ADS-C / CPDLC IMPLEMENTATION CHECKLIST

Requirements and readiness checks for ICAO SMEs across nine technical areas



ICAO

GROUND SYSTEMS // CSP // AIRCRAFT // INFRASTRUCTURE // INTERFACES // REDUNDANCY // RECORDING // CYBERSECURITY // TESTING

NOVEMBER 2026

Nine areas to verify before go-live

01

Ground systems

ATSU automation and data link processing

02

Communication service provision

CSP agreements and service levels

03

Aircraft capabilities

Equipage, approvals and PBCS eligibility

04

Infrastructure

Subnetworks, ground links and coverage

05

Interfaces

ATM systems, neighbouring ATSUs, CSP links

06

Redundancy

Failover, diversity and voice fallback

07

Recording and monitoring

Evidence, performance tracking, reporting

08

Cybersecurity

Protection of links, systems and data

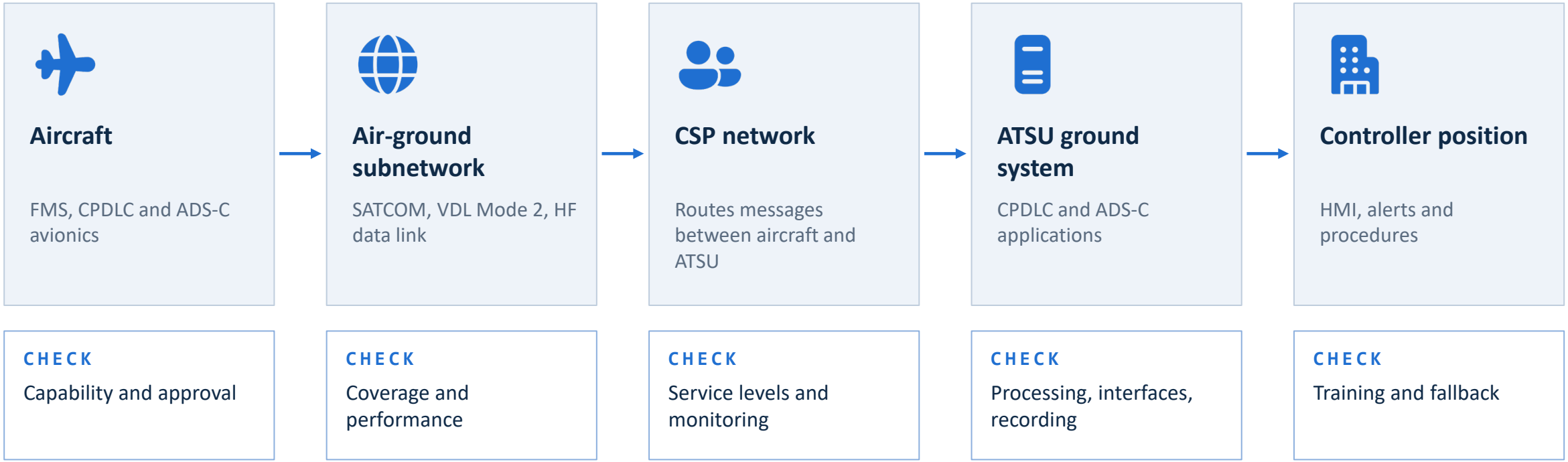
09

Testing and validation

Verification before and during operations

Each area is developed on its own slide as a checklist, with ICAO references and a check question for SMEs.

How ADS-C and CPDLC work end to end



ADS-C Contract-based position and intent reports from the aircraft: periodic, event or demand.

CPDLC Text message exchange between controller and pilot, replacing routine voice exchanges.

Ground systems: the ATSU data link core

IMPLEMENTATION CHECKLIST

- **Data link processing**
  CPDLC and ADS-C applications integrated with flight data processing
- **Logon and connection management**
  Current and next data authority, and transfer of CPDLC connections
- **Message set support**
  Uplink and downlink messages aligned with PANS-ATM and GOLD
- **ADS-C contract management**
  Periodic, event and demand contracts, with controlled report load
- **Controller HMI and alerting**
  Message display, response timers, error alerts and voice fallback

ICAO REFERENCES

- Annex 10, Vol. II and III: aeronautical telecommunications
- Doc 4444 (PANS-ATM): CPDLC and ADS-C procedures
- Doc 10037 (GOLD): global operational data link guidance

SME CHECK

Can the ATSU show end-to-end handling of logon, contracts and transfers with every adjacent FIR?

