OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. Most importantly - If your organization require direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal- our team will work with you to ensure all necessary support is available through the member submission and RFI process.

Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

Aviation OT in Asia-Pacific

Threat, vulnerability and operational resilience brief | 3 November 2026

Field	Detail
Classification	TLP:CLEAR – may be shared without restriction
Intended readers	Airport operators, ANSPs, airlines, ground handlers and airport fuel operators; their OT engineering, security, facilities and safety teams; their suppliers

Key judgements

• In the reviewed public record, APAC aviation disruption is evidenced mainly through IT/service dependencies and GNSS RFI; no specific malicious compromise of APAC airside control equipment was substantiated by this review. This is not proof of absence.
• Published vulnerabilities affect general-purpose controllers, facilities platforms, access control and remote-access infrastructure that may appear in aviation estates. Public contracts do not establish vulnerable models, firmware or exposure at named airports.
• Actively exploited remote-access vulnerabilities merit urgent attention wherever they support engineering or vendor access; CISA added two further Ivanti Connect Secure KEVs on 30 October 2026.
• Navigation and data-link resilience is not solved by patching: ANSPs need validated backups, reporting, surveillance cross-checks and trained voice/terrestrial reversion. Protocol research must not be mistaken for observed airspace exploitation.

Five actions for this week

• Inventory all internet-exposed access gateways; check current CISA KEV and vendor advisories, including the three Ivanti Connect Secure KEVs. Preserve evidence and assess compromise where applicable.
• Perform authorised, non-intrusive external exposure discovery first. Do not run active scans against production PLCs, HMIs, CNS/ATM, BMS or life-safety systems without engineering approval and a tested method.
• Request a component/firmware inventory, support-access map and owner for each BHS, AGL, fuel, BMS and physical-security integrator path, including cellular/cloud links.
• Confirm 24-hour manual-service and supplier-outage procedures for check-in, baggage handling, FIDS and airline/airport messaging, with named operational decision-makers.
• ANSPs: review ICAO APAC GNSS RFI and associated data-link disruption guidance (V1.0, Aug 2026); validate interference reporting, surveillance cross-check and voice reversion.

1. How to use this report

If you are…	Start with
Airport OT / facilities engineering	Section 4 action cards A–E, then the 72-hour checklist in Section 8
Airport or airline IT security	Section 4 card F (remote-access edge), Section 6 priority matrix
ANSP CNS / ATM engineering	Section 4 card G, Section 5 protocol watchlist, GNSS panel in Section 7
Airport fuel farm operator	Section 4 card C
Operations, crisis and business continuity	Section 4 card H, Section 7 incidents, Section 8 exercise action
Senior leadership	Key judgements and Section 8

2. Scope, method and confidence

- Scope: civil aviation OT in Asia-Pacific – airside, terminal and building systems, baggage handling, fuel, air navigation and surveillance, and the shared platforms they depend on.
- Method: cross-check of vendor PSIRT and CISA advisories/KEV, ICAO APAC material, primary aviation and government notices, and selected public tender/contract records. Research cut-off: 3 November 2026. Product presence, vulnerability exposure and operational effects are separately assessed.
- Limitations: no airport-level scanning or firmware attestation was performed. Announced contracts are not an installed-base inventory; specific airport exposure is unknown absent operator/integrator confirmation. No exploitation procedures are included. Operator-specific exposure evidence may be shared separately under appropriate TLP controls.
- Confidence: Confirmed = a clearly scoped assertion supported by primary official material or independent corroboration; Probable = credible but incomplete; Possible = limited or disputed; Unverified = claim only. Confirmation of a vulnerability or cyber incident does not confirm its deployment at an airport, its exploitation there, or OT safety impact.

Evidence rule: A publicly reported contract is not proof of installation; a CVE is not proof of local deployment, vulnerable version or reachability; KEV is not proof of exploitation at an airport; reported passenger-platform disruption is not evidence of OT compromise. These distinctions govern all assessments below.

3. Publicly reported aviation technology: contracts and deployments in APAC

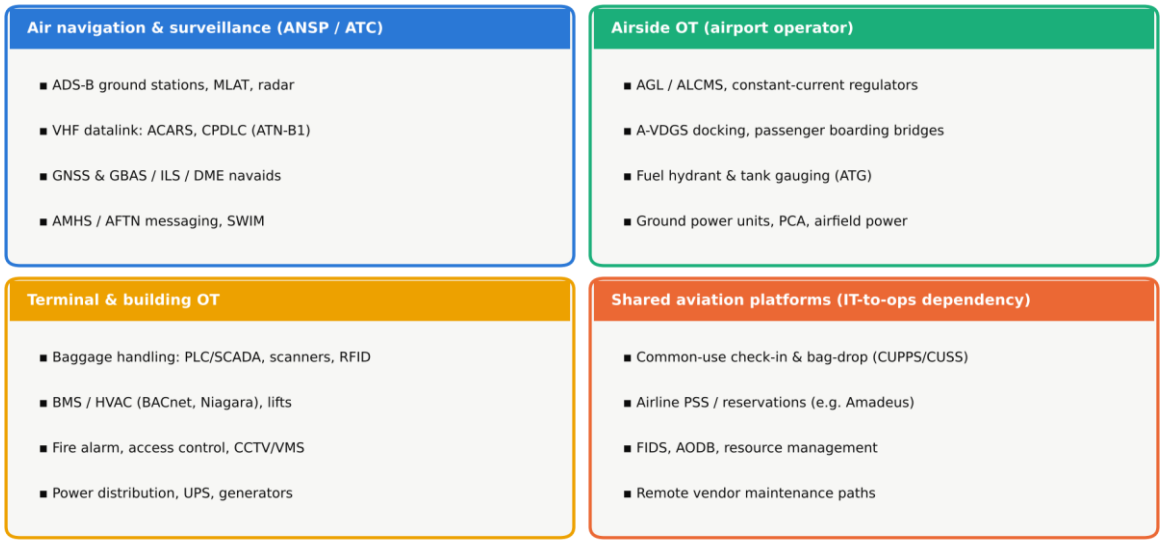

Figure 1. Aviation OT zones and representative device classes (OT-ISAC framing).

