

CSO Conference & Awards

Produced by **CSO** |  **IDC**

United Airlines

Distributed Isolation for Airport Operational Technology (OT)

Christopher Peters

Principal Architect – Operational Technology Cybersecurity

**CSO Conference
& Awards**



Produced by



The need for change

Operational Technology:

"Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)" - NIST

Why Focus on Isolation?

Difficult to patch

- OT is often 3rd party proprietary
- Patching can 'brick' OT devices

Older than IT

- Decades service life expectancies
- No priority/funds if device is working

Operationally critical

- Security like door access or cameras
- Airline customers expect that their checked baggage arrives on-time

Why Now?

Increasing Threat Landscape



- Stuxnet (2010)
- Ukraine power grid (2015)
- WannaCry (2017)
- Colonial Pipeline (2021)
- Volt Typhoon (2024)
- Arkansas City water treatment (2024)

TSA AOSSP Regulation



- Develop Segmentation Policies and Controls
- Prevent Unauthorized access to OT Systems
- Implement continuous monitoring of OT
- Establish vulnerability patching program

OT isolation objectives

Operational Resiliency

Isolating OT from IT ensures that a cyber incident in IT doesn't impact the operation or the safety of employees and customers.

Regulatory Compliance

Solutions should meet compliance requirements of the TSA's AOSSP.

Scalability & Future Proofing

Solutions should be flexible to accommodate airline growth, changing requirements and new tooling functionality.

Cost & Complexity Avoidance

Solutions need to meet the above objectives while minimizing cost (tooling, headcount) and operational complexity (processes, technology).

Challenges:

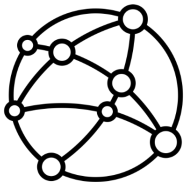
Air Gap – Would require duplicating miles of cabling/fiber at each airport

Firewall – Would require more than 100 new firewalls dedicated to OT due to sprawling network.

Host-based isolation – OT unmanaged assets do not support software agents.

Integrating OT tooling with network access control

Current State



Sprawling airport networks with intermixed IT and OT systems create Cyber security risk



Modern cloud-based OT intelligence platform

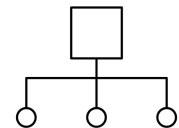
- Passively monitors network traffic
- Identifies and categorizes OT devices
- Provides vulnerability management
- Enables threat detection and incident response capabilities



IT access policy management

- Centrally manages NAC policy and provides role-based NAC enforcement
- Already integrates with Network Infrastructure

Future State



OT assets isolated from IT assets via role-based NAC policy distributed to point of use, complying to AOSSP

Business impact

Network isolation – OT systems inaccessible by IT

Cost avoidance – Uses existing tools

Regulatory compliance – Meets TSA AOSSP requirements

CSO Conference
& Awards

UNITED
AIRLINES 

Produced by

CSO | IDC

Successful OT isolation – at scale

New device plugged into airport network

Traffic interpreted, UAL context applied, and OT device profile created

Device OT context passed via custom integration from Armis to Clearpass

Matching Isolation ruleset assigned to device and NAC enforced



Axis IP Camera

ARMIS

Axis Communications

High Risk | 0 Alerts

Site

IAH (Auto Assignment) ▾

Boundaries

All OT Boundaries ✕

Camera ✕

ARMIS

Axis Communications

High Risk | 0 Alerts

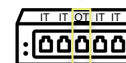
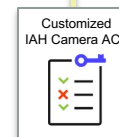
Tags

Port_Based_NAC_Applied ✕

ARUBA_CLEARPASS_CREATE_ENDPOINT ✕

aruba ClearPass

Endpoint	Attributes	Device Fingerprints
1.	ArmIs Boundaries	= Corporate
2.	ArmIs Boundaries	= Camera
3.	ArmIs Boundaries	= AS OT Boundaries
4.	ArmIs Category	= IMAGING
5.	ArmIs Manufacturer	= Axis Communications
6.	ArmIs Model	= PTZ Dome Network Camera
7.	ArmIs Risk Level	= H
8.	ArmIs Site	= IAH
9.	ArmIs Tags	= ARUBA_CLEARPASS_CREATE_ENDPOINT
10.	ArmIs Type	= IP_CAMERA
11.	Click to add...	



IAH Camera Switch