized network and device visibility.

Avcomm’s airport experience is relevant to these projects because the company has participated in airport environments where many of these digital technologies were incorporated during new construction or large-scale expansion.

The intent is not to transfer one airport’s architecture directly into another market.

Every U.S. airport must follow its own security program, design standards, network architecture, cybersecurity requirements, procurement rules and operational priorities.

Instead, Avcomm offers a body of practical airport implementation experience that owners and design organizations can evaluate when developing their own modernization strategies.

With applications across approximately 20 large and regional airports, Avcomm brings field-proven experience in connecting airport perimeter systems, video surveillance, remote operational facilities, emergency communications and distributed edge devices over resilient industrial Ethernet networks.

This experience allows Avcomm to contribute not only individual products, but also practical lessons in how airport edge networks can be designed, deployed, monitored, maintained and expanded throughout their operational lifecycle.

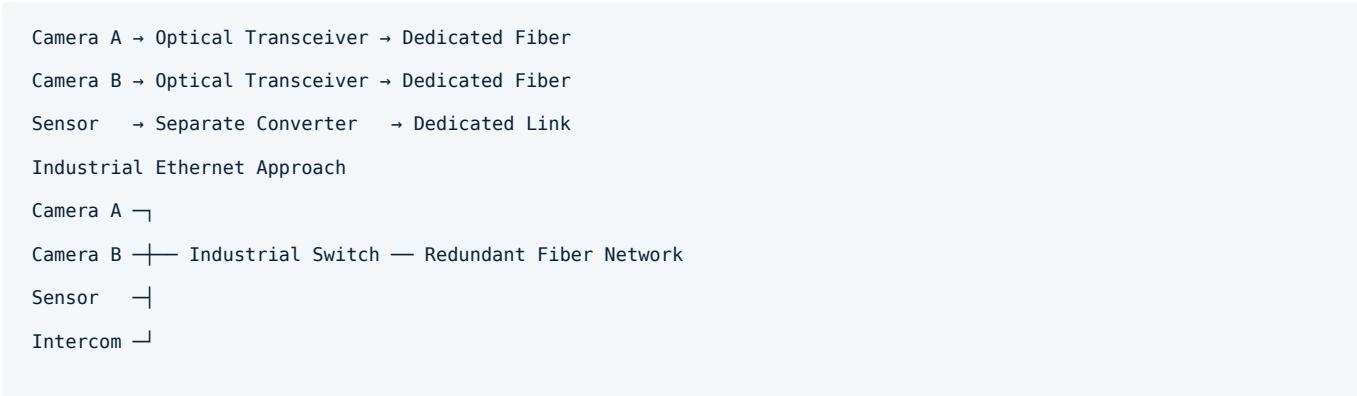
5.2 From Optical Transceivers to Managed Industrial Ethernet

In 2009, Avcomm began applying industrial Ethernet ring-networking technology to airport airfield-perimeter applications.

At the time, many field-video designs relied on independent point-to-point optical transceivers. These devices transported video or Ethernet signals, but offered limited centralized visibility and made multi-device expansion difficult.

The transition to managed industrial Ethernet introduced a different architecture:

Legacy Approach



This transition provided several benefits:

- Multiple devices could share a managed field node;
- Fiber resources could be used more efficiently;
- Redundant communication paths could be introduced;
- Network faults became visible;
- Remote devices could be monitored;
- Additional services could be added without rebuilding the entire transmission system;
- Different applications could be separated through VLANs;
- Maintenance teams could diagnose network conditions centrally.

The significance of the change was not simply replacing one transmission product with another.

It moved the field network from passive signal conversion toward an actively managed communication infrastructure.

5.3 Airport Perimeter and Airfield Applications

Typical Avcomm-supported airport edge applications have included:

- Airfield perimeter video;
- Remote cameras;
- Access gates;
- Emergency communications;
- Industrial telephones;
- Environmental sensors;
- Tunnel and service-road systems;
- Equipment monitoring;
- Fiber ring networks;
- Remote cabinet connectivity;
- Network monitoring and fault alarms.

