International Civil Aviation Organization

THE FIFTH MEETING OF THE SURVEILLANCE STUDY GROUP (SURSG/5)

(Bangkok, Thailand 23-24 March 2026)

Agenda Item 3: States' experience with Surveillance data sharing

UPDATES ON THE GUIDANCE MATERIALS FOR THE SHARING OF SURVEILLANCE DATA IN SWIM

(Presented by Hong Kong China)

SUMMARY

This paper presents the development of the Guidance Materials for the sharing of surveillance data in SWIM and the latest status.

1. INTRODUCTION

1.1 After the successful conduct of the Joint Event of SWIM Demonstration over CRV and surveillance data in SWIM trial held in Hong Kong China, from 28 – 29 May 2024, SURSG has started to prepare the last deliverable of the Study Group (i.e. Guidance Materials, GMs) based on the proposed framework to include (1) surveillance information service security; (2) infrastructure and bandwidth consideration; (3) surveillance data performance requirement; and (4) data formats.

1.2 Hong Kong China, Singapore and USA have volunteered and contributed to producing the GMs.

1.3 The GMs was planned to be completed in a 2-year timeframe (i.e. from mid-2024 to mid-2026) and targeted for endorsement by SURICG/11 and CNS SG/30 in 2026.

2. DISCUSSION

Guidance Materials

2.1 With the joint effort from the volunteers, the first draft of the GMs was completed in August 2025 and circulated for SURSG members' review. ICAO Secretariat also helped to distribute the first draft of the GMs for SWIM TF members' review in November 2025. Comments received were then addressed and a second draft of the GMs was completed in January 2026.

2.2 No further comments were received on the second draft of the GMs, the finalized version of the GMs attached as Appendix A to this WP is considered as the agreed-upon version for seeking endorsement in SURICG/11 and CNS SG/30, by the following draft decision.

<table>
<tr><td colspan="3">Draft Decision SURSG/5/XX – Guidance Materials for the sharing of surveillance data in SWIM</td></tr>
<tr><td colspan="2">What: The finalized version of the Guidance Materials for the sharing of surveillance data in SWIM as completed by SURSG be endorsed by SURICG and CNS SG.</td><td>Expected impact:
☐ Political / Global
☐ Inter-regional
☐ Economic
☐ Environmental
☒ Ops/Technical</td></tr>
<tr><td>Why: To assist APAC States/Administrations in their SWIM development and implementation on the sharing of surveillance data, the finalized version of the Guidance Materials for the sharing of surveillance data in SWIM as completed by SURSG is ready for seeking endorsement from SURICG and CNS SG.</td><td colspan="2">Follow-up: ☐Required from States</td></tr>
<tr><td>When: 24-Mar-26</td><td colspan="2">Status: Draft to be adopted by Subgroup</td></tr>
<tr><td colspan="3">Who: ☒Sub groups ☐APAC States ☐ICAO APAC RO ☐ICAO HQ ☒Other: SURICG</td></tr>
</table>

Future Works

2.3 During SWIM TF/10, it was discussed that the current data exchange models developed by SURSG is applicable only at the regional level, and there is a need for a global surveillance information exchange format. SURSG proposed that it should be handled separately by both SURICG and SWIM/TF, based on the GMs developed by SURSG, to seek consideration from other upper bodies. Both SURICG and SWIM TF should be consulted for future development of the surveillance data exchange model for global adoption.

2.4 The SWIM development in the region is ongoing and it is anticipated that future updates on the GMs could be necessary, especially on any further required details of the surveillance information services. SURSG proposed that SURICG could take up this responsibility and to react appropriately when the relevant standard(s) becomes mature.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) provide support in providing the finalized version of the Guidance Materials for the sharing of surveillance data in SWIM to SURICG and CNS SG for endorsement;

c) provide support for the proposed future works to be taken up by the relevant upper bodies; and

d) discuss any relevant matter as appropriate.

– – – – – – – – – – – – –

Guidance Materials for the sharing of surveillance data in SWIM

Jan 2026

Study Group Under SURICG On Sharing of Surveillance Data In SWIM (SURSG)

Table of Contents

1. Introduction

1.1. Background

1.1.1. Surveillance Study Group (SURSG)

The establishment of the SURSG and its Terms of Reference (TOR) was endorsed by the CNS SG/24 on 4 December 2020 under the ***"Decision CNS SG/24/16 (SURICG/5/1) - Establishment of Study Group under SURICG on Sharing of Surveillance Data in SWIM"***. Based on the TOR, the objectives of the Study Group are to:

1) Study, provide expert views and recommendations:
   a) to achieve harmonized sharing of surveillance data in SWIM in the Asia and Pacific Regions (APAC) according to the Surveillance Strategy adopted by APANPIRG and in support of ICAO's GANP and ASBU initiatives; and
   b) on the possible models of sharing surveillance data in SWIM in the SWIM environment, in consideration of the SWIM technical infrastructure, SWIM information service, Common aeRonautical Virtual Private Network (CRV) infrastructure and any applicable governance, and technical requirements.