These publicly reported procurements and agreements illustrate technology families relevant to APAC aviation. They do not identify vulnerable product versions, prove installations are complete, or establish cyber exposure at the cited facilities.

Country	Site / owner	Technology / implementation status (as reported)	Date	Source
Vietnam	Tan Son Nhat T3; Long Thanh International	Vanderlande baggage-handling contracts announced in 2024; installation/current versions not independently attested. [20]	May 2024	[20]
India	Bhogapuram (Andhra Pradesh)	ADB SAFEGATE LED AGL and ILCMS contract announced in 2024; site commissioning status not verified. [21]	Jul 2024	[21]
Indonesia	Jakarta en-route centre; Balikpapan, Medan, Pontianak approach	Indra ManagAir ATM/GAREX IP voice modernisation contract announced in 2025; implementation varies by site. [22]	Mar 2025	[22]
Singapore	Civil Aviation Authority of Singapore	CAAS awarded NexGen ATMS/ATC radar work to Thales in July 2026; project targeted for completion in 2030, not currently operational. [23][41]	Jul 2026	[23]
Australia	Sydney Airport	SITA Flex common-use and SITA Bag Message services agreement reported in 2021; current version/deployment to confirm. [24]	Mar 2021	[24]

OT-ISAC assessment

• Publicly disclosed contracts identify classes of specialist aviation technology, not site-specific CVE exposure. An airport or ANSP must map integrator-supplied controllers, firmware, operating systems and remote-access paths before claiming that a published vulnerability is present.

• For each system, record system owner, operator, support provider, externally reachable interfaces, approved change window, safety dependencies and validated fallback arrangements.

4. Device-by-device: exploitable vulnerabilities and actions

The following are vendor/CISA-published vulnerabilities affecting device classes sometimes used in aviation support environments. They are NOT evidence of exploitation or installation at a particular APAC airport. “Access needed” is conditional on the specific CVE, network configuration and authentication preconditions.

A. Baggage handling and other PLC-controlled ground systems

What is inside	PLCs, remote I/O, drives, HMIs and SCADA servers; serial-to-IP converters; scanners and RFID. Protocols: PROFINET, EtherNet/IP/CIP, S7comm, Modbus TCP, OPC.
Exploitable vulnerabilities	Rockwell Logix / Studio 5000, CVE-2021-22681: network-accessible authentication-bypass weakness; added to CISA KEV in March 2026. Rockwell PN1550 (rev 1.6) lists corrective patch: No, workaround: Yes. [1][2] Siemens S7-1200/S7-1500, CVE-2022-38465: offline extraction of a family private key from a CPU may enable later attacks on legacy protected communication; not an internet-exploitation claim. [3] Unitronics Vision/Samba, CVE-2023-6448: insecure default-access configuration; known exploited where reachable. [4][42] Moxa NPort 6000 / CN2600, CVE-2026-10831: unauthenticated network commands can disrupt active serial sessions (CVSS 4.0 6.9). CISA SSVC records no observed exploitation and not automatable. [5][46]
Access needed	Rockwell/Moxa: network path to affected device. Siemens: access to a CPU for offline key recovery, then potential follow-on misuse. Unitronics: network access to exposed controller services.
Check now	Validate exact controller family/firmware with the integrator; remove unnecessary internet exposure. Test authorised change paths and applicable RUN/key-switch protections without assuming they mitigate every exploit condition.
Fix	Rockwell: implement Rockwell PN1550 compensating controls (CIP Security/1783-CSP, segmentation and least-privilege engineering access); the advisory lists no corrective patch. Siemens: apply current vendor branch-specific mitigations and migrate legacy protected communication. Unitronics: use VisiLogic 9.9.00 or later with compatible updated controller OS per the vendor advisory (OS 12.38; release bundle 4.12.38); verify retained-memory initialization and modem compatibility before any upgrade. Moxa: request NPort v2.3.9 / CN2600 v4.6.11 security patches through vendor support. [1][3][5][42]
Detect	New engineering-workstation connections to PLCs; program downloads or mode changes outside work orders; serial session drops on converters.

B. Airfield ground lighting (AGL / ALCMS / ILCMS) and stand systems

What is inside	Control servers and Windows HMIs, PLC or proprietary links to constant-current regulators, field monitoring; A-VDGS and boarding bridges use PLCs and vendor IP interfaces.
Exploitable vulnerabilities	No ADB SAFEGATE AGL-specific CISA ICS advisory was identified in this source review. Exposure analysis therefore centres on confirmed component versions, workstation OS, control-server configuration and supplier access; a 2025 US Windows 7 ALCMS tender is illustrative only, not proof of an APAC deployment. [25]
Access needed	Internal network, or vendor remote-support path.

Check now	Record HMI and server operating-system versions; list every vendor remote-access route into the ALCMS; confirm the lighting control network is not shared with general terminal IT.
Fix	Plan OS upgrades with the vendor; enforce on-request, MFA-protected vendor access; keep tested offline backups of ALCMS configuration; confirm local and manual lighting control works.
Detect	Logons to ALCMS servers outside maintenance windows; configuration changes not linked to work orders; unexpected outbound traffic from the lighting network.