The design approach combines industrial switching with application-level integration rather than treating the network as an isolated product layer.

5.4 Regional Airports and Cost-Effective Modernization

Large hub airports often have established enterprise architecture, approved-product lists and extensive internal engineering resources.

Regional airports may face different constraints:

- Smaller engineering teams;
- Limited fiber availability;
- Fewer communication rooms;
- Greater reliance on outside integrators;
- Smaller capital budgets;
- Need for simple maintenance;
- Mixed generations of equipment.

Industrial Ethernet can provide a practical modernization path because it allows the airport to:

- Retain usable legacy devices;
- Add IP cameras incrementally;
- Consolidate field communication;
- Introduce redundancy selectively;
- Monitor remote infrastructure;
- Expand without building a full communication room at every location.

The architecture can therefore scale from a small number of perimeter nodes to a large multi-area airport network.

5.5 ATMS: Connecting Networks, Devices and Operational Workflows

Avcomm's Airport Tunnel and Technology Management System experience extends beyond physical connectivity.

The ATMS concept provides an integration and operations layer for:

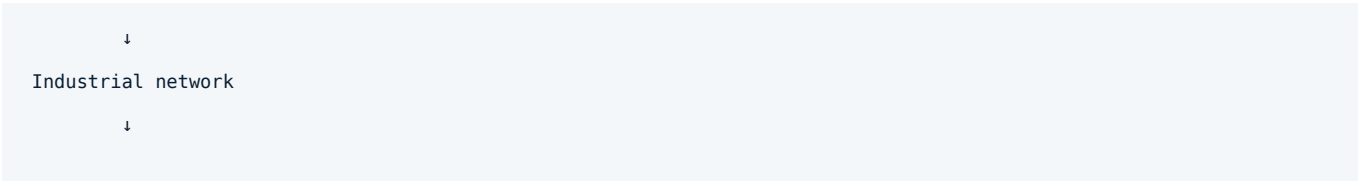
- Network devices;
- Video-system interfaces;
- Sensors;
- Alarm devices;
- Emergency telephones;
- Public-address interfaces;
- Environmental systems;
- Field controllers;
- Maps;
- Event workflows;
- Maintenance records.

The platform is not positioned as a replacement for an airport’s approved VMS, access-control system or emergency-communication platform.

Instead, it can provide a controlled integration layer through which authorized systems exchange status, alarms and operational information.

A typical workflow may include:

Field device alarm



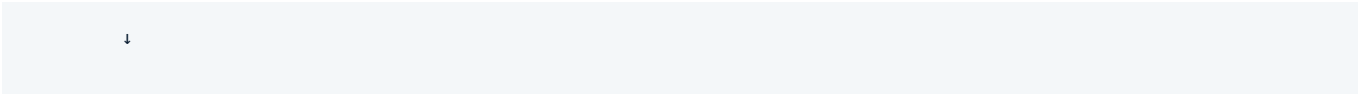
ATMS / IoT integration layer



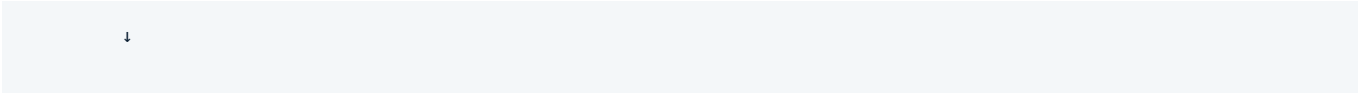
Geographic location and event classification



Request related video from existing VMS



Present event to authorized operator



Record response and maintenance history

This approach can help airports connect distributed devices more quickly and economically while preserving existing system ownership.

Potential benefits include:

- Faster onboarding of new edge devices;
- Unified network and equipment visibility;
- Reduced custom integration effort;
- More efficient alarm handling;

- Better coordination between IT, operations and maintenance;
- Historical records for troubleshooting;
- Foundation for future analytics.

5.6 Lessons Learned from Airport Deployments

Long-term airport experience has produced several practical lessons.

Design for maintenance, not only commissioning

The system should make it possible to identify the failed component remotely.