2) Review, identify and provide expert views and recommendations to address major issues, raised to the SURSG by ICAO APAC, in the technical, operational or regulatory aspects of surveillance data sharing to facilitate the implementation of surveillance from "departure to destination" in APAC.

1.1.2. SURSG Study Report

With members' support, inputs, and efforts from task leads, all tasks in the feasibility study stage were completed in Feb 2022 with a Concept of Operations (CONOPS) and a Study Report been published in ICAO portal (SURICG/6-IP17 and Appendix E in CNS SG/26-WP13) which formed the basis for shaping the performance requirements and service categorization of surveillance data sharing in the region. One of the recommendations and moving forward from the Study Report was the proposal for the establishment of a Surveillance Sharing in SWIM Trial Implementation Group (S3TIG) to oversee a trial with the following main responsibility and objectives:

1) Coordinating with the SWIM Task Force, CRV OG to reflect SWIM development in the trial
2) Leading and coordinating with interested states/administrations, and stakeholders (commercial and non-commercial) to conduct the trial:
   a) to demonstrate as far as practicable the general, technical and administrative aspects of surveillance sharing in SWIM in the Study Report; and
   b) to serve as a reference model for future surveillance sharing implementation in SWIM.

1.1.3. S3TIG and Joint Event

S3TIG was then established in December 2022 to support and promote the trial implementation of surveillance data sharing based on SWIM. With the endorsement of SURSG/3, SWIM TF/7, and SURICG/8, the SWIM Demonstration over CRV and surveillance data sharing in the SWIM trial were

successfully conducted as a Joint Event by S3TIG in Hong Kong, China, from 28 to 29 May 2024. The report of the joint event can be found in the ICAO portal (SWIM TF/10-WP/05).

1.1.4. Guidance Materials

Guidance materials (i.e. this document) for the sharing and access of surveillance data is one of the deliverables under SURSG. Upon successful completion of the Joint Event, States/Administrations including Hong Kong China, Singapore, and the USA have volunteered and contributed to producing this document.

1.2. Purpose of the Document

This document provides guidance for system planning, design, and implementation of SWIM platforms in the APAC region for surveillance data sharing, with the purpose of ensuring continuous and coherent development of the SWIM platforms for surveillance data sharing that is harmonized and interoperable within the region.

2. Summary of Major Considerations from the Study Report and their Outcomes from the Joint Event

2.1. Implementation Model

2.1.1. Starting small and simple

To align with the philosophy and roadmap for the implementation of SWIM in APAC, the same incremental approach (i.e. starting small and simple) has been leveraged for surveillance data sharing in the Joint Event. With a focus on operations selected (i.e. ATFM, FF-ICE, and MET) to benefit from surveillance data sharing, the infrastructure and associated information service have been identified and implemented. Where the first implementation of surveillance data sharing of ADS-B data proved feasible and beneficial.

2.1.2. SWIM over CRV

CRV has been endorsed as the carrier of SWIM data at CRV OG/5 and SWIM TF/3 meetings. S3TIG considered that the option to use the operational CRV for the Joint Event was not preferred considering the potential bandwidth impact and cyber security risks, even if remote, on the operational CRV, which is the network carrying safety critical operation data.

Instead, PCCWG established a pseudo-CRV network for the Joint Event. The pseudo-CRV operated exactly like the operational CRV, utilizing a dedicated and segregated CRV network with the same hardware setup. Similar to the operational CRV, dedicated network interface devices were installed at the site for each participant participating with an EMS.

For participants without an EMS, PCCWG provided SIM cards for mobile connection through its Console Connect platform. This platform allows users to access the simulated SWIM environment in the Joint Event to publish/subscribe data services and interact with the HMI of the SWIM services provided by PCCWG. The network infrastructure used in the Joint Event is illustrated in Figure 1 below.

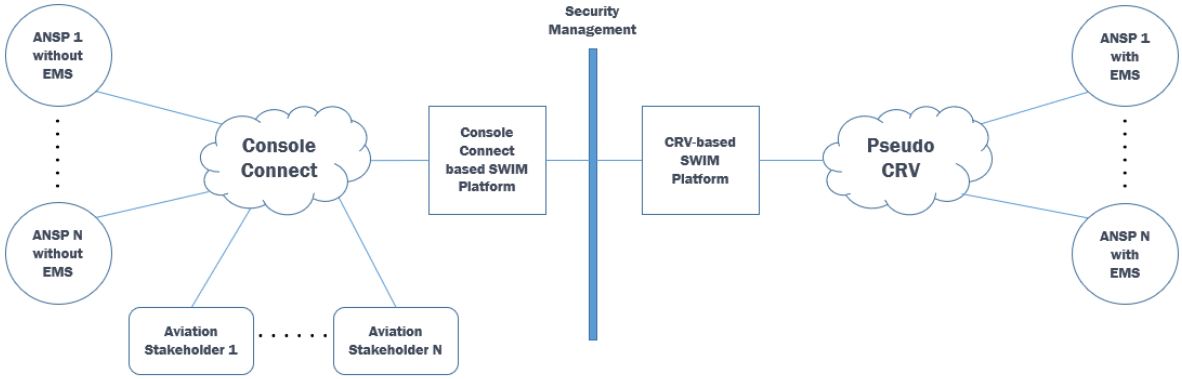


Figure 1 – Network Infrastructure for the Joint Event

The outcome of the Joint Event confirmed that the proposed implementation of surveillance data sharing using a SWIM platform, as depicted in Figure 1 above, with a combination of CRV-based SWIM platform and third-party/commercial interest providing the internet-based SWIM platform (i.e. Console Connect in the case of the Joint Event) for different kinds of stakeholders is feasible.