C. Fuel hydrant and tank gauging

What is inside	Automatic tank gauges (ATG), leak detection, pump and valve PLCs, serial-to-IP converters.
Exploitable vulnerabilities	Veeder-Root TLS4B: CVE-2025-58428 affects an authenticated SOAP web-service interface and may permit system command execution; CVE-2025-55067 concerns a time/2038 rollover condition with potential availability effects if system time is manipulated. No in-the-wild exploitation was established by the cited advisory. [6][7]
Access needed	CVE-2025-58428: network path plus valid credentials; CVE-2025-55067: conditions enabling system-time error/manipulation. Internet exposure is not a prerequisite for every scenario.
Check now	Find ATG consoles at airport fuel farms; confirm none is internet-reachable; change default or shared credentials.
Fix	For both TLS4B issues (CVE-2025-58428 and CVE-2025-55067), verify installation of vendor firmware 11.A or later as applicable; confirm device variant and implementation with Veeder-Root. Limit SOAP/ATG management to authorised hosts, review credentials and audit changes; test time/date functions during approved maintenance. [6][7]
Detect	ATG log-ins and configuration changes outside work orders; alarm suppressions; product-level changes not matching deliveries.

D. Building management (BMS / HVAC)

What is inside	Supervisors and JACE-class controllers, BACnet/IP and Modbus field devices, energy meters.
Exploitable vulnerabilities	Niagara Framework: Nozomi reported multiple 2025 issues that may enable high-impact chains when insecurely configured. Separately, Tridium disclosed CVE-2026-11804 (July 2026), a program-module privilege-escalation issue affecting specified Niagara 4.14u5/4.15u4 branches. No aviation-specific exploitation confirmed. [8][9][43]
Access needed	Depends on flaw: internal reachable Fox/web services and/or existing elevated privileges (2026 program-module issue). Do not assign a single access prerequisite to all Niagara CVEs.
Check now	Identify Niagara stations and versions; confirm TLS is enabled on Fox and web interfaces; confirm BMS is not reachable from guest or general corporate networks.
Fix	Apply a vendor-confirmed fixed build for each affected branch. For CVE-2026-11804, Tridium specifies 4.14u6 / 4.15u5 or corresponding module patches. Older 2025 findings require their own version mapping; use Niagara Hardening Guide and vendor-approved maintenance process. [43]
Detect	Fox or web sessions from unexpected hosts; changes to encryption settings; new station-to-station connections.

E. Physical security and life safety

What is inside	Access control (airside doors and turnstiles), CCTV and VMS, fire alarm management workstations.
Exploitable vulnerabilities	Hikvision CVE-2021-36260: previously exploited unauthenticated command injection; KEV-listed, applicable only to affected firmware. [10][11] Johnson Controls: C-CURE/victor CVE-2026-21655 (deserialisation/RCE), CVE-2026-21653 (SSRF), and victor Web CVE-2026-34496; component and access preconditions differ. [12][47] Simplex Incident Manager CVE-2026-27875: local, low-privilege credential exposure from memory; no public exploitation confirmed. [13]
Access needed	Hikvision: network to affected service, potentially internet if exposed. C-CURE/victor: route and privileges vary by CVE/component. Simplex: local host access with low privileges.
Check now	Search camera fleet for affected Hikvision firmware and any internet exposure; list C-CURE 9000/victor versions; confirm VMS and access-control servers sit in their own zone.
Fix	Update Hikvision per affected model/firmware. For C-CURE 9000, victor Application Server and victor Web, apply component-specific JCI advisories and fixed builds (do not substitute one product version for another). Simplex: the CISA advisory inconsistently cites patched v2.01.01 and an upgrade recommendation of v1.01.05 or later; obtain written vendor confirmation of the applicable fixed branch before change approval. Restrict local access and monitor for credential dumping. [12][13][47]
Detect	Inbound connections to camera web services; outbound traffic from cameras; new sessions to C-CURE/victor servers from IT subnets.

F. Remote-access edge (the usual entry route)

What is inside	VPN gateways, application delivery controllers and firewalls used by staff and vendors to reach airport and airline networks.

Exploitable vulnerabilities (KEV, Sep–Oct 2026)	Selected edge CVEs from Rev3 include Cisco CVE-2026-20079, Citrix CVE-2026-19490 / CVE-2026-88771 / -88772 / -88779, PAN-OS CVE-2026-0322 and Fortinet CVE-2025-25249 / CVE-2025-61624. Verify each product, exploitation status and prerequisites against live vendor/CISA records; the list is not exhaustive. [14][15] CISA confirmed exploitation of Ivanti Connect Secure CVE-2026-104935 (KEV 13 Oct), CVE-2026-111357 and CVE-2026-118527 (KEV 30 Oct), with in-memory activity capable of evading a clean Integrity Checker Tool result. [39][40]
Access needed	CVE-specific: a reachable service is required; some flaws are unauthenticated, whereas others may require authentication, role or a prerequisite vulnerability. “Internet-facing” is a screening criterion, not a universal exploit prerequisite.
Check now	Reconcile gateway/firmware inventory with vendor advisories and CISA KEV. For affected Ivanti devices, check updated versions and assess compromise using network/memory evidence, not ICT output alone. [39][40]
Fix	Prioritise vendor-supported fixed releases, preserving available volatile evidence when compromise is suspected. For exploited Ivanti CVEs, coordinate reset/rebuild, password/token/API-key and certificate remediation under incident-response procedures. Use monitored, MFA-protected vendor access via approved jump hosts. [39][40]
Detect	New gateway administrator/session activity; anomalous VPN authentication; new trusted devices or certificates; unknown outbound connections from appliances; paths from VPN into engineering, BHS or operational support zones; signs of web shell or data exfiltration.