Keep failure domains manageable

A large ring may save fiber but create excessive operational impact if poorly segmented.

Monitor power as well as data

Many apparent network failures are actually power, PoE or cabinet-environment failures.

Standardize configurations

Field switches should use controlled templates, naming conventions and documented VLAN assignments.

Leave expansion capacity

Cameras, sensors and operational devices are likely to increase after commissioning.

Preserve system boundaries

Integration should not create uncontrolled access between security, operations and enterprise networks.

Treat the edge as part of cybersecurity

Remote cabinets and field ports must be included in security policy.

CHAPTER 6

Modernizing Existing Airport Systems and Preparing for the Future

6.1 The Immediate Opportunity Is Modernization

Artificial intelligence will influence the future of airport operations, but most airports first need to modernize existing infrastructure.

Common current conditions include:

- Analog cameras connected through encoders;
- First-generation IP cameras;
- Unmanaged field switches;
- Independent optical transceivers;
- Single-path fiber links;
- Mixed 100 Mbps and Gigabit networks;
- Limited PoE capacity;
- Incomplete device inventories;
- Flat VLAN designs;
- Obsolete switches;
- No centralized field-network monitoring;
- Inconsistent cybersecurity configuration.

These conditions create a practical and immediate application for industrial Ethernet.

The objective is not to force a complete replacement. It is to establish a structured migration plan.

6.2 Video-System Modernization

An airport may wish to add:

- Higher-resolution cameras;
- Thermal cameras;
- Panoramic cameras;
- AI-capable cameras;
- Additional coverage at blind spots;
- New storage;
- Centralized VMS access.

Before adding these devices, the airport should evaluate:

- Existing switch capacity;
- Uplink bandwidth;
- PoE budget;
- Fiber topology;
- Network redundancy;
- Camera VLAN structure;
- Cybersecurity;
- Time synchronization;
- Monitoring and maintenance.

A field cabinet that previously supported two low-resolution cameras may not support six high-resolution PoE cameras without redesign.

Industrial switches provide a way to upgrade field capacity while retaining the airport's existing VMS and core infrastructure.

6.3 Replacing Standalone Optical Transceivers

Standalone optical transceivers can be effective for individual point-to-point connections, but they often provide limited management.

Replacing groups of converters with managed industrial switches can provide:

- Port aggregation;
- VLANs;
- Redundant uplinks;
- SFP diagnostics;
- Centralized alarms;
- PoE;
- Remote troubleshooting;
- Additional capacity.

This should be evaluated carefully. Some critical point-to-point links may remain appropriate. The goal is not universal replacement, but rationalization of the edge architecture.

6.4 Upgrading Unmanaged Field Networks

An unmanaged switch offers basic connectivity but cannot provide the operational information required for a growing airport network.

A phased upgrade may proceed as follows:

Phase 1: Inventory

Document:

- Field switches;
- Connected devices;
- Fiber paths;
- Cabinet power;
- IP addresses;
- Existing VLANs;
- Environmental conditions.

Phase 2: Criticality assessment

Classify sites by:

- Safety impact;
- Security impact;
- Operational impact;
- Number of connected devices;
- Difficulty of physical access.

Phase 3: Managed switching

Replace priority unmanaged nodes with industrial managed switches.

Phase 4: Segmentation

Introduce VLANs and controlled routing.

Phase 5: Redundancy

Add diverse fiber paths or ring protection where justified.

Phase 6: Centralized management

Integrate switch status, optical levels and alarms into the airport's NMS or approved operational platform.

6.5 Adding Network Intelligence at the Edge

The edge is handling more network functions than in earlier generations.

A modern airport edge node may need to support:

- VLAN assignment;
- Traffic prioritization;
- Multicast filtering;
- Access-control lists;
- Device authentication;
- Local routing;
- DHCP protection;
- Network address translation in limited use cases;
- Secure remote management;
- Time synchronization;
- Port mirroring for diagnostics.

This is driven by the number and diversity of connected devices.

The edge switch is no longer merely a multiport media converter. It is a controlled extension of airport network policy.

