

Digital Spine for Airports

Connect and Protect Critical Airport Infrastructure



What if your airport infrastructure could sense passenger demand, optimize energy use, protect critical OT systems, run local intelligence at the edge, and give airport teams a single operational view in real time?

Cisco and Schneider Electric present the Digital Spine for Airports: a converged, cyber-secure, data-centric IT/OT foundation that connects airport workplaces, terminals, baggage systems, power infrastructure, building operations, industrial IoT (IIoT) devices, Cisco® Unified Edge, cybersecurity telemetry, and enterprise analytics across a multibuilding airport campus.

Cisco secures and connects the airport. Schneider Electric powers, automates, and optimizes the airport. Cisco Unified Edge brings compute, data processing, and application hosting closer to airport operations. Together, the solution helps you support low-latency analytics, local resilience, IEC 62443-aligned cyber defense, AI-ready airport intelligence, sustainability, and cyber resilience across terminals, baggage systems, plant rooms, lounges, airside facilities, cargo areas, and airport city precincts.

Benefits

- Improve airport cyber resilience with an IEC 62443-aligned security architecture using Cisco Industrial Threat Defense, Cyber Vision, Secure Firewall, Software-Defined Access, Identity Services Engine (ISE), Duo MFA, Secure Equipment Access, and Splunk for visibility, segmentation, threat detection, response, and auditability.
- Run airport intelligence closer to operations with Cisco Unified Edge, which provides distributed compute for local data processing, Splunk collection, security telemetry, airport applications, integration services, and edge analytics across terminals, baggage areas, central plants, lounges, cargo buildings, car parks, and airside facilities.
- Modernize multibuilding campus connectivity with Cisco Catalyst 9300 Series access switches, IE3500 Series switches, 8000 Series routers, Catalyst 9800 Series controllers, Wi-Fi access points, Catalyst Center, Software-Defined Access, and URWB.
- Reduce energy and carbon impact by integrating Schneider Electric EcoStruxure Building Operation, Power Monitoring Expert, Power Advisor, Microgrid Advisor, connected meters, and building controls with Cisco Spaces, Wi-Fi telemetry, Unified Edge, IIoT data, and Splunk analytics to automate energy optimization based on occupancy and operating conditions.
- Create unified airport visibility by using Splunk to correlate IT logs, OT security telemetry, building management system (BMS) alarms, power data, passenger flow events, wireless events, maintenance signals, vendor access activity, and edge-generated insights into a shared operational intelligence layer for the airport operations center.

Overview

Airports across the Global region are modernizing rapidly. Passenger volumes are returning, terminal expansions are accelerating, sustainability mandates are tightening, and cyber resilience is becoming a board-level priority. At the same time, many airports still operate with fragmented IT, OT, building, power, baggage, security, and workplace systems. These silos create blind spots, slow incident response, increase energy waste, and make it harder to deliver consistent passenger and staff experiences across terminals and airport campuses.

The Digital Spine for Airports is a joint architecture that brings together Cisco future-proofed workplaces, cybersecurity, Industrial IoT and Splunk®, with Schneider Electric EcoStruxure Building Operation, Digital Energy, Secure Power, APC infrastructure, power monitoring, microgrid, and building automation capabilities. The solution provides a blueprint for a secure, scalable, multibuilding airport platform that connects power, systems, people, and data so airport operators can improve passenger experience, reduce operating cost, strengthen cyber resilience, support local edge operations, and advance sustainability goals.

Trends and challenges

Airports are becoming cyber-physical digital platforms

Modern airports are no longer only transport facilities. They are connected, energy-intensive, data-rich, multibuilding campuses that depend on IT and OT systems working together. Passenger processing, baggage handling, HVAC, lighting, access control, security systems, power distribution, runway support systems, lounges, retail, collaboration tools, and airport operations centers all depend on reliable digital infrastructure.

Legacy silos limit performance and increase risk

Many airport systems were deployed as isolated projects. BMS, baggage, power, security, Wi-Fi, collaboration, and maintenance platforms often have separate networks, separate dashboards, separate vendor access paths, and separate data models. This makes it difficult to detect OT risk, understand energy performance, correlate passenger movement with building demand, or respond quickly to disruptions.

IEC 62443-aligned security is becoming essential

Airports are nationally important infrastructure. They need security architectures that align with established industrial cybersecurity principles, including asset visibility, zones and conduits, least privilege access, secure remote access, event logging, vulnerability awareness, network segmentation, and incident response. IEC 62443 provides a practical framework for designing and operating cyber-secure OT environments. Cisco and Schneider Electric help you apply these principles across airport building systems, power systems, baggage systems, airside assets, wireless infrastructure, edge compute, and enterprise networks.

A converged architecture can eliminate silos and improve efficiency and security

Airport leaders are under pressure to reduce emissions, improve energy efficiency, increase asset uptime, protect critical infrastructure, and deliver better passenger experiences. The challenge is that these outcomes cannot be achieved by isolated point solutions. They require a converged architecture that securely connects systems, standardizes data, enables automation, places intelligence at the edge, and gives operational teams a shared view of the airport.

“Cisco secures and connects the airport. Schneider Electric powers, automates, and optimizes the airport. Cisco Unified Edge brings airport intelligence closer to operations.”

“IEC 62443 gives airport operators a practical way to structure OT cybersecurity around asset visibility, zones, conduits, access control, monitoring, and response.”

How it works

The Digital Spine for Airports is a secure IT/OT architecture for airport campuses. It connects airport buildings, infrastructure, systems, assets, users, data, and applications through a common digital foundation.

The architecture is designed to support:

- Terminal buildings
- Airport operations centers
- Baggage handling areas
- Security screening zones
- Passenger gates and lounges
- Retail and commercial precincts
- Car parks and transport interchanges
- Airside support buildings
- Cargo and logistics facilities
- Central utility plants
- Electrical substations
- Microgrid and battery energy storage systems (BESS)
- EV charging and electrified ground support infrastructure
- Airport city developments and multitenant real estate
- Remote buildings and regional airport facilities
- Multi-airport portfolios

The key architectural principle is to move away from siloed airport systems and toward a secure, open, IP-based, data-centric operating model.

Cisco provides secure connectivity, segmentation, cybersecurity, workplace experience, IIoT telemetry, Cisco Unified Edge, and the Splunk operational intelligence layer. Schneider Electric provides power infrastructure, building automation, energy management, microgrid capabilities, Secure Power, APC edge infrastructure, connected room solutions, and EcoStruxure software.

Together, the solution enables airport operators to connect, protect, process, monitor, automate, and optimize airport infrastructure across the campus.

The solution is modular. You can start with one terminal, one energy use case, one OT cyber segment, one Cisco Unified Edge node, one airport operations dashboard, or one multibuilding campus architecture. You can then scale the model across the airport campus or portfolio.