Moreover, stakeholders who are currently outside the CRV network's coverage can subscribe to the surveillance data sharing service (whether it is within the CRV network or not) through Console Connect (left side of the diagram), using various connection means. With proper security management, the Console Connect-based SWIM platform will be able to communicate with the CRV network and allow surveillance data exchange between the two platforms.

It should be noted that the 2Mbps bandwidth tentatively offered for each State/administration in the pseudo-CRV was not sufficient to carry surveillance data sharing with a 1s data rate. Section 4 of this document provides more detailed bandwidth considerations for surveillance data sharing.

2.2. Infrastructure Model

2.2.1. SWIM Technical Infrastructure

The hybrid infrastructure model as proposed by the Study Report, comprising private EMSes owned by States/Administrations and public/commercial EMSes was adopted in the Joint Event. While setting up the EMS architecture for the Joint Event, the SWIM Implementation Pioneer Group (SIPG) noted that a GRE tunnel would have to be established between each communication pair under the CRV provision. This approach would put restrictions on the future SWIM implementation as lots of GRE tunnels have to be constructed for any-to-any connections. To mitigate the impact of such restriction, a 2-tier hierarchical architecture was proposed by SWIM TF and was adopted for the Joint Event. In the hierarchical architecture, participants were divided into sub-communities and one representative from each sub-community would act as the gateway for message exchange among all sub-communities (“the Gateway EMS”). Participants under each sub-community with EMS provision would act as the EMS provider (“the Edge EMS”) for their local downstream users. This approach could effectively reduce the number of GRE tunnels required. For participants without EMS, PCCWG would act as the 3rd party EMS provider to provide network-based EMS services for them. Figure 2 below shows a schematic diagram of such EMS architecture.

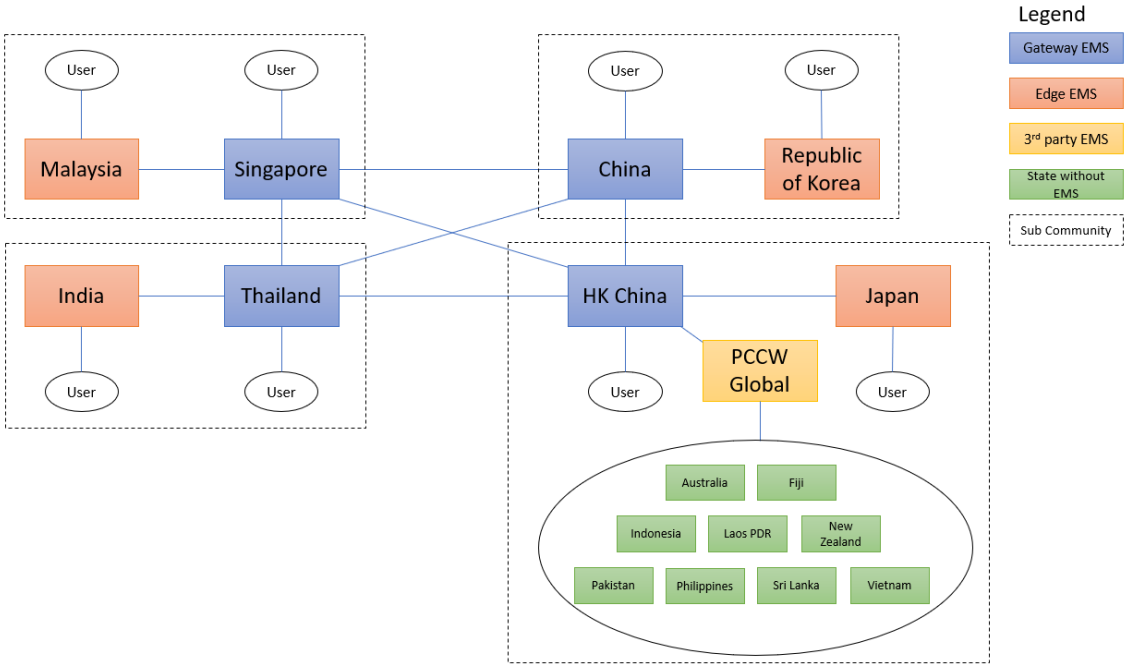


Figure 2 – EMS Infrastructure for the Joint Event

Some participants had expressed doubts about whether the hierarchical architecture is the appropriate architecture for the APAC region. There were several observations with this architecture identified during the preparation of the Joint Event, such as specific configuration required for different brands of EMS, potential message loop back if source and recipient checking was not implemented properly, combining byte message and text message into a single queue, single point of failure of the current architecture, etc.