G. Air navigation, surveillance and datalink (ANSP)

What is inside	ADS-B ground stations, MLAT, radar; GNSS/GBAS, ILS, DME; VHF datalink ground stations; ATM automation (e.g. ManagAir, TopSky) and voice switches.
Exploitable vulnerabilities	ATN-B1 CPDLC research, ICSA-26-219-01 (CVE-2025-71409–71413): laboratory-demonstrated injection/disconnection conditions over legacy RF links. Do not infer observed malicious interference in operational airspace or a universally exploitable path. [16][17] ADS-B/ACARS authenticity limitations are documented in research; GNSS RFI is separately evidenced by APAC authorities. These are distinct protocols and threat scenarios. [18][19][32]
Access needed	Specific radio-frequency access and protocol preconditions for CPDLC/ADS-B. GNSS interference may have unintentional or intentional causes; attribution requires additional evidence.
Check now	Confirm conventional navaids and radar coverage around GNSS-sensitive approaches; confirm CPDLC session-reset monitoring exists.
Fix	Use ICAO APAC V1.0 (non-binding regional GNSS RFI/data-link reporting and coordination guidance), plus regulator/ANSP procedures. Rehearse voice reversion and terrestrial navigation/surveillance fallbacks; assess Galileo OSNMA-capable receivers for appropriate non-safety-critical PNT use only after aviation approval, not as a universal operational solution. [19][45]
Detect	Clusters of degraded ADS-B navigation integrity (NIC); repeated CPDLC resets across several aircraft; crew RFI reports.

H. Shared passenger and airline platforms (IT dependency, not OT)

What is inside	Common-use check-in and bag-drop, passenger service systems, AODB, FIDS, baggage messaging.
Observed weakness	Confirmed third-party reservation-data access: JAL/JTA reported ~92,000 affected customers and Cathay reported ~53,000 affected bookings; these are different units and must not be added as individuals. Both airlines explicitly said their flight operations were unaffected. Other airlines require independent confirmation. [27][28] Amadeus unauthorised reservation-data access was disclosed by airlines in October 2026.
Access needed	Compromised supplier service-account credentials / external access to Amadeus reservation data; no confirmed airport OT access or flight-operation disruption. [27][28]
Check now	List which shared platforms your check-in, bag-drop and FIDS depend on, and each supplier’s incident-notification commitment.
Fix	Contract terms for notification time, recovery time and manual-mode support; rehearsed manual procedures with printed reference material.
Detect	Supplier incident notifications; unexpected access to PNR data; abnormal service-account login or export patterns; message-queue failures between check-in, baggage and flight-information systems; time to manual fallback.

5. Protocol watchlist

Protocol	Used for	Native authentication	Secure option	What operators should do
ADS-B (1090ES)	Aircraft position to ATC	No	None standardised	Cross-check with MLAT and radar; monitor NIC anomalies
ACARS	Airline and ATC messages	No	ACARS Message Security (ARINC 823)	Treat uplinks as untrusted unless secured; confirm via voice where safety-relevant
CPDLC over ATN-B1	Controller–pilot clearances	Legacy baseline has no general native auth	No retrofit protocol fix for surveyed ATN-B1 weaknesses	Monitor resets; maintain voice reversion

Protocol	Used for	Native authentication	Secure option	What operators should do
Civil GNSS	Navigation, ADS-B, ground timing	Depends on constellation/receiver; no universal authentication	Galileo OSNMA authenticates navigation messages (receiver support required); not anti-jam or authenticated ranging	Preserve independent navaids and timing, detect discrepancies, verify certified receiver capability and approval. [45]
BACnet/IP	BMS, HVAC	No	BACnet Secure Connect (TLS)	Zone the BMS; plan BACnet/SC for new works
Modbus TCP	Meters, fuel, power	No	Modbus/TCP Security (TLS)	Allow TCP/502 only from named masters
S7comm / PROFINET / EtherNet/IP	BHS and ground-equipment PLCs	No (legacy)	S7comm-plus with TLS; PROFINET Security Classes; CIP Security	Restrict engineering access to named workstations; enable secure modes on new installs

6. Prioritisation

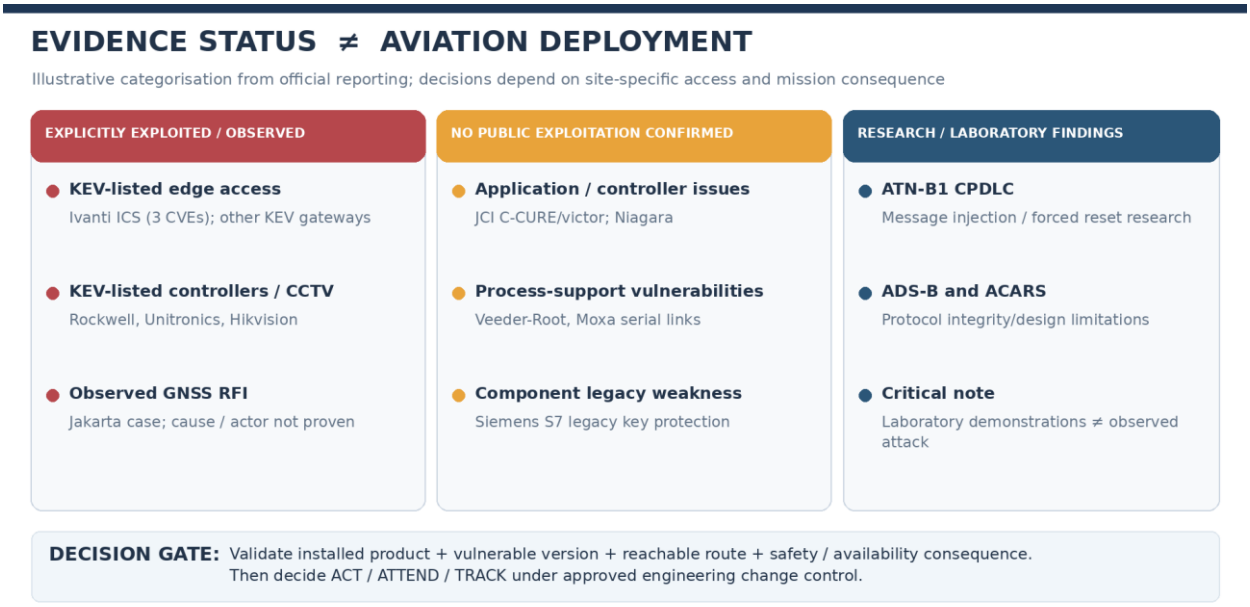

Figure 2. Evidence classes and OT-ISAC decision gates. Categories are not measured airport exposure and are not a substitute for CISA SSVC records.