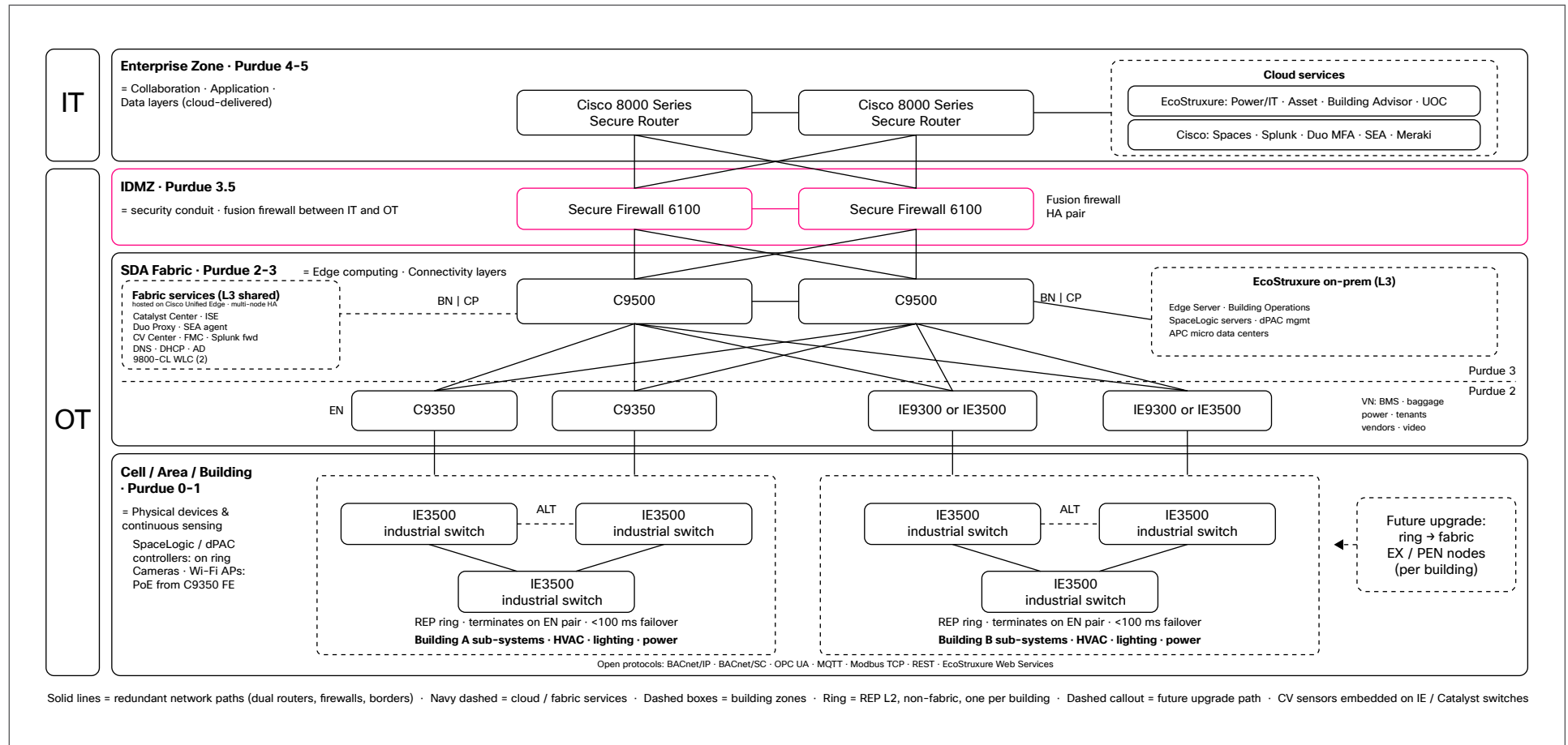


Figure 1. Digital Spine – Buildings Reference Architecture

Design principles

1. Start with IEC 62443 zones and conduits

Do not connect OT systems to the enterprise network without a segmentation model. Define zones and conduits for terminal systems, baggage, BMS, power, tenants, vendors, edge compute, and enterprise IT.

2. Use Cisco Software-Defined Access for policy consistency

Use Software-Defined Access where appropriate to simplify segmentation and apply consistent policy across users, devices, wireless access, edge nodes, and airport systems.

3. Use Secure Firewall for controlled conduits

Use Cisco Secure Firewall to inspect and enforce communication between critical zones such as enterprise, industrial demilitarized zone (DMZ), BMS, baggage, power, edge compute, and vendor access.

4. Use Cisco ISE and Duo MFA for identity

Use Cisco ISE to profile endpoints and enforce access policy. Use Duo MFA where stronger user verification is required.

5. Place intelligence where it is needed

Use Cisco Unified Edge to run local data processing, security telemetry, Splunk collection, and selected airport workloads close to operational systems.

6. Use open protocols where practical

Prioritize Building Automation and Control Networks (BACnet)/IP, BACnet/Secure Connect (SC), Open Platform Communications Unified Architecture (OPC UA), Message Queuing Telemetry Transport (MQTT), Modbus TCP, REST, and EcoStruxure Web Services to reduce proprietary lock-in and improve data access.

7. Keep control local

Use EcoStruxure Edge Server, Enterprise Server, SpaceLogic automation servers, distributed Programmable Automation Controllers (dPACs), Soft dPAC, APC micro data centers, and Cisco Unified Edge to keep critical control and operational functions close to the physical process.

8. Use Splunk as the shared operational intelligence layer

Do not create another siloed dashboard. Use Splunk to correlate data across IT, OT, building, energy, security, wireless, edge, and airport systems.

9. Design for lifecycle operations

Include monitoring, patching, remote access, audit logs, external log storage, certificate management, reporting, edge node health, and support models from the beginning.

10. Build for multibuilding scale

Design the first terminal or pilot zone in a way that can scale to a full campus, airport city, or multi-airport portfolio.

Table 1. Cisco solution components

Cisco component	Role in the airport architecture
Cisco Catalyst 9300 Series access switches	Secure access switching for IT, OT, IoT, Wi-Fi access points, Power over Ethernet (PoE) endpoints, workplace devices, and connected airport systems.
Cisco IE3500 Series switches	Ruggedized industrial switching for OT environments such as baggage systems, plant rooms, power systems, airside assets, and industrial control areas.
Cisco 8000 Series routers	High-performance routing for airport WAN, campus edge, data center interconnect, cloud connectivity, and resilient airport backbone connectivity.
Cisco Catalyst 9800 Series wireless core control plane	Wireless control capability for airport Wi-Fi services, delivered through the Catalyst 9800 wireless architecture and 9800 Series WLC.
Cisco Catalyst 9800 Series WLCs	Wireless control plane for airport Wi-Fi access points, supporting passenger, staff, IoT, and operational wireless services.
Cisco Wi-Fi access points	Wireless connectivity and telemetry source for passenger mobility, staff devices, IoT, location services, and Cisco Spaces occupancy insights.
Cisco Ultra-Reliable Wireless Backhaul (URWB)	Reliable wireless backhaul for selected mobile, airside, temporary, or hard-to-cable airport use cases requiring resilient wireless connectivity.
Cisco Software-Defined Access	Policy-based campus fabric for segmentation, automation, and consistent access policy across users, devices, edge nodes, and airport systems.
Cisco Identity Services Engine (ISE)	Identity-based access control, device profiling, policy enforcement, and segmentation across IT, OT, IoT, wireless, and edge devices.
Duo MFA	Multifactor authentication for user, administrator, and remote access workflows where applicable.

Cisco component	Role in the airport architecture
Cisco Catalyst Center	Network automation, assurance, provisioning, telemetry, and operational visibility across Cisco enterprise networks.
Cisco future-proofed workplaces	Secure networking, collaboration, smart building technology, Cisco Spaces, workplace experience, and user protection for airport workspaces, lounges, and operations areas.
Cisco Unified Edge	Distributed edge compute platform for hosting local airport applications, telemetry collectors, security services, Splunk forwarders, analytics workloads, and integration services close to terminals, baggage systems, power systems, and airside assets.
Cisco Industrial Threat Defense	OT asset visibility, security posture, segmentation, secure remote access, and cross-domain threat detection.
Cisco Cyber Vision	OT asset discovery, industrial protocol visibility, vulnerability context, and process-aware security monitoring.
Cisco Secure Firewall	Zone-based enforcement, secure conduits, traffic inspection, policy control, and boundary protection between airport zones.
Cisco Secure Equipment Access	Zero-trust remote access for approved vendors, maintainers, and OT specialists.
Splunk Enterprise, Cloud, SIEM, and SOAR	Unified operational intelligence, dashboards, alerting, data correlation, incident investigation, and automation.
Cisco collaboration and Webex devices	Airport workplace collaboration, control rooms, meeting spaces, staff areas, lounges, and embedded environmental telemetry where applicable.

Reference architecture: Seven-layer model

The solution is best understood as a seven-layer architecture. Each layer has a clear role, and each layer connects to the layers above and below.