It should be highlighted that the development of the SWIM technical infrastructure for APAC region is still ongoing. States/Administrations should refer to the latest development status as published by SIPG from time to time.

2.2.2. Surveillance Central Data Processor (SCDP)

Surveillance data sharing can be supported by direct interfacing between data contributor and data consumer. If any 3rd party wishing to provide a centralized surveillance data-sharing service may do so by way of an SCDP, which filters and collates surveillance data feeds from data contributors and outputs user-selectable data streams as a SWIM service. Figure 3 below shows a conceptual model of SCDP. While the SCDP functions were not tested in the Joint Event as such functions cannot be delivered by the SCDP service provider on time, it should be noted that the SCDP concept could bring benefit on bandwidth saving, especially for non-contributing EMS that only interested data will be transmitted from the SCDP, rather than receiving all surveillance data from all the contributing EMSes.

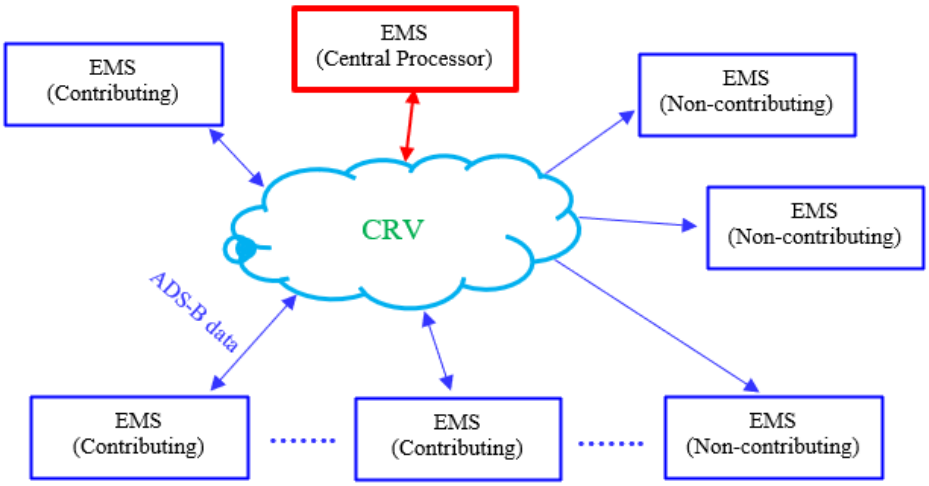


Figure 3 – Conceptual Model of SCDP

2.3. Business Model

The following are the major recommendations from the Study Report on the business model. For details, please refer to the Study Report as referred to in Section 1.1.2.

2.3.1. CONOPS

It is envisaged that States/Administrations will have varying needs for the shared surveillance data. Based on the nature of ATS applications, the service levels of shared surveillance data may be roughly classified into two types as below:

1) Level 1 Data Services for supporting ATS applications which make use of the shared surveillance data for aircraft separation.
2) Level 2 Data Services for supporting ATS applications which do not use shared surveillance data for aircraft separation (e.g. Air Traffic Flow Management (ATFM), situation awareness at FIR boundaries, etc.)

It should be highlighted that the APAC Common SWIM Information Services for surveillance data sharing in the region is not specified to support the provision of aircraft separation (i.e. Level 1 Data Services).

The Level 2 Data Services is suitable for:

a. FIR coordination.
b. Air situation awareness at FIR boundaries.
c. Flight tracking.
d. Strategic planning and analysis.

and is **not suitable** for:

a. Separation assurance.
b. Controller tactical operations.
c. Surveillance-based conflict resolution.

2.3.2. Format of Data

ASTERIX CAT 21 Edition 2.1 is recommended for the initial implementation, as most of the States/Administrations can support without additional data conversion efforts. The SCDP would be able to provide data conversion services between different ASTERIX CAT 21 editions, to support legacy systems if required. Accordingly, S3TIG proposed the data structure for surveillance data sharing. Such data structure could serve as a reference model for future surveillance-sharing implementation in SWIM. Two message payloads (i.e. ASTERIX and JSON) were tested in the Joint Event. The finalized data structure can be found in Section 6.2 - Annex 2.

2.3.3. Integrity of ADS-B Data

The data contributors should not modify the content of the surveillance data except for the following purposes:

1) ASTERIX Edition upgrading or downgrading;
2) Format conversion to meet the agreed data format for sharing;
3) SAC/SIC amendment; and
4) Fusion of data from multiple sensors, such as removal of duplicated ADS-B position reports. Position report extrapolation shall not be shared.

The time stamp of the surveillance data report shall be based on a reliable time source with timeliness performance as mentioned in Section 5.4, without any modification by the data contributors.

2.3.4. Report Filtering

Screening out special or non-civilian flights (e.g. State aircraft) is allowed with the filters being agreed upon prior to implementation. The filtering mechanism shall be detailed in the data services provided. For ADS-B data, the data contributors shall not perform any data filtering based on ADS-B quality indicators or blacklist. All the ADS-B data shall be shared with users as far as possible. Considering that States/Administrations will be making the assessment of data usability, and that lower NUC/NIC can still support lower-level operations, all data should be sent without filtering based on NUC/NIC.