6.6 Network Visibility as a Primary Design Requirement

Future airport specifications should not describe only:

- Port quantity;
- Fiber type;
- Bandwidth;
- Temperature.

They should also define visibility requirements:

- What alarms must be reported?
- Which protocols are permitted?
- Where are logs stored?
- Can optical power be monitored?
- Can PoE status be viewed remotely?
- Can configurations be backed up?
- Can device topology be discovered?
- Can firmware versions be inventoried?
- Can the airport identify unauthorized changes?

For many airport operators, improved visibility may provide more immediate value than increasing theoretical bandwidth.

6.7 Preparing for AI and Data-Driven Operations

Once the airport has reliable, managed and segmented edge connectivity, it becomes possible to support advanced applications such as:

- Video analytics;
- Perimeter target classification;
- Automated stand-occupancy detection;
- Ground-service-equipment analytics;
- Predictive device maintenance;
- Network anomaly detection;
- Digital-twin visualization;
- Robotics;
- Drone-based inspection;
- Automated incident correlation;
- Natural-language maintenance assistance.

AI depends on data availability and data quality.

A camera cannot support useful analytics if its network is unstable. Predictive maintenance is not possible if switch alarms, power status and optical measurements are not collected. A digital twin cannot reflect airport conditions if field devices are isolated.

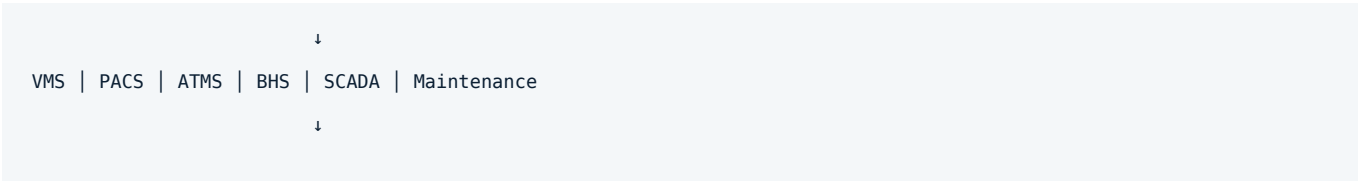
Industrial Ethernet is therefore not the final intelligent application. It is the infrastructure that makes future airport intelligence practical.

6.8 An AI-Ready Airport Edge Architecture

Field Devices



Secure Airport Data and Integration Layer



Analytics and AI



Operator Decision and Controlled Automation

This structure preserves human and system authority.

AI may assist with:

- Detection;
- Classification;
- Diagnosis;
- Recommendation;
- Trend analysis.

Final control decisions remain subject to airport policy, safety requirements and authorized personnel.

CHAPTER 7

Selecting Industrial Ethernet for Airport Applications

7.1 Environmental Requirements

Designers should evaluate:

- Operating-temperature range;
- Storage-temperature range;
- Humidity;
- Shock and vibration;
- Electromagnetic compatibility;
- Surge and electrical-transient tolerance;
- Fanless construction;
- Metal enclosure;
- Grounding;
- Certification requirements.

The specified environmental rating should reflect actual cabinet conditions, not only local outdoor temperature.

7.2 Physical Installation

Important requirements include:

- DIN-rail or rack mounting;
- Cabinet dimensions;
- Connector access;
- Terminal-block orientation;
- Fiber bend radius;
- Heat dissipation;
- Maintenance clearance;
- Cable-management space;
- Grounding point;
- Removable terminal blocks.

7.3 Port and Bandwidth Planning

Designers should calculate:

- Current endpoints;
- Planned expansion;
- Camera bitrate;
- Simultaneous streams;
- Uplink utilization;
- Multicast traffic;
- PoE power;
- Fiber-port quantity;
- Need for 1G, 2.5G, 10G or higher capacity.

A switch should not be selected only according to today's device count.

7.4 Redundancy

The specification should identify:

- Permitted redundancy protocol;
- Required recovery time;
- Ring or uplink topology;

- Dual-power requirements;
- Link-failure alarms;
- Test procedures;
- Maximum number of field nodes per protection domain.