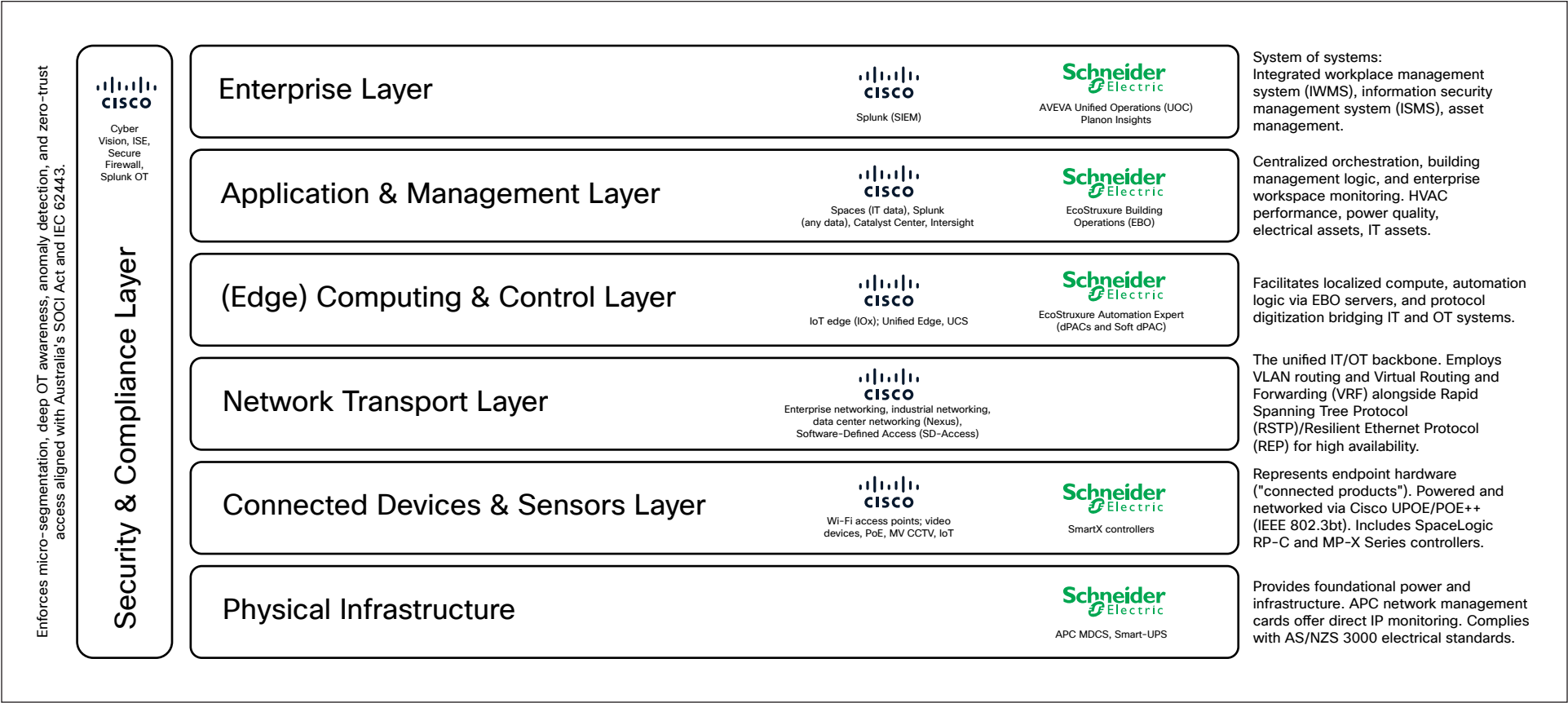


Figure 2. Digital Spine - Technology Stack

Layer 1: Physical infrastructure

This layer includes the power, cabling, cabinets, racks, uninterruptible power supply (UPS), switchgear, cooling, and physical containment that support airport digital systems.

It provides resilient, monitored, and secure physical infrastructure for IT, OT, Cisco Unified Edge, Schneider Electric EcoStruxure systems, and distributed airport workloads. Airport environments need resilient power and compute close to the assets they support. APC micro data centers can be placed in terminals, plant rooms, baggage areas, remote buildings, or airside facilities to host local control, telemetry, security, and analytics workloads.

Layer 2: Connected devices and sensors

This layer includes the field devices that create airport telemetry or execute physical control.

It enables the capture of high-quality, real-time data from airport spaces, assets, power systems, and operational equipment. This layer is where airport systems become observable. The richer the telemetry, the more effectively the airport can automate energy, predict maintenance issues, improve passenger flow, and detect OT risk.

Layer 3: Network transport layer

This is the converged IT/OT transport foundation. It carries airport application traffic, OT protocol traffic, telemetry, control commands, security data, user traffic, and management traffic.

It uses a secure, resilient IP network as the common foundation for airport IT, OT, IoT, edge, and building systems. This does not mean every system must collapse into one flat network. It means airport systems can share a common network architecture while remaining segmented by function, criticality, tenant, building, and security zone.

Layer 4: Edge computing and control layer

The edge computing and control layer is where airport data becomes locally actionable. This layer supports local control, local application hosting, protocol translation, telemetry filtering, security monitoring, and operational analytics close to the airport systems that create the data.

Cisco Unified Edge provides the compute platform for local airport intelligence. Schneider Electric EcoStruxure platforms provide local building, power, and automation control. APC Secure Power protects the edge node with UPS, rack, power distribution, and physical infrastructure. Cisco networking securely connects the edge node to OT devices, airport systems, Splunk, and enterprise platforms.

This creates a repeatable edge pattern for the airport campus: connect locally, process locally, control locally, secure locally, and synchronize globally.

Layer 5: Application and management layer

This layer provides operational applications, dashboards, configuration tools, analytics, and management platforms.

It gives airport engineering, operations, facilities, security, energy, and executive teams the right operational tools while allowing Splunk to act as the shared data and observability layer across domains.

Layer 6: Enterprise and airport systems layer

This layer connects airport-specific systems and enterprise platforms.

Airport systems often contain valuable context: flight schedules, passenger demand, gate allocation, resource planning, asset status, and tenant data. When these systems are securely integrated with building, power, edge, network, and security telemetry, the airport can move from reactive operations to predictive and outcome-driven operations.

Layer 7: Security and compliance layer

Security is not a separate overlay. It is embedded across every layer of the architecture.

This layer supports cyber resilience and compliance readiness across critical airport infrastructure. Requirements vary across countries, so this solution supports security and compliance programs but does not replace formal regulatory or legal guidance. The architecture provides the visibility, segmentation, access control, logging, edge telemetry, and auditability needed to help airports prepare for critical infrastructure expectations, privacy requirements, breach reporting obligations, and cyber insurance scrutiny.

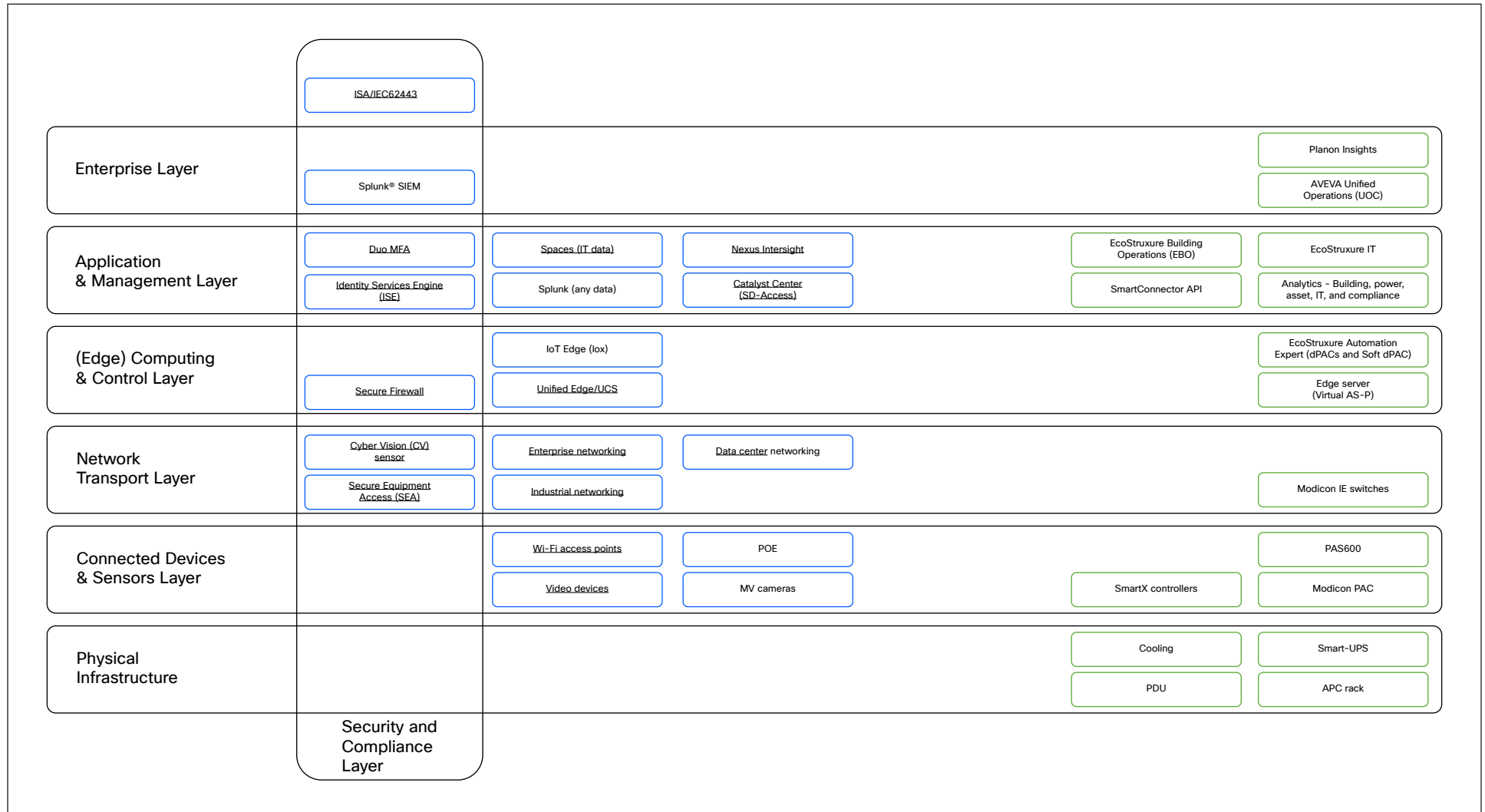


Figure 3. Digital Spine - Conceptual Architecture

IEC 62443-aligned security architecture

IEC 62443 provides a practical framework for securing industrial automation and control systems. For airports, this is especially relevant because airport operations depend on cyber-physical systems: baggage handling, power distribution, HVAC, lighting, access control, airside assets, and building automation.