2.3.5. Serviceability

Two data services, namely Level 1 (use for aircraft separation) and Level 2 (not use for aircraft separation) Data Services, were recommended to support the operation needs on surveillance data sharing in the region. These two data services are equivalent to Category 1 (support aircraft separation) and Category 3 (support enhanced flight operation) under "*Baseline ADS-B Service Performance Parameters*" of ICAO'S *ADS-B Implementation and Operations Guidance Document Edition 15.0 – September 2022"* with details as below.

Service Parameters	Level 1[1]	Level 2[2]
System Availability	Total Service Availability > 99.9%	Total Service Availability > 90%
System Reliability	Total Service MTBF > 50,000 hours	Total Service MTBF> 200 hours
Aircraft Updates	0.5 second < Interval < 10 seconds	0.5 second < Interval < 60 seconds
Data Latency	95%: < 2 seconds	95%: < 60 seconds

2.3.6. Data Coverage

Data contributor to share ADS-B data from stations that are near the FIR boundaries (useful to cover surveillance gaps) to support Level 1 data service and/or ADS-B stations that are near airports for international flights (useful for ATFM) to support Level 2 data service is recommended to be the minimum for a data contributor. Other choices to share ADS-B data from (i) all its ADS-B stations; (ii) one of its ADS-B stations; and (iii) all its international flights could be considered if such a use case is available.

2.4. Participation Model

2.4.1. Data Contributors

Due to the varying degrees of SWIM implementation status of States/Administrations, data contributors should offer flexibility to allow surveillance data sharing to the data consumers either by direct interfacing or by centralized SCDP services provided by a 3rd party.

Direct interfacing between data contributor and data consumer can be established regardless of whether an SCDP exists. However, an SCDP is expected to greatly accelerate the implementation of surveillance data sharing and popularize its utilization in accordance with the "starting small and simple" philosophy. SWIM-enabled States/Administrations can choose this collaboration model for an initial trial with a "local SCDP" and then populate the SCDP services through further collaboration in a later stage by expanding their capabilities or by way of 3rd-party SCDP centralized services.

Surveillance data sharing services (Level 1 and Level 2), if offered via SCDP, require the collaboration between States/Administrations (as data contributors) and the SCDP service provider for the data provision mechanism, including data format, data update rate, etc., to ensure the SCDP can deliver the ultimate surveillance data sharing services, meeting the service parameters mentioned in Section 2.3.5.

Data charging schemes or incentives provided to States/Administrations who are data contributors to the SCDP should be explored to encourage data contribution to the SCDP.

[1] Level 1 standards are for supporting ATS applications which make use of the shared surveillance data for aircraft separation. It should be highlighted that the service parameters mentioned in the table have been referenced from AIGD for 5NM separation, and may differ from any specific performance requirements specified in EUROCONTROL-SPEC-147 (EUROCONTROL Specification for ATM Surveillance System Performance (Volume 2 Appendices))

[2] Level 2 standards are for supporting ATS applications which do not use shared surveillance data for aircraft separation (e.g. Air Traffic Flow Management (ATFM), situation awareness at FIR boundaries, etc.)

With the presence of SCDP, States/Administrations without SWIM infrastructure can also contribute their data by legacy means and in legacy data formats (if this is the case) to the SCDP, which will then take care of data conversion and onward data surveillance sharing service for dissemination.

2.4.2. Data Consumers

States/Administrations, based on their own SWIM implementation status, can choose between direct interfacing with the data contributor or using the surveillance data sharing service provided by SCDP. States with SWIM infrastructure may participate in the initial trial by directly interfacing with data contributors. Data consumers without SWIM infrastructure can subscribe to the surveillance data sharing services from the SCDP to benefit from shared surveillance data.

Data will be shared among all the participating users in the spirit of sharing and benefiting the aviation community.

2.4.3. Data Governance

It should be highlighted that the development of the SWIM data governance for APAC region is still ongoing. States/Administrations should refer to the latest development status as published by SIPG from time to time.

2.5. Implementation Roadmap and Timeframe

2.5.1. Development of CONOPS

Singapore, Hong Kong, China, Thailand, and Vietnam have developed a proposed concept of operations (CONOPS) for surveillance data sharing in SWIM (SURICG/6-IP/17). A comprehensive discussion has been included, ranging from practical models for collaboration and operation to business models, considering available platform(s) and other technical considerations.

2.5.2. Preparation of guidance material and multilateral agreement

With reference to the models and recommendations advised in the Study Report, guidance material, specified system requirements, performance requirements, operation and maintenance practice, and so forth, should be developed to facilitate and harmonize the implementation of surveillance data sharing. The guidance material should also provide guidance for the design, testing, and commissioning of the system for surveillance data sharing to ensure coherent system development.

A multilateral agreement may involve a lengthy negotiation process, depending on the size of the participant group and agendas. Despite the considerable time it may take, a multilateral agreement is considered a more suitable option over a bilateral agreement to attain non-discrimination data sharing with transparent, fair, and equitable treatment.