Service provision: CSP responsibilities

IMPLEMENTATION CHECKLIST

- **Service agreements**
  Roles of ANSP, CSP and operators are formally defined
- **Service performance**
  Delivery within the allocated RCP and RSP transit time and availability
- **Monitoring and reporting**
  Regular performance reports and prompt outage notification
- **Change management**
  Coordinated notice of network upgrades and routing changes
- **Incident response**
  Contact points, escalation paths and recovery targets for interruptions

ICAO REFERENCES

- Doc 9869 (PBCS Manual): RCP and RSP, roles of CSPs
- Annex 10, Vol. II: aeronautical telecommunication service
- Doc 10037 (GOLD): ANSP, CSP and operator responsibilities

SME CHECK

Does every CSP agreement map to the RCP and RSP specifications that the State has prescribed?

Aircraft: equipage, approval, eligibility

IMPLEMENTATION CHECKLIST

- **Data link equipage**
  FANS 1/A or ATN B1 avionics with CPDLC and ADS-C functions
- **Airworthiness and operational approval**
  Approval by the State of the Operator for the airspace in use
- **PBCS eligibility**
  Authorisation for RCP 240 or 400, and RSP 180 or 400, where prescribed
- **Flight plan indication**
  Item 10 J-codes and Item 18 RCP and RSP entries filed correctly
- **Crew procedures**
  Training on message handling, abnormal cases and voice fallback

ICAO REFERENCES

- Doc 9869 (PBCS Manual): performance-based approvals
- Doc 10037 (GOLD): aircraft and operator procedures
- Annex 6: operation of aircraft, equipage and approval

SME CHECK

How does the State verify that aircraft entering the airspace are approved and correctly filed?

Infrastructure: links, ground network, sites

SUBNETWORK	TYPICAL ROLE	WHAT TO VERIFY
SATCOM	Oceanic and remote airspace	Satellite coverage, latency, handover between beams
VDL Mode 2	Continental, high-density airspace	VHF ground station coverage, channel capacity
HF data link	Polar regions and backup	Ground station availability and propagation limits

GROUND NETWORK

- Secure links between CSP and ATSU
- Managed bandwidth and latency
- Diverse physical routes

SITES AND POWER

- Protected power with backup
- Environmental controls
- Physical access control

COVERAGE VERIFICATION

- Compare coverage to FIR boundary
- Check against RCP and RSP
- Re-survey after network changes

Interfaces: every connection is specified

CSP NETWORK

Message formats, addressing, acknowledgements and link health status

ADJACENT ATSUS

Transfer of communications, AIDC or OLDI coordination, next authority notification

ATSU DATA LINK SYSTEM

- CPDLC application
- ADS-C application
- Logon and connection management
- Message validation and timers
- Versioned interface control documents

FDP AND ATM AUTOMATION

Flight plan correlation, route data and ADS-C reports to surveillance tools

RECORDING AND MONITORING

Time-stamped message feed, performance statistics and alarms

SME CHECK Interface control documents are agreed, versioned and tested for every link.

Redundancy: no single point of failure

LAYER	DESIGN MEASURE	VALIDATE BY
Air-ground link	Diverse subnetworks where equipped, with automatic link selection	Link loss and switchover tests
CSP and network	Diverse routes and dual circuits, with no shared failure points	Route cut simulation
ATSU ground system	Redundant servers with hot standby and automatic failover	Failover with live contracts
Operations	Voice fallback, loss-of-data-link procedures and trained controllers	Exercises and drills

SME CHECK Has each failover been demonstrated, not just designed, and is the recovery time known?

Recording and monitoring: evidence and trends

RECORD

- All CPDLC messages and ADS-C reports, time-stamped in UTC
- Retention aligned with Annex 11 and accident investigation needs (Annex 13)
- Clocks synchronised across ATSU, CSP and recorder

MONITOR

- Measure actual performance against RCP and RSP
- Track transaction times, availability and continuity by CSP and subnetwork
- Real-time alarms for link or service degradation

REPORT

- Send problem reports to the Central Reporting Agency and regional groups
- Periodic performance reports to States and operators
- Track corrective actions to closure

SME CHECK Can the State show monitored performance against RCP 240 or 400 and RSP 180 or 400?