The Cisco and Schneider Electric architecture supports IEC 62443-aligned design by applying the following principles.

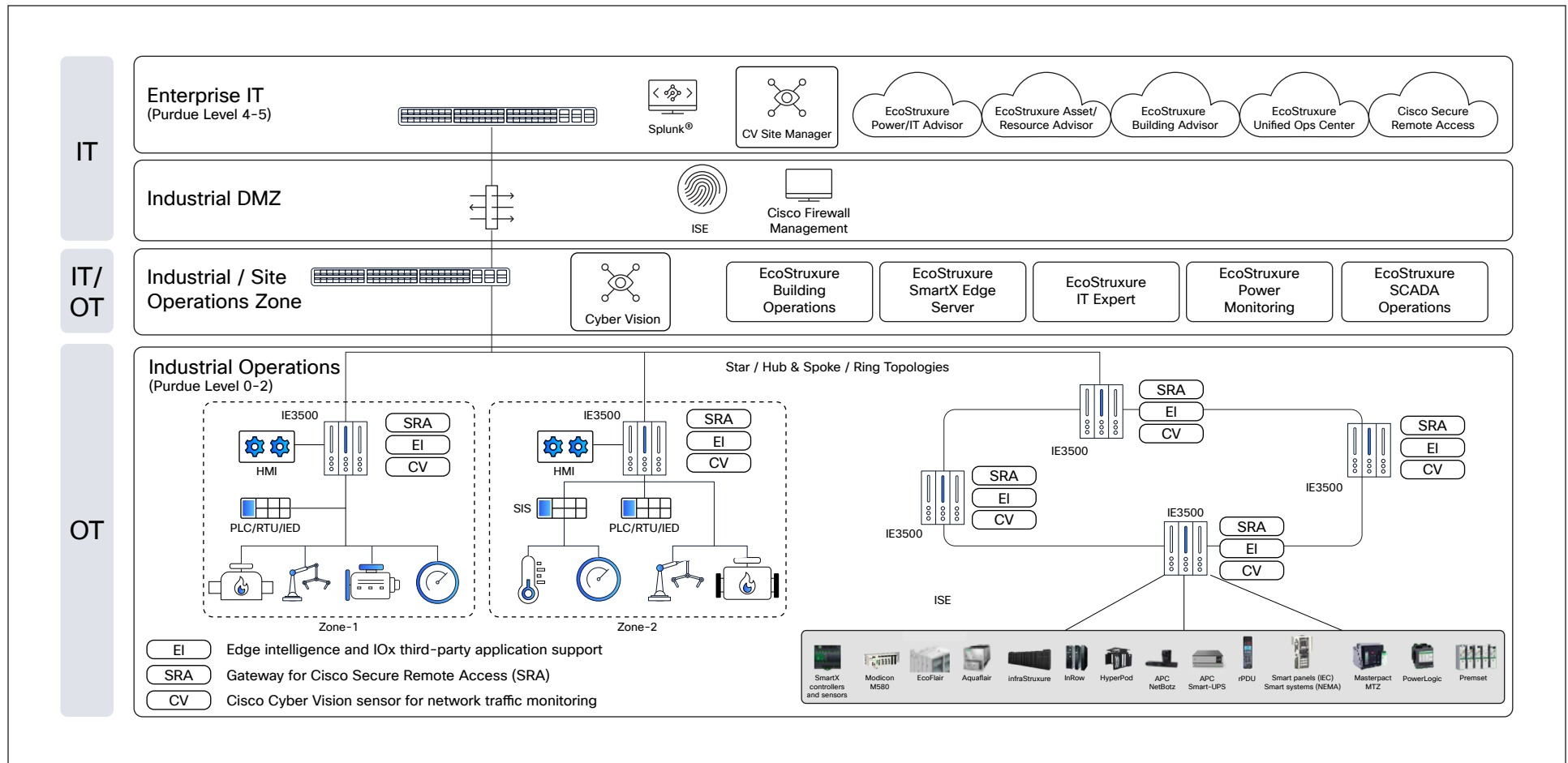


Figure 4. Digital Spine - Industrial IoT Reference Architecture

Asset visibility

You cannot secure what you cannot see. Cisco Cyber Vision and Industrial Threat Defense help discover OT assets, identify industrial protocols, map communication flows, and provide vulnerability context. Schneider Electric EcoStruxure systems provide asset, alarm, event, trend, and configuration data from BMS, power, and automation systems.

Airport examples:

- Identify programmable logic controllers (PLCs) and controllers in baggage systems.
- Discover power meters and UPS devices in electrical rooms.
- Map BMS communication paths across terminals.
- Identify unmanaged OT devices connected to industrial switches.
- Monitor unexpected traffic between zones.

Zones and conduits

IEC 62443 uses the concept of zones and conduits. A zone groups assets with similar security requirements. A conduit controls communication between zones.

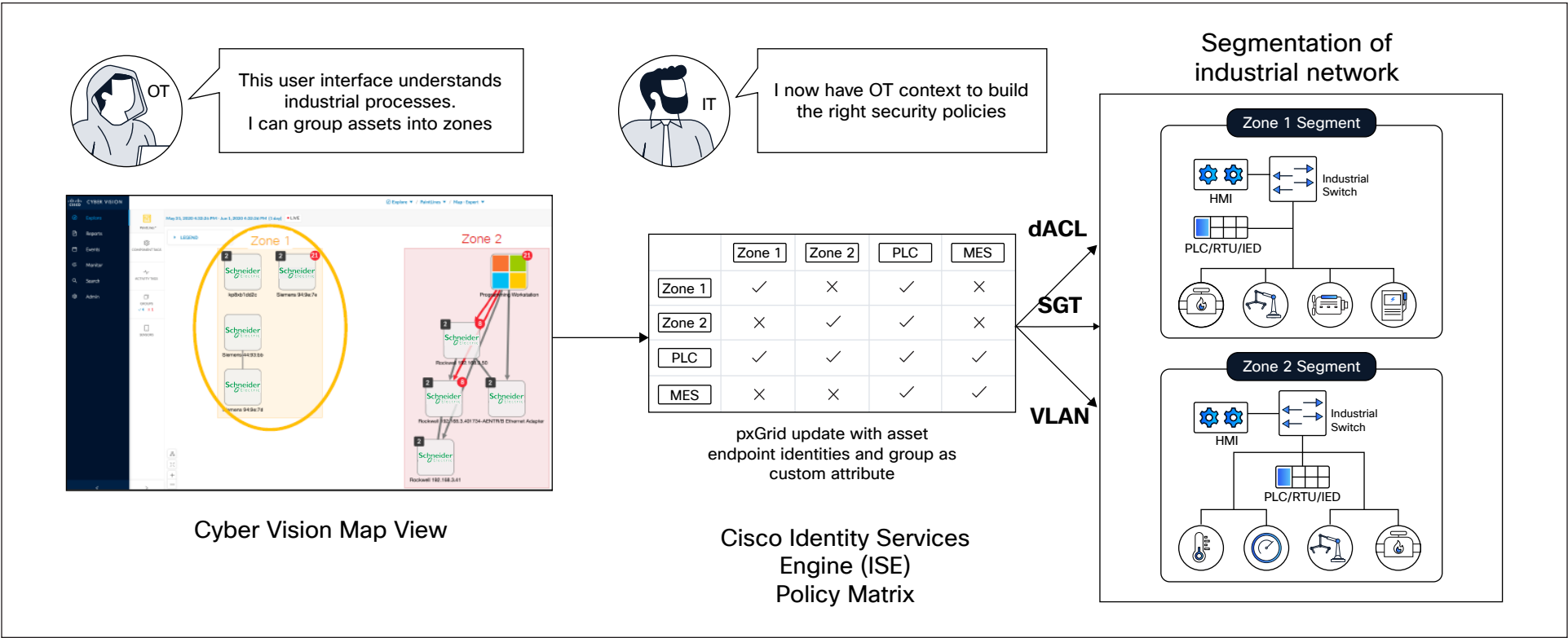


Figure 5. Protection - IEC 62443 network enforced zone segmentation

Airport zones may include:

- Enterprise IT zone
- Airport operations zone
- Security operations zone
- Industrial DMZ
- BMS zone
- Power systems zone
- Baggage handling zone
- Airside systems zone
- Passenger Wi-Fi zone
- Staff Wi-Fi zone
- Tenant/retail zone
- Vendor remote access zone
- Data center zone
- Edge compute zone
- Management zone

Cisco enforcement points include:

- Cisco Secure Firewall between high-risk or high-criticality zones
- Cisco Software-Defined Access virtual networks and policy
- Cisco ISE identity and device profiling

- Cisco TrustSec® and security group tags (SGTs)
- Virtual routing and forwarding (VRF) and VLAN segmentation
- Access control lists where appropriate
- Secure remote access through Cisco Secure Equipment Access

Least privilege access

Access should be based on role, device identity, location, and operational need. Cisco ISE and Duo MFA help verify users and devices. Cisco Secure Equipment Access helps restrict vendor access to specific assets, sessions, and time windows.

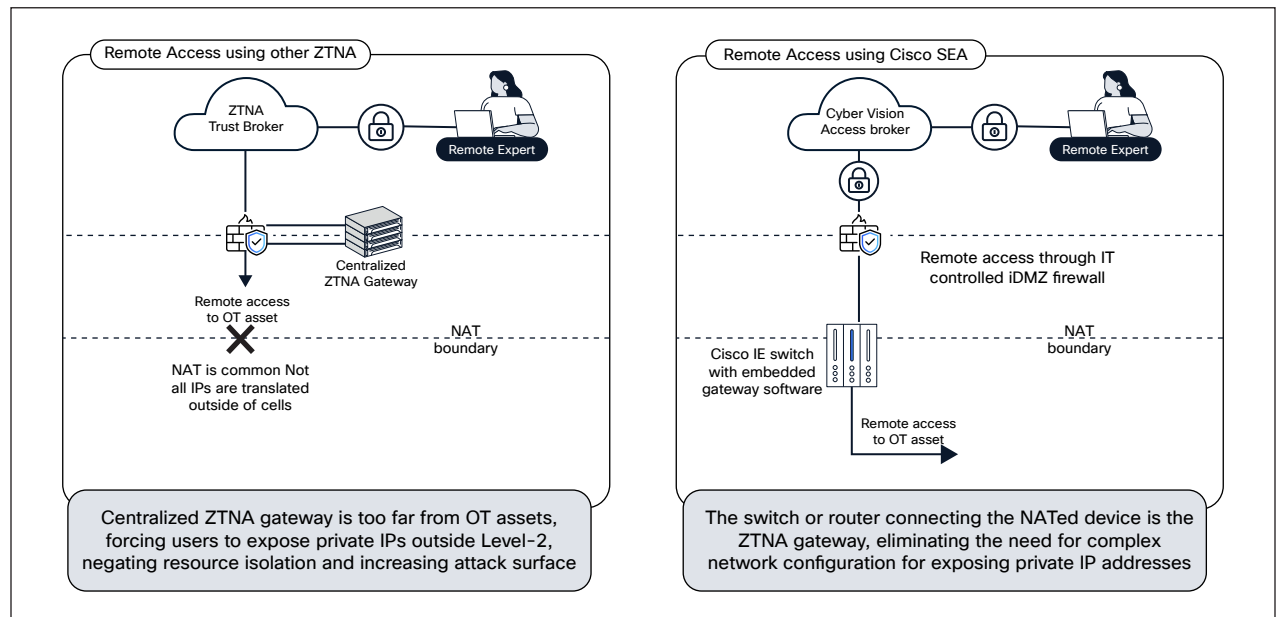


Figure 6. Protection - Secure remote access (ZTNA)

Airport examples:

- BMS vendors access only approved EcoStruxure systems
- Baggage vendors access only baggage OT assets
- Power specialists access only approved power monitoring systems
- Airport staff access only the networks and applications required for their role
- Contractors do not receive broad VPN access to the airport network

Secure conduits

Cisco Secure Firewall and Software-Defined Access help control communication between zones. BACnet/SC, TLS, OPC UA, MQTT over TLS, and HTTPS help secure application-level communications where supported.

Airport examples:

- BMS-to-enterprise reporting traffic passes through a controlled conduit
- OT telemetry flows to Splunk through approved collectors
- Vendor access is brokered through secure access services
- Power system data is forwarded through segmented, monitored paths
- Cisco Unified Edge hosts local collectors to reduce broad cross-zone data movement

Monitoring and detection

Cisco Cyber Vision, Secure Firewall, ISE, Catalyst Center, Unified Edge telemetry, Schneider Electric EcoStruxure logs, and Splunk create a cross-domain monitoring architecture.

Airport examples:

- Detect new or unauthorized devices in a baggage OT segment.

- Detect unusual communication between BMS and enterprise systems.
- Correlate a firewall event with a BMS alarm.
- Identify a vendor session linked to a configuration change.
- Detect changes in power quality associated with equipment degradation.

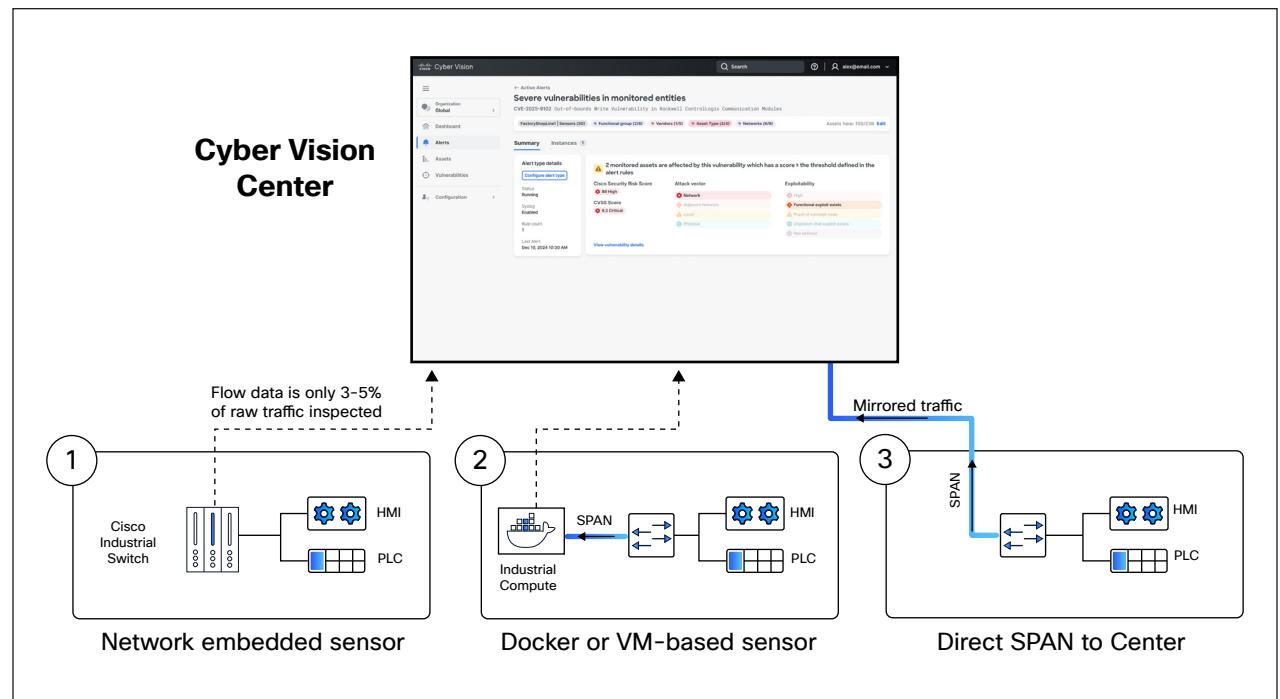


Figure 7. Visibility – OT asset visibility and security posture

Incident response and recovery

Splunk SIEM and SOAR, Cisco XDR integrations, Cisco Secure Firewall, Cisco ISE, and operational workflows help teams investigate and respond. Schneider Electric systems provide operational context such as alarms, trend logs, and control state.