2.5.3. Implementation of infrastructure – SWIM, CRV and EMS

SWIM over CRV is the default means to share surveillance data. The hybrid infrastructure model is considered the most suitable one with maximum efficiency and minimal geopolitical concerns. The States/Administrations are suggested to evaluate and determine which options to be adopted, based on their own context. The infrastructure should be implemented according to the

requirements set out with considerations of latency, throughput, network security, system reliability, and cost effectiveness.

2.5.4. Implementation of information service

It is envisaged that information services developed based on the functional and performance requirements, such as message format and data filtering, will be properly tested and validated locally or with the adjacent regions to ensure a reliable system for surveillance data sharing.

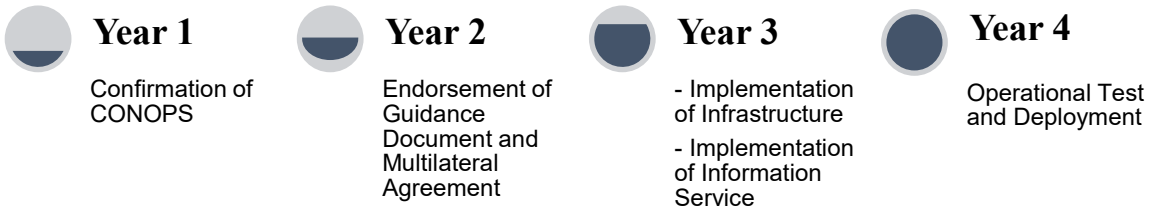
2.5.5. Operational test, validation user acceptance, and operation deployment

Upon the completion of the implementation of infrastructure and information service, the overall functions of sharing surveillance data could be verified through operational tests and user acceptance tests. State/Administration's involvement in this stage is important to identify system deficiencies or interface issues, if any, for further investigation and improvement before putting into operation.

After comprehensive testing and review, the system would be ready to deploy for operation. Regular meetings across the States/Administrations should be held with an operations group to review performance and examine any issues found. A collaborative review process and cooperative system fine-tuning will be crucial for the continuous improvement and further development of surveillance data sharing.

2.5.6. Timeframe

The implementation timeline chronologically arranges the tasks identified in the implementation roadmap proposed in Sections 2.5.1 to 2.5.5. The timeline may differ to some extent depending on the actual deployment model and approach, and also for the level of services to be delivered (e.g. quicker deployment for Level 2 Data Services than Level 1 Data Services). The implementation of the SWIM platform is a key contributing factor to the timeline of surveillance data sharing.



3. Surveillance Information Service Security

The security of the Surveillance Information Service in the SWIM platform is critical to ensuring the integrity, confidentiality, and availability of surveillance data. While the overall SWIM-related information security would be based on the guidance documents developed by the Trust Framework Panel (TFP), this document will focus on industrial best practices for securing surveillance information services and their interfaces.

3.1. General Security Principles

1) **Authentication and Authorization**: Verify the identity of all entities accessing the SWIM services and enforce strict role-based access control (RBAC).
2) **Confidentiality**: All surveillance data exchanged between systems must be encrypted to prevent unauthorized access.
3) **Integrity**: Mechanisms must be in place to detect and prevent any unauthorized alterations to surveillance data.
4) **Availability**: Ensure that the SWIM platform and its services remain operational and resistant to denial-of-service (DoS) attacks.

3.2. Security for External Interfaces

The external interface of the SWIM platform would be over CRV or the internet. This interface is vulnerable to external cyber threats and requires robust protection mechanisms, such as:

1) Data Encryption
   a) Use TLS for encrypting data exchanged over the external interface.
   b) Ensure that all endpoints support secure transport protocols.

2) Authentication
   a) Implement mutual TLS (mTLS) to authenticate both the SWIM platform and external entities.
   b) Use digital certificates issued by a trusted Certificate Authority (CA) for secure communications.

3) Access Control
   a) Apply firewall rules to restrict access to the SWIM platform to only authorized IP addresses or ranges.
   b) Use Application Layer Gateways (ALG) or dedicated API gateways to filter and validate incoming and outgoing messages.

4) Monitoring and Intrusion Detection
   a) Deploy an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) to monitor traffic between the SWIM platform and external entities.
   b) Log all access attempts and regularly audit logs for suspicious activity.

5) Message Validation
   a) Validate incoming messages for conformance to the expected format (e.g. ASTERIX CAT 21 or SWIM-based messages).
   b) Reject malformed or unexpected messages to prevent injection attacks or malformed data propagation.

6) Rate Limiting and DoS Protection
   a) Apply rate limiting to prevent excessive requests from external entities.

b) Use traffic filtering and scrubbing solutions to mitigate DoS or Distributed Denial of Service (DDoS) attacks.

3.3.Security for Internal Interfaces

The SWIM platform's internal interface would be connected to the data conversion engine and the internal ADS-B system. While the internal network is more protected, it still requires robust security to prevent insider threats or breaches.