Item / pathway	Evidence	Access / prerequisites	Effect if exploited	Applicability to aviation	Decision*
Ivanti / other KEV edge gateways	Active exploitation (CISA)	Affected service; prerequisites differ	Gateway takeover, credential exposure / lateral access	High when supports vendor or OT access	ACT if exposed
Hikvision CVE-2021-36260	KEV exploited	Network to affected firmware	Camera/NVR code execution	Site-specific security network	ACT if affected
Rockwell CVE-2021-22681	KEV exploited	Network path to Logix controller	Unauthorised controller changes possible	Only if deployed in BHS or ground systems	ACT if reachable
Unitronics CVE-2023-6448	KEV exploited	Network to affected device; insecure defaults	Controller access / process manipulation	Only where devices are confirmed	ACT if exposed
GNSS RFI (not a CVE)	Observed APAC interference	RF propagation; cause often unknown	Degraded navigation/timing and workload	ANSP / aircraft / select ground systems	ACT: procedures
Veeder-Root CVE-2025-58428	No reported exploitation	Authenticated SOAP service and network access	Potential system command execution	Only if TLS4B deployed	ATTEND

Item / pathway	Evidence	Access / prerequisites	Effect if exploited	Applicability to aviation	Decision*
JCI C-CURE / victor	No reported exploitation	Depends on specific component/CVE	Server compromise or service impact	Physical security / access control	ATTEND
Tridium Niagara, 2025/2026	No reported exploitation	Flaw-specific; some privileges required	BMS supervisor/control risks	Only if Niagara deployed	ATTEND
Siemens CVE-2022-38465	No reported exploitation	Offline family-key extraction prerequisite	Legacy protected comms exposure	Where relevant S7 family is installed	ATTEND
Moxa CVE-2026-10831	No reported exploitation; SSVC No auto	Network to command port	Serial-session disruption	Depends on connected system	TRACK / ATTEND
ATN-B1 CPDLC / ADS-B / ACARS	Lab research / design issues	RF and protocol-specific conditions	Operational workload / integrity concerns	ANSP; not proven exploitation	TRACK: procedures
JCI Simplex CVE-2026-27875	No reported exploitation	Local host privileges	Credential exposure	Only on affected host	TRACK / ATTEND

* Decisions are illustrative OT-ISAC judgements, NOT formal CISA SSVC outcomes. Re-score by verified installation, attacker accessibility, operational/safety criticality, change constraints and recovery capability. “No reported exploitation” does not prove none has occurred.

7. Observed incidents and GNSS interference

Figure 3. Selected incidents and disclosures. Dates represent occurrence, observed access periods or disclosure (as labelled). Hollow markers denote an incident outside APAC, included as operational precedent.

Date	Event	What was reported	Confidence	Source
26 Dec 2024	Japan Airlines – DDoS	Network equipment hit from about 07:24; automated baggage check-in and same-day ticket sales affected; flight delays reported. No data leak or safety impact reported.	Confirmed	[29]
23 Mar 2025	KLIA (MAHB)	NACSA and MAHB confirmed an attack on KLIA computer systems and said operations were unaffected; other sources reported FIDS, check-in and baggage handling disrupted for hours. Ransom demand of USD 10 million refused. Attribution not confirmed.	Confirmed (attack); Possible (impact)	[30][31]
19–22 Sep 2025	Collins MUSE (Europe)	ENISA confirmed ransomware on the shared check-in and bag-drop platform; manual processing at several airports; large-scale cancellations at Brussels.	Confirmed	[26]
8 Apr 2026	Jakarta terminal-area GNSS interference (mechanism suspected)	Indonesia reported a ~3-hour 8 April event affecting 44 flights across seven operators; 39 of 112 observed flights showed degraded ADS-B NIC. Government paper describes suspected GNSS jamming, not confirmed hostile attribution. [32]	Confirmed interference; cause not attributed	[32]
Aug 2023–Sep 2026 access; Oct 2026 disclosure	Amadeus passenger service system	Amadeus PSS third-party reservation-data exposure: JAL/JTA said ~92,000 customers had records accessed (Amadeus notification 23 Oct); Cathay reported ~53,000 affected bookings (notification 28	Confirmed for JAL/JTA and Cathay; other carriers not	[27][28]

Date	Event	What was reported	Confidence	Source
		Oct). Access traces span Aug 2023–Sep 2026. Both confirmed no effect on their flight operations; no aviation OT compromise established. [27][28]	independently assessed	

Figure 4. GNSS evidence snapshots (different geographies and observation periods; not a single APAC total). Sources: India Ministry of Civil Aviation, March 2026 [44], and Indonesia CNS SG/30 paper, July 2026 [32].

Threat actors

Among the reviewed public sources up to 3 November 2026, OT-ISAC did not substantiate a specifically attributed intrusion into an APAC airport or ANSP airside-control network. This is a bounded open-source finding, not proof that such activity has never occurred. Documented campaigns against aviation IT and separately against exposed OT elsewhere inform defensive scenarios, not airport-specific attribution.