Airport examples:

- Quarantine an OT device by policy
- Restrict vendor access during an incident
- Correlate cyber events with operational alarms
- Preserve logs and audit trails for investigation
- Use local edge processing to maintain visibility during upstream disruption

Cisco Unified Edge in the Airport Digital Spine

Cisco Unified Edge becomes the distributed compute layer of the Airport Digital Spine. It allows airport operators to place compute, storage, application services, telemetry

collection, and analytics closer to operational systems instead of sending every data stream directly to a central data center or cloud.

In a multibuilding airport campus, this matters because airport operations are distributed by nature. Terminals, baggage systems, central utility plants, airside support buildings, cargo facilities, car parks, lounges, and airport city buildings all create high volumes of operational data. Many of these environments also need local survivability, low-latency decision making, and secure segmentation.

Cisco Unified Edge helps provide that local digital foundation. It can be deployed with Schneider Electric Secure Power and APC micro data center infrastructure to create resilient edge nodes across the airport campus. These nodes can host or support workloads such as:

- Splunk forwarders
- Local data collectors
- OT security telemetry services

- Cisco Cyber Vision and Industrial Threat Defense integrations
- Airport analytics workloads
- Occupancy and environmental data processing
- Video or metadata processing where applicable
- EcoStruxure integration services
- Local dashboards
- Local airport operations applications
- AI-ready data processing pipelines

Cisco Spaces and EcoStruxure integration

Cisco Spaces provides real-time location and occupancy insights using Cisco network infrastructure, Wi-Fi access points, sensors, and collaboration devices. The Cisco Spaces and EcoStruxure Building Operation (EBO) integration allows occupancy count events to be processed and used by Schneider Electric systems for energy-saving automation.

“Airport operators do not need another siloed dashboard. They need a shared operational intelligence layer that connects IT, OT, edge, power, buildings, wireless, passenger flow, and security.”

Functional flow

1. Cisco Wi-Fi access points generate occupancy and location data.
2. Cisco Spaces uses the network and sensors to generate occupancy and location insights.
3. Occupancy events are provided through Cisco APIs.
4. Cisco Unified Edge can host local collectors or integration services where an airport requires local processing or buffering.
5. Schneider Electric Data Selection Tool maps locations into EBO objects.
6. Occupancy points are created in EcoStruxure Building Operation.
7. Building Data Platform and EBO use the occupancy data for automation logic.
8. HVAC, lighting, blinds, and space utilization dashboards can respond to actual occupancy.
9. Splunk correlates occupancy, energy, comfort, network, and security events.

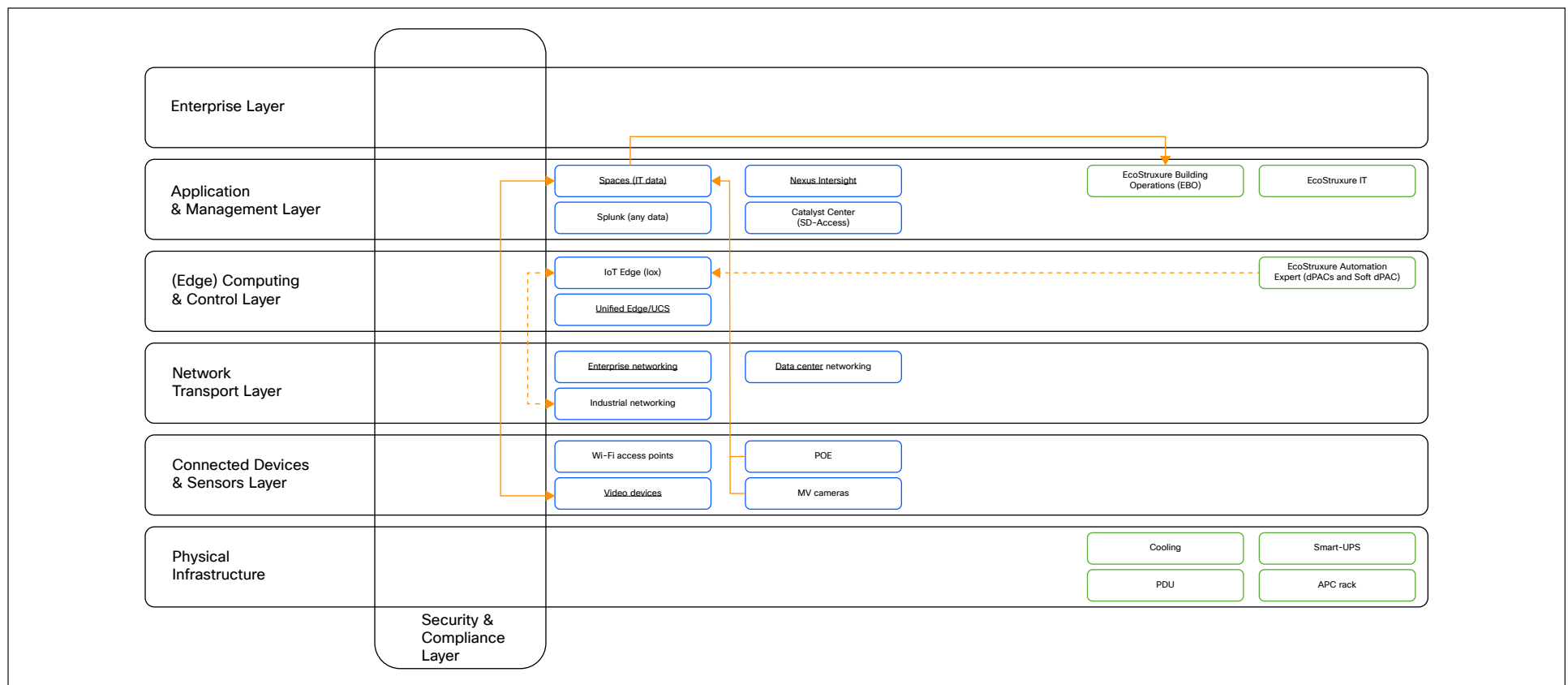


Figure 8. Digital Spine - Occupancy-driven building automation

Airport use cases enabled

- Gate area HVAC optimization based on passenger density
- Lounge energy optimization based on occupancy
- Cleaning and staffing optimization based on dwell time
- Queue and congestion insights
- Retail and concession dwell-time analytics
- Dynamic environmental control in staff workspaces
- Meeting room and operations room conditioning
- Reduced energy waste in unoccupied terminal wings

Splunk as the airport operational intelligence layer

Splunk provides the shared data layer that helps airport teams correlate events across IT, OT, energy, security, edge, and operations.

Table 2. Data sources for Splunk

Data source	Example data
Cisco Cyber Vision	OT assets, protocol activity, vulnerabilities, anomaly alerts
Cisco ISE	Device identity, policy decisions, authentication, profiling, SGT data
Cisco Secure Firewall	Traffic logs, security events, zone enforcement events
Cisco Catalyst Center	Network availability, performance, assurance, device telemetry
Cisco Spaces	Occupancy, location, utilization, movement events
Cisco Unified Edge	Local telemetry, application logs, edge workload status, local collectors, data pipeline health
Cisco Catalyst 9800 Series WLCs	Wireless performance, access point status, client telemetry, RF conditions, and operational events
Cisco Wi-Fi access points	Client association, telemetry, IoT presence, and location-related data
Cisco Ultra-Reliable Wireless Backhaul (URWB)	Wireless backhaul status and connectivity telemetry for selected airport use cases
Schneider EcoStruxure Building Operation	Alarms, trend logs, HVAC status, schedules, events
EcoStruxure Power Monitoring Expert	Energy, power quality, meter data, electrical events
EcoStruxure Building Advisor	Fault detection, diagnostics, comfort, maintenance insights
APC UPS and power distribution units	Power status, UPS events, battery health, load data
Airport operational database (AODB) and enterprise systems	Flight schedules, resources, asset records, maintenance tickets

Secure Firewall, Software-Defined Access, and ISE policy model

Cisco Secure Firewall, Software-Defined Access, and ISE work together to create a policy-based airport segmentation model.