1) **Network Segmentation**
   a) Separate the SWIM platform, data conversion engine, and internal ADS-B system into distinct network zones.
   b) Use firewalls to enforce strict segmentation and limit communication to only necessary connections.
2) **Encryption**
   a) Secure internal communications using IPSec or TLS to prevent interception or tampering of data.
3) **Data Validation and Filtering**
   a) Validate and sanitize all messages exchanged between the data conversion engine and the SWIM platform.
   b) Ensure that no unauthorized or malformed data is passed through the internal interface.
4) **Authentication**
   a) Use secure tokens or certificate-based authentication for all communications between internal systems.
   b) Implement two-factor authentication (2FA) for administrative access to internal components.
5) **Access Control**
   a) Enforce strict access control policies for internal systems. Only authorized personnel and systems should have access to the SWIM platform and the data conversion engine.
6) **Audit and Logging**
   a) Maintain detailed logs of all interactions between the SWIM platform, data conversion engine, and internal ADS-B system.
   b) Implement real-time monitoring to identify unauthorized access or unusual activity.

3.4.Security for Data Conversion Process

The data conversion engine, which converts legacy ASTERIX format data to SWIM-based messages, must be secured to ensure reliable and accurate data transformation.

1) **Input Validation:**
   a) Validate and sanitize all data received from the internal ADS-B system before processing.
   b) Ensure that only ASTERIX CAT 21 messages are accepted for conversion.
2) **Controlled Data Transformation:**
   a) Perform data conversion within a sandboxed environment to mitigate the risk of malicious payloads affecting the SWIM platform.
3) **Error Handling and Exceptions:**

a) Implement robust error handling to prevent corrupted or incomplete data from being transmitted to the SWIM platform.

4) **Data Integrity Checks:**
   a) Use hashing algorithms (e.g. SHA-256) to verify the integrity of data before and after conversion.

3.5.Security Governance and Compliance

1) **Compliance with Standards:**
   a) Ensure compliance with ICAO guidelines, such as the Global Air Navigation Plan (GANP) and Aviation System Block Upgrade (ASBU) framework.
   b) Follow guidance documents developed by the TFP.
2) **Regular Security Assessments:**
   a) Conduct periodic vulnerability assessments and penetration testing for both internal and external interfaces.
   b) Review and update security policies regularly to address emerging threats.
3) **Incident Response Plan:**
   a) Develop and maintain an incident response plan to quickly detect, respond to, and recover from security incidents.
   b) Conduct regular drills and simulations to ensure readiness.
4) **Training and Awareness:**
   a) Provide cybersecurity training to all personnel involved in the operation and management of the SWIM platform.
   b) Promote awareness of phishing, social engineering, and other common threats.

4. Infrastructure and Bandwidth Considerations

4.1. Infrastructure Considerations

The ANSP's infrastructure to support surveillance data sharing over SWIM should include at least the following components and interconnections among them.

1) Internal ADS-B system;
2) An interfacing module with flight plan system (for supporting surveillance data with flight plan information)
3) A data conversion engine/services to convert legacy ASTERIX format data to SWIM-based surveillance messages, which would most likely be a new system to be implemented, as existing automation systems typically incorporate surveillance data processing which create surveillance tracks no longer representative of the original data source (i.e. existing automation system outputs will not meet the requirement to supply the unprocessed ADS-B data).
4) An EMS to publish the SWIM based surveillance messages

Schematic diagrams showing the possible infrastructures are depicted below, with option 1 to be owned by ANSP and option 2 be cooperated with 3rd party service provider.

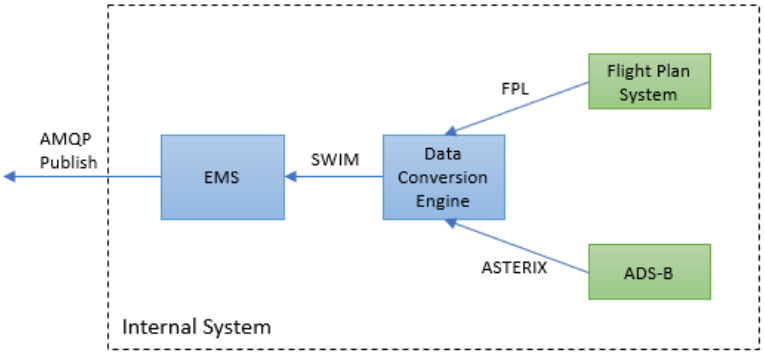


Figure 4 – Possible infrastructure (option 1)

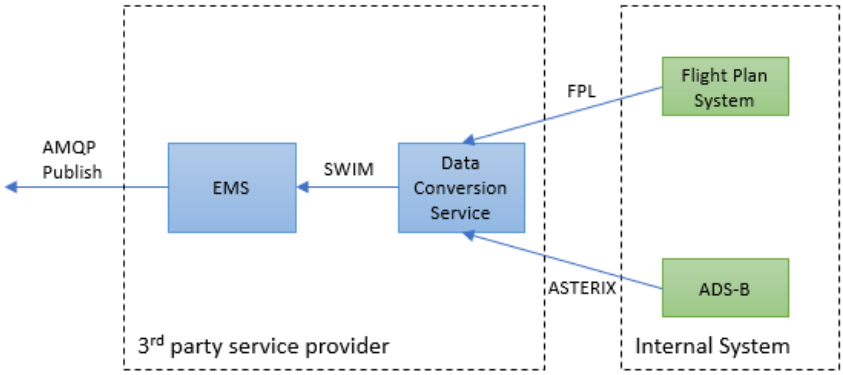


Figure 5 – Possible infrastructure (option 2)

The comparison between the two options are similar to other provision of SWIM services and could be considered by ANSP according to its situation. Some consideration factors are listed below.