Actor (as named by source)	Documented aviation-related activity	Relevance to APAC aviation OT
Scattered Spider	FBI warned in 2025 that the group expanded targeting to airlines; help-desk social engineering, MFA manipulation [36]	Identity compromise leading to remote access into airline and airport networks
Qilin (ransomware)	A relevant identity-led entry pathway to airline or airport IT; no proof of APAC aviation OT intrusion by this actor.	Validate exposure of help-desk, identity, supplier support and VPN-to-OT trust boundaries; do not attribute unrelated events.
IRGC-affiliated actors (CyberAv3ngers)	Exploited internet-exposed Unitronics PLCs with default credentials across sectors (CISA AA23-335A) [37]	Any small PLC/HMI on the internet, including ground equipment
Pro-Russian hacktivists (NoName057(16))	Claimed DDoS against Milan airport websites, December 2024 [38]	Availability of public-facing and booking services

8. Action plan

Timeframes are recommended planning windows, not permission to bypass safety assurance or operational change control. For 24/7 airside, baggage and CNS/ATM systems, coordinate with owners, integrators and ATC where applicable. Prioritise suspected gateway compromise and immediate exposure containment; schedule production OT changes only after safety and availability checks.

Operational constraints this plan accounts for

- Split ownership: airport operator, airlines, ground handlers, fuel consortia, ANSP and concessionaires each own part of the estate; baggage systems are often run by the integrator under an operations contract.
- 24/7 operations: work windows are short and overnight; airfield lighting changes need ATC coordination, and peak travel seasons bring change freezes.
- Safety assurance: changes to airfield lighting, navaids and ATC systems may require a safety assessment and regulator acceptance before deployment.
- Vendor dependency: integrators often own the PLC code and firmware access; self-patching may affect warranty or certification.
- Limited visibility: OT components are rarely in the IT asset register, and vendor cellular or cloud links do not show in external scans.
- Unpatchable elements: legacy HMIs and radio protocols (ADS-B, ACARS, CPDLC) need isolation, monitoring and procedure instead of patches.

When	Action	Who	Depends on	Interim if late	Done when
72 hours	Inventory internet-facing VPN/ADC/firewall and vendor gateways; apply active KEV/vendor fixes and trigger compromise triage for affected Ivanti systems.	All – IT Security	Change approval; failover window	Restrict access, collect logs and preserve forensic evidence before disruptive resets where possible.	Asset/firmware status verified; fixed or isolated; suspected compromise investigated, actions recorded.
72 hours	Use passive inventory and authorised, non-intrusive external exposure assessment for PLC, HMI, cameras, ATG, BMS and access control. No unapproved active OT scans.	All – IT Security	OT engineering authorisation for active probes; documented safe method and window	Review firewall/NAT rules, asset registers, cloud/cellular inventory; block unnecessary reachability after owner approval.	Reachable management endpoints listed, validated and remediated without unplanned OT disruption.
72 hours	Check camera estate for CVE-2021-36260; list any known Rockwell Logix or Unitronics devices	Airport operator – Facilities (OT Eng.)	Accuracy of asset records	Block camera and NVR internet access	Affected devices listed with owner
30 days	Census of vendor remote connections: written request to baggage, airfield lighting, fuel, BMS and boarding-bridge integrators for every path, including cellular modems	Airport operator; fuel operator – Procurement (OT Eng.)	Integrator responses	Disable always-on vendor accounts when not in use	Register of every vendor path with an owner
30 days	Obtain a component bill of materials from each integrator: controllers, firmware, operating systems, remote-access method	Airport operator; fuel operator – OT Eng. (Procurement)	Integrator cooperation; contract terms	Use Cards A–E to ask about the highest-risk components first	Component data held for each system
30 days	Restrict network access to PLCs, ALCMS servers, BMS, fuel gauges and access-control servers with ACLs	Airport operator – Network (OT Eng.)	Confirm SCADA and monitoring polling still works	–	ACLs in place and documented
30 days	Plan vendor-approved fixes/compensating controls for Cards A–E; Rockwell PN1550 requires mitigations rather than assuming a corrective firmware patch.	Airport operator; fuel operator – OT Eng. (Integrators)	Integrator availability; ATC coordination for airfield systems; change freezes	ACLs above; monitor configuration changes	Each change or compensating control has an owner, documented acceptance criteria and scheduled revalidation.
30 days	Confirm manual fallback for check-in, bag-drop, baggage sortation and FIDS: named decision-makers, printed procedures, staffing for 24 hours	Airport operator; airlines; ground handlers – Operations	Agreement across parties	–	Fallback plan signed off by each party

When	Action	Who	Depends on	Interim if late	Done when
30 days	Review ICAO APAC V1.0 GNSS RFI / associated data-link disruption coordination and reporting guidance; map to national and ANSP procedures.	ANSP – Operations (CNS Eng.)	Internal procedure approval	Interim controller briefing	Applicable procedure issued, controllers briefed and report escalation pathway tested.
90 days	Apply approved fixes and verify telemetry/control functionality; create end-of-support HMI/OS replacement plan with interim isolation and rollback criteria.	Airport operator; fuel operator – OT Eng. (Integrators)	Safety assessment where airfield or navigation systems are affected; overnight windows	ACLs and change monitoring stay in place	Fixed versions installed, or replacement plan recorded
90 days	Confirm CPDLC reset monitoring and ADS-B/MLAT cross-checks; rehearse voice reversion	ANSP – CNS Eng. (Operations)	System capability; roster time	Controller briefing only	Monitoring live; reversion rehearsed
90 days	Exercise a shared-platform outage combined with a baggage or FIDS failure; measure time to stable manual operation	Airport operator; airlines; ground handlers – Crisis Mgmt	Availability across parties	–	Times recorded; improvement plan owned
90–180 days	Zone baggage, physical-security, BMS and fuel networks with controlled conduits; route vendor access through an MFA-protected, monitored jump host	Airport operator – Network (Security)	Network redesign; integrator agreement	ACLs from the 30-day action	Firewall rules match documented conduits
At next contract renewal	Add notification-time, recovery-time and manual-mode support terms for shared passenger platforms and OT integrators	Airport operator; airlines – Procurement	Contract cycle	Written supplier commitments in the meantime	Terms included in renewed contracts

Operational monitoring: first 0–72 hours – correlate remote-access authentications, privileged session changes, gateway-to-OT flows, supplier notices, new engineering connections, GNSS RFI/CPDLC reset reports and safety-system alarms. Record baseline and evidence before emergency remediation. Do not create new logging traffic that could destabilise OT.