Cisco ISE

Cisco ISE identifies users and devices, profiles

endpoints, and applies access policy. It can help classify airport endpoints such as:

- Staff devices
- Contractor devices
- Wi-Fi clients
- IP cameras
- BMS controllers

- Power meters
- UPS network management cards
- PLCs
- IoT sensors
- Wireless infrastructure
- Edge nodes

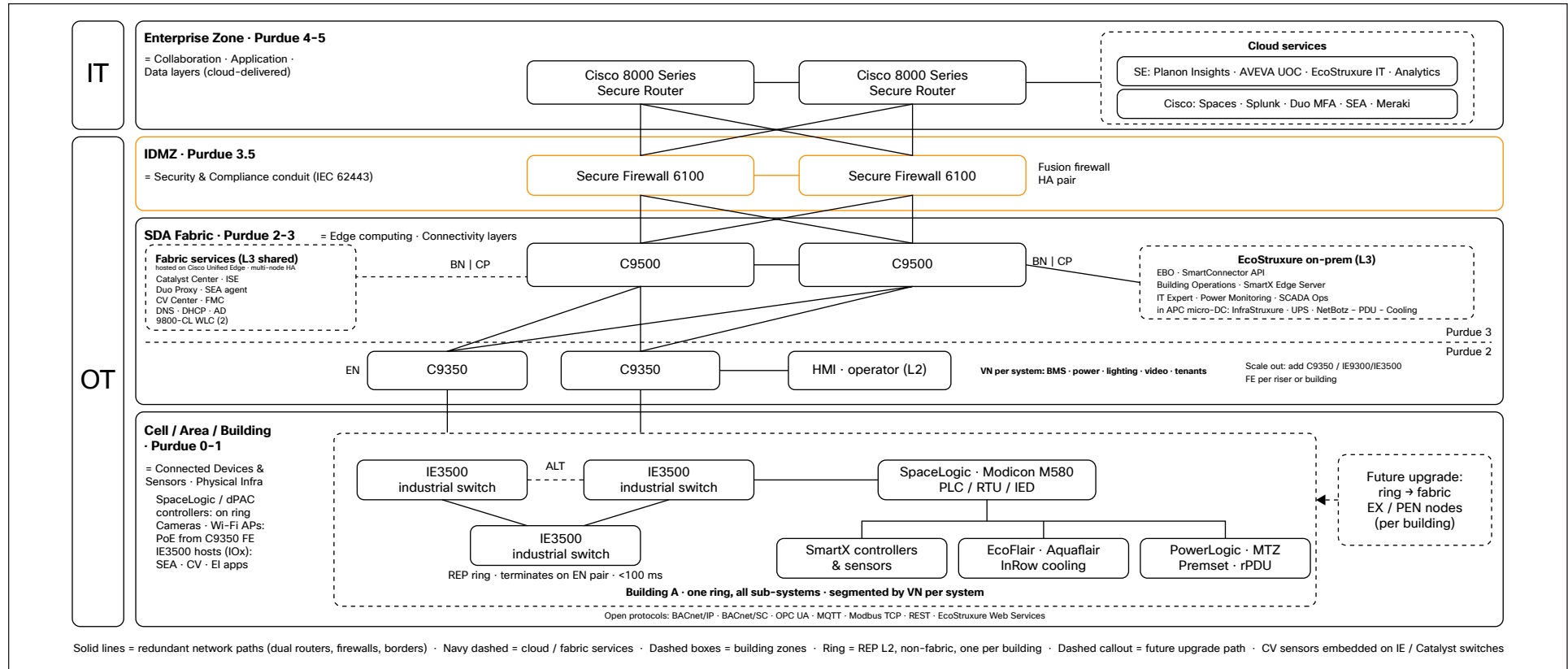


Figure 9. Digital Spine – Building Fabric Software Defined Access Reference Architecture

Cisco Software-Defined Access

Cisco Software-Defined Access (SD-Access) enables policy-based segmentation across the airport campus. It can separate virtual networks and apply group-based access policy.

Examples of virtual networks include:

- Enterprise IT
- Airport operations
- OT/industrial systems
- BMS
- Power systems
- Security systems
- Tenants and retail
- Guest services
- Management
- Edge compute

Cisco Secure Firewall

Cisco Secure Firewall provides enforced conduits between major zones, such as:

- Enterprise to industrial DMZ
- Industrial DMZ to BMS
- Industrial DMZ to baggage

- Management to OT
- Vendor access to approved assets
- Edge compute to Splunk
- Power systems to energy platforms

Wireless and URWB architecture

Airports need multiple types of wireless connectivity. Passenger Wi-Fi, staff mobility, IoT telemetry, location services, airside operational connectivity, temporary works, and mobile assets may all require different design patterns.

Cisco Catalyst 9800 Series wireless controllers and Wi-Fi access points

The Cisco Catalyst 9800 wireless architecture and WLC manage wireless policy, security, and operations for Cisco Wi-Fi access points. In the airport architecture, wireless supports:

- Passenger Wi-Fi
- Staff Wi-Fi
- Operational devices
- IoT endpoints
- Cisco Spaces telemetry
- Location-aware services
- Future-proofed workplace use cases
- Lounge and retail connectivity
- Maintenance team mobility

Cisco Ultra-Reliable Wireless Backhaul

URWB can support selected airport use cases where wired connectivity is difficult, temporary, mobile, or operationally constrained.

Potential airport use cases include:

- Airside operational connectivity
- Temporary terminal expansion zones
- Mobile maintenance environments
- Remote buildings or temporary facilities
- Construction and commissioning areas
- Backhaul for selected operational cameras or sensors where appropriate
- Hard-to-cable logistics or cargo environments

Security integration

Wireless services should be integrated into the same security model:

- Authentication and authorization through Cisco ISE
- Segmentation through Software-Defined Access, VLANs, VRFs, or policy
- Firewall inspection between zones
- Splunk ingestion for wireless telemetry
- Cisco Spaces data integration for occupancy and passenger-flow use cases

Future-proofed workplaces for airport staff and passengers

Cisco future-proofed workplaces extend the architecture into airport workplaces, control rooms, lounges, retail areas, collaboration spaces, and staff zones.

Relevant capabilities:

- Secure wired and wireless networking
- Collaboration devices and software
- Cisco Spaces
- User protection
- Smart building technology
- PoE switching
- IoT sensors and cameras
- Environmental telemetry
- Location services
- Wayfinding
- Digital signage integration
- Workplace analytics
- Secure segmentation
- Cisco Unified Edge for local workplace data processing and application hosting where required

Airport workplace examples include:

- Airport operations center collaboration rooms
- Airline and airport staff workspaces
- Engineering team workspaces
- Crisis coordination rooms
- Premium lounges
- Business traveler spaces

- Retail and concession offices
- Maintenance control rooms

Cisco Spaces and collaboration endpoints can contribute telemetry such as occupancy, device presence, environmental conditions, and space utilization. Schneider Electric EcoStruxure systems can use this data to adjust comfort, lighting, and energy consumption.