7.5 Network Management

Recommended capabilities may include:

- Web interface;
- CLI;
- SNMPv3;
- Syslog;
- LLDP;
- Configuration backup;
- User-role control;
- Secure firmware upgrade;
- SFP digital diagnostics;
- Port utilization;
- PoE monitoring;
- Relay alarms.

7.6 Cybersecurity

Airport edge switches should be evaluated for:

- HTTPS and SSH;
- SNMPv3;
- AAA integration;
- Role-based access;
- Password policy;
- Disabled insecure services;
- Port security;
- 802.1X where required;
- ACLs;
- Signed firmware;
- Vulnerability disclosure;
- Software bill of materials;
- Product-security lifecycle;
- Logging and auditability.

7.7 Integration and Interoperability

The switch must operate within the airport's approved architecture.

Interoperability considerations include:

- Existing core-switch vendors;
- Spanning-tree or ring protocols;
- VLAN standards;
- Network-management platforms;
- VMS;
- Access-control systems;
- PLCs;
- IP audio;
- Time services;
- Optical standards;
- Multicast requirements.

CHAPTER 8

Avcomm Airport Edge Networking

Avcomm provides industrial communication products and application experience for distributed airport infrastructure.

Relevant capabilities include:

- Unmanaged industrial Ethernet switches;
- Managed Layer 2 industrial switches;
- Layer 3 industrial switches;
- Industrial PoE switches;
- Gigabit and multi-gigabit fiber connectivity;
- Industrial firewalls;
- Industrial wireless;
- Network-management and visualization;
- Edge-device integration;
- ATMS and IoT-oriented operational integration.

Avcomm's approach is based on three principles.

Connect

Provide reliable communication for distributed airport devices.

Protect

Use redundancy, segmentation and secure management to protect availability and system boundaries.

Understand

Make networks and connected devices visible to airport operations and maintenance teams.

Avcomm does not propose one universal topology for every airport.

The company works with airport owners, engineering consultants and system integrators to adapt the architecture according to:

- Existing airport standards;
- Approved systems;
- Available fiber;
- Environmental conditions;
- Cybersecurity requirements;
- Operational criticality;
- Funding and procurement requirements;
- Maintenance capabilities.

Conclusion

Modern airports depend on systems that extend far beyond terminal communication rooms.

Cameras, sensors, access gates, weather systems, docking guidance, baggage automation, emergency communications and utility equipment are increasingly connected through Ethernet. Many of these devices are installed in remote, unattended and environmentally challenging locations.

This creates a growing need for industrial edge networks.

Industrial Ethernet switches provide the physical and logical bridge between distributed airport devices and centralized airport systems. Their value includes:

- Long-distance fiber connectivity;
- Compact field installation;
- Environmental resilience;
- Multi-device aggregation;
- PoE;
- Redundancy;
- VLAN separation;
- Network visibility;
- Remote maintenance;
- A foundation for future integration and AI.

The most successful airport edge architecture is not the one with the largest number of features. It is the one that fits the airport's operational model, preserves system boundaries, simplifies maintenance and provides a controlled path for modernization.

Avcomm's airport experience—from early industrial Ethernet ring deployments to current multi-system integration—demonstrates how managed edge networking can replace isolated transmission links with resilient, visible and scalable infrastructure.

The opportunity now is to apply those lessons within the regulatory, cybersecurity and design framework of each airport.

About Avcomm

Avcomm Technologies develops industrial networking, cybersecurity, wireless communication and network-management solutions for critical infrastructure.

Its products and application experience support airports, transportation, municipal infrastructure, power utilities, manufacturing, energy and other industrial environments.

For airport projects, Avcomm works with owners, engineering consultants and system integrators to develop resilient edge-network designs for perimeter security, remote apron monitoring, airfield infrastructure, baggage systems, utilities and connected operational technologies.

Avcomm Technologies

Industrial Networking for Connected Airport Operations

AVCOMM TECHNOLOGIES

Industrial networking, cybersecurity, wireless communication and network-management solutions for critical infrastructure.