Within 3–30 days – validate SIEM/OT sensor coverage with integrators; compare configuration changes to signed work orders; test escalation to ANSP/airport operations for GNSS or communications anomalies; confirm manual processing and controlled recovery procedures.

Evidence gaps / collection priorities – exact installed make/model/version, reachable services and authentication requirements; vendor cellular/cloud access; whether a vulnerable system supports safety or merely passenger processing; independent confirmation of any claimed OT impact or actor attribution.

9. Intelligence gaps and how to contribute

- Which controller families and firmware sit inside APAC BHS, AGL and fuel systems? Integrator bills of materials shared anonymously would let OT-ISAC issue targeted alerts.
- What failed at KLIA in March 2025, and how long did manual operation take?
- Have GNSS interference events affected ground systems (timing, ADS-B ground stations) in your area?
- EVA Air and Evergreen Aviation Technologies reported network intrusions on 15 September 2026; Publicly available information remains insufficient to assess the scope and operational impact.

Share information through established OT-ISAC member channels, applying FIRST TLP 2.0 and existing information-sharing agreements. Do not disclose member network topology, vulnerabilities or supplier access paths in a TLP:CLEAR submission.

10. Sources

[1] Rockwell Automation – PN1550, revision 1.6 (10 Mar 2026), CVE-2021-22681; no corrective patch, mitigations available – https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1550.html

[2] SecurityWeek – Rockwell vulnerability exploited; KEV record (added 5 Mar 2026) – https://www.securityweek.com/rockwell-vulnerability-allowing-remote-ics-hacking-exploited-in-attacks/

[3] CISA – ICSA-22-286-04 Siemens SIMATIC S7-1200 and S7-1500 – https://cisa.gov/uscert/ics/advisories/icsa-22-286-04

[4] CISA – ICSA-23-348-15 Unitronics Vision and Samba – https://cisa.gov/news-events/ics-advisories/icsa-23-348-15

[5] Moxa – MPSA-262370, CVE-2026-10831, 16 Jun 2026 – https://moxa.com/en/support/product-support/security-advisory/mpsa-262370-cve-2026-10831-improper-authorization-vulnerability-in-serial-device-servers

[6] CISA – ICSA-25-296-03 Veeder-Root TLS4B – https://www.cisa.gov/news-events/ics-advisories/icsa-25-296-03

[7] CVE record – CVE-2025-58428 – https://db.gcve.eu/vuln/CVE-2025-58428

[8] Nozomi Networks – Tridium Niagara vulnerabilities, Jul 2025 – https://nozominetworks.com/blog/critical-vulnerabilities-found-in-tridium-niagara-framework

[9] CVE-2025-3940 record (fixed versions) – https://cvefeed.io/vuln/detail/CVE-2025-3940

[10] Rapid7 – CVE-2021-36260 analysis – https://www.rapid7.com/blog/post/ra-cve-2021-36260-analysis/

[11] CVE-2021-36260 KEV record – https://db.gcve.eu/vuln/CVE-2021-36260

[12] CISA – ICSA-26-204-01 Johnson Controls C-CURE 9000 and victor – https://www.cisa.gov/news-events/ics-advisories/icsa-26-204-01

[13] CISA – ICSA-26-232-01 Johnson Controls Simplex Incident Manager – https://www.cisa.gov/news-events/ics-advisories/icsa-26-232-01

[14] The Hacker News – CISA KEV additions, 9 Sep 2026 – https://thehackernews.com/2026/09/cisa-flags-exploited-cisco-citrix.html

[15] Safeguard – Edge device zero-days, Oct 2026 (secondary; verify against CISA KEV) – https://safeguard.sh/resources/blog/edge-device-zero-days-october-2026

[16] CISA – ICSA-26-219-01 CPDLC over ATN-B1 (bulletin, 7 Aug 2026) – https://content.govdelivery.com/accounts/USDHSCISA/bulletins/423fbf3

[17] CVE-2025-71413 record – https://app.opencve.io/cve/CVE-2025-71413

[18] SecurityWeek – ADS-B spoofing research – https://www.securityweek.com/air-traffic-control-systems-vulnerabilities-could-make-unfriendly-skies-black-hat/amp/

[19] ICAO APAC – GNSS RFI and Data Link Disruption Guidance V1.0, Aug 2026 – https://www.icao.int/sites/default/files/APAC/Documents/edocs/ATM/Asia_Pacific-Regional-Guidance-for-GNSS-and-Datalink-Version-1.0.pdf

[20] Future Travel Experience – Vanderlande BHS at two Vietnamese airports, May 2024 – https://www.futuretravelexperience.com/2024/05/vanderlande-to-provide-baggage-handling-systems-at-two-vietnamese-airports/

[21] AviationPros – ADB SAFEGATE AGL at Bhogapuram, Jul 2024 – https://www.aviationpros.com/directory/airport-facilities-buildings/press-release/55093791/adb-safegate-adb-safegate-to-bring-airfield-ground-lighting-technology-to-new-greenfield-airport-project-at-bhogapuram

[22] Asian Aviation – Indra ATM upgrade in Indonesia, Mar 2025 – https://asianaviation.com/indra-wins-deal-to-upgrade-atm-in-indonesia

[23] TechNode Global – CAAS awards Thales NexGen ATMS, 30 Jul 2026 – https://technode.global/2026/07/30/singapore-awards-frances-thales-contract-for-ai-enabled-air-traffic-management-system-towards-2030-launch/

[24] Airport Technology – Sydney Airport SITA contract, Mar 2021 – https://www.airport-technology.com/news/sydney-airport-technology-contract-sita/