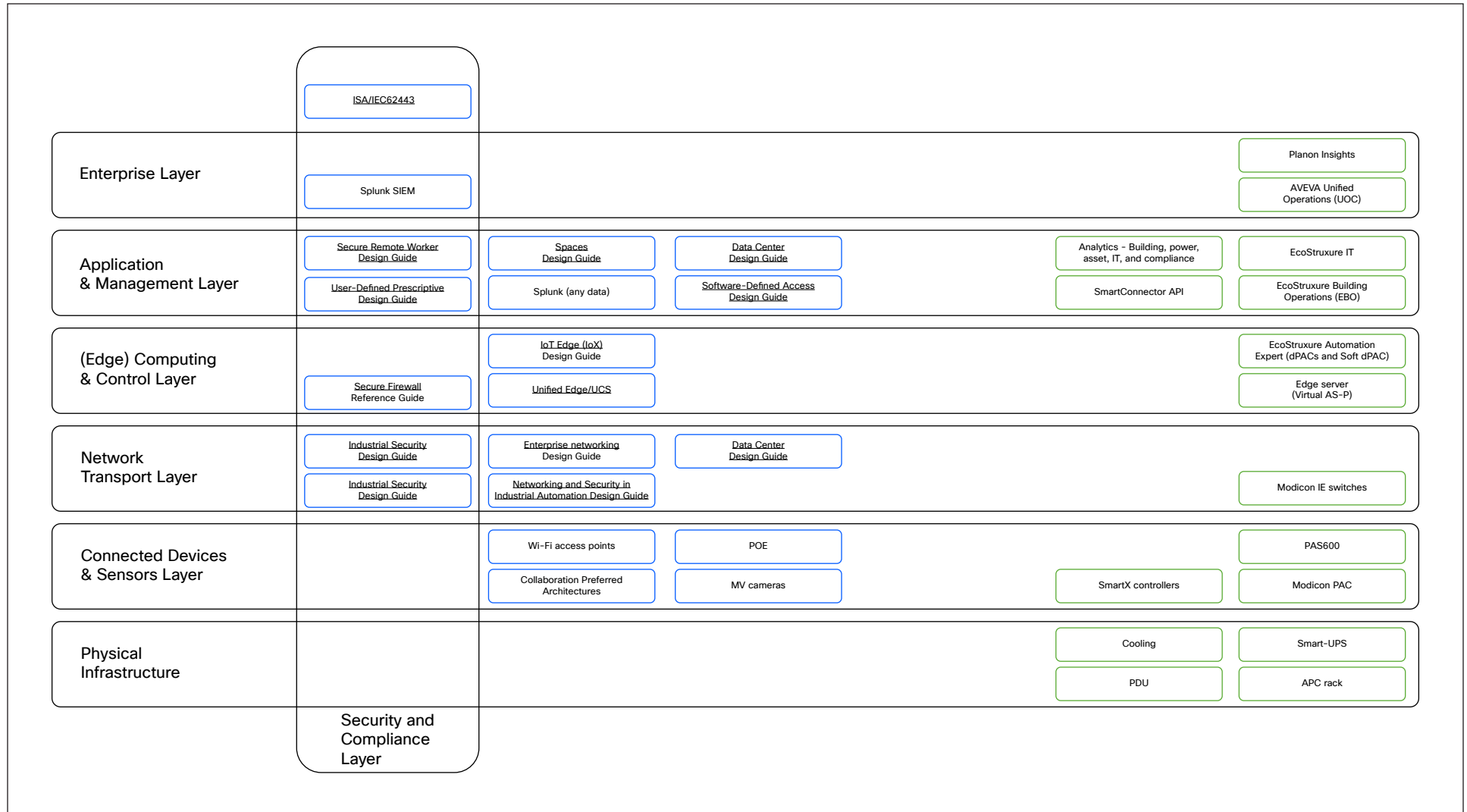


Figure 10. Cisco Validated Design Guide map

Use cases

Table 3. Use cases

Description	Customer challenge	Joint solution	Business ROI
Cyber-secure baggage handling and logistics	Legacy OT systems often use mixed or unencrypted protocols, creating ransomware and downtime risk.	Cisco Cyber Vision, Industrial Threat Defense, ISE, Secure Firewall, SD-Access, Unified Edge, Splunk, and Schneider automation systems provide OT asset visibility, segmentation, and monitoring.	Helps avoid baggage shutdowns and associated delay costs; baggage shutdowns can cost up to US\$120,000 per hour in flight delay penalties.
IEC 62443-aligned OT security architecture	Airport OT environments need structured security governance, asset visibility, zones, conduits, least privilege access, and controlled remote access.	Cisco Secure Firewall, SD-Access, ISE, Duo MFA, Cyber Vision, Secure Equipment Access, Splunk, and Schneider EcoStruxure security controls support an IEC 62443-aligned model.	Reduces cyber exposure, improves audit readiness, supports insurance and regulatory expectations, and reduces risk of operational disruption.
Net-zero smart terminal and microgrid optimization	Terminals waste energy by heating, cooling, and lighting underused gates, lounges, and terminal wings.	Cisco Spaces occupancy data, Cisco Unified Edge, EcoStruxure Building Operation, Power Monitoring Expert, Microgrid Advisor, and Splunk correlate occupancy, energy, tariffs, and building control.	Up to 22% reduction in terminal energy costs and the potential for full capital payback within 18 months.
Predictive airside asset maintenance	Runway lighting, jetways, ground power units, and plant assets can fail unexpectedly and disrupt turnaround times.	IIoT sensors, Cisco secure connectivity, Cisco Unified Edge, EcoStruxure alarms and trend logs, Building Advisor, Power Advisor, and Splunk analytics detect degradation earlier.	Asset lifecycle extended by up to 30%, and up to 15% reduction in gate delays.

Description	Customer challenge	Joint solution	Business ROI
Future-proofed smart lounge and airport workplace	Business travelers and airport staff need secure connectivity, high-quality collaboration, and comfortable spaces.	Cisco future-proofed workplaces, Wi-Fi, Webex, Cisco Spaces, Cisco Unified Edge, segmentation, and Schneider Connected Room Solutions optimize comfort, security, and experience.	Up to 18% increase in premium lounge subscription and retail concession revenue.
Unified IT/OT airport operations center	Data silos across baggage, power, security, facilities, wireless, and passenger flow slow response to disruptions.	Splunk consolidates IT logs, OT telemetry, BMS alarms, power data, Cisco Unified Edge data, Cisco Spaces events, wireless events, and maintenance workflows into a shared dashboard.	Up to 25% improvement in operational efficiency and faster passenger movement through terminals.
Distributed airport edge intelligence with Cisco Unified Edge	Airport data is generated across many terminals, plant rooms, baggage systems, lounges, and airside assets. Sending all data to a central location can increase latency, bandwidth use, and operational dependency.	Cisco Unified Edge, APC micro data centers, EcoStruxure Edge Server, Cisco secure networking, and Splunk collectors create distributed edge nodes for local processing, control, and analytics.	Improves local resilience, reduces unnecessary data backhaul, supports faster analytics, and creates a scalable foundation for AI-driven airport operations.
Resilient airport power and electrification readiness	Airports are adding EV charging, electric ground support equipment, renewables, and battery storage, increasing load complexity.	Schneider power management, microgrid, UPS, BESS, and metering integrate with Cisco secure networking, Unified Edge, and Splunk analytics.	Avoids outages, reduces peak demand, improves power quality, and creates greater resilience for critical terminal operations.
Secure vendor access for airport OT	Vendors need remote access to BMS, baggage, power, and plant systems, but broad VPN access increases risk.	Cisco Secure Equipment Access, ISE, Secure Firewall, Duo MFA where applicable, Unified Edge telemetry, and Splunk audit logs provide controlled, time-bound access.	Reduces operational risk, improves audit readiness, and requires less manual effort for vendor access governance.

Why IEC 62443 is vital for airports

Airports rely on connected OT systems such as baggage handling, HVAC, lighting, power, access control, and building management. As these systems move onto IP networks, IEC 62443 provides a globally recognized framework for securing industrial automation and control environments.

For airport leaders, IEC 62443 is more than a technical standard. It is a practical blueprint for reducing cyber risk across systems that affect terminal uptime, passenger experience, operational continuity, and resilience.

IEC 62443 helps airports define security zones and conduits, apply role-based access, manage OT asset risk, harden controllers, and protect systems across their lifecycle. It is especially relevant to the Cisco and Schneider Electric Airport Digital Spine because the architecture is built around secure IT/OT segmentation, asset visibility, encrypted communications, secure remote access, audit trails, and continuous monitoring.

Cisco Industrial Threat Defense, Cyber Vision, ISE, Secure Firewall, and Splunk, and Schneider Electric EcoStruxure capabilities can help airports support IEC 62443-aligned operations.

What makes the Airport Digital Spine different?

Traditional airport infrastructure often has separate IT, OT, building systems, power systems, wireless, edge compute, and security tools. This siloed structure creates duplicated networks, inconsistent security policies, limited automation, and incomplete data.

In contrast, the Airport Digital Spine is a converged, secure IT/OT solution that:

- Uses a secure IP foundation
- Supports open protocols and APIs
- Applies IEC 62443-aligned zones and conduits
- Places distributed compute capability through Cisco Unified Edge
- Connects building, power, workplace, wireless, and airport systems
- Adds OT asset visibility and segmentation
- Uses Splunk as a shared operational intelligence layer
- Supports multibuilding campus scale
- Allows energy and maintenance optimization based on real operational data
- Gives airport teams a pathway from connected infrastructure to autonomous operations

“By combining Cisco Spaces occupancy data, Cisco Unified Edge, and Schneider Electric EcoStruxure automation, airports can make terminal environments responsive to real passenger demand.”

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)

The Cisco Advantage

Only Cisco, in partnership with Schneider Electric, can provide a end-to-end IP architecture that converges your building's operational technology with enterprise-grade security. We don't just connect your devices; we secure the entire fabric of your building, helping ensure that your path to net zero is both efficient and defensible.

Learn more

Start your journey to a smarter, compliant, and more profitable airport today.

For additional information, visit:

- [Cisco future-proofed workplaces](#)
- [Cisco Spaces](#)
- [Cisco Industrial IoT](#)
- [Cisco Industrial Threat Defense](#)
- [Cisco Software-Defined Access](#)
- [Cisco Splunk](#)
- [Global Partners - Schneider Electric and Cisco](#)