Cybersecurity: protect links, systems, data

Authentication and integrity

Verify message source and integrity across the data link path

Network protection

Segmentation, firewalls and encrypted links between CSP and ATSU

Access control

Role-based access, privileged accounts managed and logged

Threat monitoring

Intrusion detection, log review and joint incident response

Patch and configuration

Controlled updates, vulnerability management, secure baselines

CSP and supplier assurance

Security requirements and audit rights written into agreements

REFERENCES Annex 17 (Security) // Doc 9985 (ATM Security Manual) // ICAO Aviation Cybersecurity Strategy

Testing: prove it before live traffic

1 Acceptance

- Factory and site acceptance tests
- Functional checks of CPDLC and ADS-C
- Message set conformance

2 Integration

- Interface tests against each ICD
- CSP link and subnetwork tests
- Neighbouring ATSU transfers

3 Simulation

- Controller scenarios with test aircraft
- Failover and degraded modes
- Load and timing checks

4 Operational trial

- Live aircraft in shadow mode
- Measured RCP and RSP performance
- Problem reports resolved

5 Go-live

- Safety assessment approved
- Ongoing performance monitoring
- Regression tests per change

EXIT CRITERIA

RCP and RSP performance met, safety assessment approved, controllers trained, fallback proven.

KEEP VALIDATING

Every software, network or CSP change triggers regression tests and a performance check.

Implementation roadmap in five phases

1 2 3 4 5

ASSESS

- Gap analysis across nine areas
- Confirm RCP and RSP targets

DELIVERABLE

Gap report

DESIGN

- Architecture and redundancy
- CSP agreements and ICDs

DELIVERABLE

Approved design

BUILD

- Install and integrate systems
- Secure and configure links

DELIVERABLE

Integrated system

VALIDATE

- Acceptance and trials
- Safety assessment

DELIVERABLE

Validation report

OPERATE

- Go-live with fallback ready
- Continuous monitoring

DELIVERABLE

Monitoring reports

Readiness checklist across the nine areas

AREA	READINESS QUESTION	EVIDENCE
01 Ground systems	End-to-end CPDLC and ADS-C handling proven with all adjacent FIRs	Integration test report
02 CSP provision	Agreements map to the prescribed RCP and RSP	Signed agreements, reports
03 Aircraft	Approvals and flight plan entries verified	Approval register, FPL checks
04 Infrastructure	Coverage and link capacity meet airspace needs	Coverage survey, capacity study
05 Interfaces	Interface control documents agreed, versioned, tested	ICD set, test records
06 Redundancy	Failover demonstrated and voice fallback ready	Failover tests, procedures
07 Recording and monitoring	Messages recorded and performance measured	Recorder audit, monitoring reports
08 Cybersecurity	Risk assessment done and controls in place	Security assessment, test results
09 Testing	Exit criteria met and regression suite in place	Validation report, safety case

Common risks and how to mitigate them

RISK	MITIGATION
Poor CSP performance goes undetected	Independent monitoring against RCP and RSP, with reporting in agreements
Aircraft filed as capable but not approved	Cross-check flight plans with approval records and feed back to operators
Single point of failure in the ground network	Diverse routes, redundant systems and tested failover
Message handling errors at ATSU transfers	Joint testing with neighbours, agreed ICDs and GOLD procedures
Compromise of the data link path	Segmentation, authentication and incident response shared with the CSP

Next steps and references

NEXT STEPS

1. Run a gap assessment against the nine-area checklist
2. Confirm CSP agreements and RCP and RSP allocations
3. Agree ICDs and a joint test plan with neighbouring ATSUs
4. Set up monitoring and reporting before go-live

ICAO REFERENCES

- Annex 10, Vol. II and III
- Annex 11: Air Traffic Services
- Annex 17: Security
- Doc 4444: PANS-ATM
- Doc 9869: PBCS Manual
- Doc 10037: GOLD
- Doc 9985: ATM Security Manual