[25] SAM.gov – ALCMS upgrade from Windows 7 (Moody AFB) – https://sam.gov/opp/68c3d1d0e3c24c4491b805997fa41fb0/view

[26] TechCrunch – ENISA confirms ransomware on MUSE, 22 Sep 2025 – https://techcrunch.com/2025/09/22/eu-cyber-agency-confirms-ransomware-attack-causing-airport-disruptions/

[27] Japan Airlines / Japan Transocean Air – Official Amadeus PSS incident notice, 30 Oct 2026 (~92,000 customers; operations unaffected) – https://www.jal.co.jp/en-jp/news/general/2026/other/261028.html

[28] Cathay Pacific – Official third-party reservation-data incident notice, 30 Oct 2026 (~53,000 bookings; operations unaffected) – https://www.cathaypacific.com/cx/es_ES/latest-news/security-and-operational-changes/personal-data-security.html

[29] Japan Times – JAL cyberattack, 26 Dec 2024 – https://japantimes.co.jp/news/2024/12/26/japan/jal-cyberattack

[30] The Edge Malaysia – NACSA/MAHB statement, 25 Mar 2025 – https://theedgemalaysia.com/node/749241

[31] New Straits Times – KLIA cyberattack, 26 Mar 2025 – https://www.nst.com.my/amp/news/nation/2025/03/1193233/cyberattack-mahb-hackers-yet-be-identified

[32] ICAO APAC – Indonesia WP32, GNSS RFI mitigation, Jul 2026 – https://www.icao.int/sites/default/files/APAC/Meetings/2026/Workshop%20on%20achieving%20High%20Resilience%20in%20Sustaining%20Operations%20of%20Critical%20Aeronautical%20Infrastructure%20and%20CNS%20SG30/03-Working%20Papers/WP32_IDN-AI.6.2-GNSS-RFI-MITIGATION-IN-INDONESIA.pdf

[33] GPS World / India Ministry of Civil Aviation – Historical 1,951 GNSS reports (Nov 2023–Nov 2025); superseded by [44] – https://www.gpsworld.com/?p=113506

[34] ICAO APAC DGCA/60 – IATA paper on GNSS RFI, 2025 – https://www.icao.int/sites/default/files/APAC/Meetings/2025/2025%20DGCA60/Agenda%20Item04-Air%20Navigation/60-DP-04-15%20GNSS%20RADIO%20FREQUENCY%20INTERFERENCE%20%28RFI%29%20%E2%80%93%20IMPACTS%20TO%20AIRSPACE%20USERS.pdf

[35] ESET – APT Activity Report Q2–Q3 2026 – https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2026-q3-2026.pdf

[36] PolySwarm – Cyber threats targeting aviation and aerospace in 2026 – https://blog.polyswarm.io/turbulence-ahead-cyber-threats-targeting-aviation-and-aerospace-in-2026

[37] CISA – AA23-335A IRGC-affiliated actors exploit PLCs – https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[38] Asero – JAL DDoS brief, including Milan airports NoName057(16) claim – https://asero.com/?p=1387

[39] CISA – Alert updated 30 Oct 2026, three exploited Ivanti Connect Secure CVEs – https://www.cisa.gov/news-events/alerts/2026/10/13/cisa-urges-patching-newly-exploited-vulnerability-ivanti-connect-secure

[40] Rapid7 – Ivanti Connect Secure 30 Oct zero-day fix mapping and investigation guidance (2 Nov 2026) – https://www.rapid7.com/blog/post/etr-additional-ivanti-connect-secure-zero-days-exploited-in-the-wild-cve-2026-111357-cve-2026-118527/

[41] CAAS – Air navigation services capabilities; NexGen ATMS target completion 2030, 22 Jul 2026 – https://www.caas.gov.sg/resources/media-and-publication/newsroom/caas-upgrades-air-navigation-services-capabilities-to-meet-rising-demand-for-air-travel/

[42] Unitronics – Security Advisory 2023-001 (CVE-2023-6448), VisiLogic/OS fixes – https://downloads.unitronicsplc.com/Sites/plc/Technical_Library/Unitronics-Cybersecurity-Advisory-2023-001-CVE-2023-6448.pdf

[43] Tridium – Security Bulletin SB 2026-Tridium-1 (CVE-2026-11804), July 2026 – https://pages1.tridium.com/index.php/email/emailWebview?email=ODA4LVNHTS0yNzEAAAGjCdbq3XkYeIW42RyXb14WuPzU8ImJlYku9tA9LURVXyITdNNapFwjuyLxX4RmyQ3Ar5ar5SJkVuGdYO5dzwLS5co8JteZiu4J

[44] Government of India, Ministry of Civil Aviation – Lok Sabha Q3233, 12 Mar 2026 (GNSS reports to Feb 2026) – https://sansad.in/getFile/loksabhaquestions/annex/187/AU3233_OJcXSG.pdf?source=pqals

[45] European Commission – Galileo Open Service Navigation Message Authentication declared operational 24 Jul 2025 – https://defence-industry-space.ec.europa.eu/galileos-osnma-authentication-service-now-operational-2025-08-25_en

[46] CISA-ADP SSVC enrichment for Moxa CVE-2026-10831, embedded in official CVE record (CIRCL viewer) – https://vulnerability.circl.lu/vuln/cve-2026-10831

[47] Johnson Controls – Product Security Advisories (C-CURE 9000, victor/victor Web and Simplex Incident Manager) – https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories

About this report

• Prepared by OT-ISAC for aviation-sector practitioners and APAC critical infrastructure stakeholders. TLP:CLEAR under FIRST TLP 2.0; public dissemination permitted.

• This source-validated version distinguishes publicly documented events from OT-ISAC assessments, and includes evidence gaps. It is not an airport inventory, product certification, penetration test or regulatory compliance assessment. Independently verify affected versions against vendor advisories before remediation.