1) On-premise vs Cloud-based SWIM infrastructure;
2) Self-development vs service-subscribed services;
3) Self-maintenance vs service-subscribed maintenance;
4) One-time cost vs recurrent cost; and
5) Level of data ownership and data sensitivity.

4.2. Bandwidth Considerations

In planning for the transmission of surveillance data over SWIM, it is essential to consider the bandwidth implications associated with the selected data format, message frequency, and operational requirements. Ensuing paragraphs provides considerations into the bandwidth calculation based on the Joint Event for surveillance data sharing over SWIM as presented in the WP05 in SURSG/4, 28 – 31 May 2024.

a) Transmission Overhead
Analysis of packet captures has revealed that Advanced Message Queuing Protocol (AMQP) messages incur an approximate 8% overhead relative to the size of the original message content (header and body).

b) Message Size
Statistical data from the Joint Event highlights that AMQP messages containing both ADS-B surveillance data and Flight Plan information can vary in size depending on the number of data fields and format used. Notably:
- Messages in JSON format that carry 32 data fields have an average size of **1.1K bytes** per message.
- Including the **8%** transmission overhead, the effective size per message increases to approximately **1.2K bytes**.

This represents the upper bound of message size observed and is suggested to be used as a reference for capacity planning.

c) Peak Bandwidth Estimation Example
In the case of Hong Kong, China, during peak traffic periods, the ADS-B system detects and processes data for approximately 300 aircraft targets per second within its area of responsibility. Assuming each target is associated with a message of 1.2 KB, the estimated bandwidth consumption is as follows:
- 300 messages per second × 1.2K bytes = 360K bytes per second
- This equates to approximately **2.88 Mbps**

This estimation provides a useful reference point for States/Administrations when planning their bandwidth provision in similar operational environments.

d) Suggested Calculation for Required Bandwidth

[maximum number of targets per second] x 1.2K bytes x 8 bps

5. Performance Requirements

5.1. Overview

This section defines the minimum performance requirements for sharing surveillance data in a SWIM-compliant environment. The framework assumes a fixed surveillance data refresh rate of between every 4 to 30 seconds and aims to support **Level 2 Data Services only** (align with the APAC Common SWIM Information Services) including strategic ATM operations such as situational awareness at FIR boundaries, planning, and safety monitoring—not tactical control. Emphasis is placed on the integrity, timeliness, and efficient distribution of surveillance data between contributing systems and consumers.

5.2. Surveillance Refresh Cycle and Data Management

5.2.1 Surveillance Refresh Rate

1. All surveillance data (track-level or processed target reports) shall be refreshed between every 4 and 30 seconds (0.25 and 0.03 Hz).
2. This interval defines the **data validity window** for each update; messages older than this window must be **discarded** and **replaced with the most current message**.
3. EMS and EMS Central Processing units must synchronize their output to this cycle and align time stamps using a standard (e.g., UTC-based ISO 8601).

5.2.2 Surveillance Central Data Processing (SCDP) Interface

1. The SCDP must act as the **authoritative node** aggregating surveillance feeds from contributing **EMS or EMS Central Processing nodes**.
2. All contributing EMS nodes must:
    a. Push updates to the SCDP in harmony with the surveillance update rate, between every 4 to 30 seconds.
    b. Include metadata indicating the source system, timestamp, and message sequence.
    c. Implement logic to **replace stale messages** and ensure that only the most current data is available for downstream dissemination.
    d. SCDP shall enforce **version control** and prevent duplication or delivery of outdated data.

5.3. Message Distribution Architecture

5.3.1 Push Message Model

1. **Definition**: Data is delivered continuously from the publisher (e.g., SCDP) to subscribed consumers without solicitation.
2. **Performance Characteristics**:
    a. Suitable for systems needing continuous streams (e.g., ground situation displays, traffic flow tools).
    b. Requires **high bandwidth**, especially during peak operational hours.
    c. Messages must be prioritized and queued efficiently to avoid congestion.
    d. Tolerable one-way distribution time: **≤ 1 second end-to-end**, including **200–400 ms over CRV**, depending on available bandwidth.

5.3.2 Pull Message Model

1. **Definition**: Consumers request specific data sets from the SCDP or an intermediary data service.
2. **Performance Characteristics**:
    a. Pull requests must be **governed and filtered**: consumers may only access messages that are:
    b. Related to their airspace of responsibility.
    c. Within their operational context or authorization.
    d. Response times to pull queries should not exceed **2 seconds**, including message retrieval and filtering.
    e. Pull services must implement **access control**, **query scope limits**, and **load-balancing mechanisms** to preserve the system.

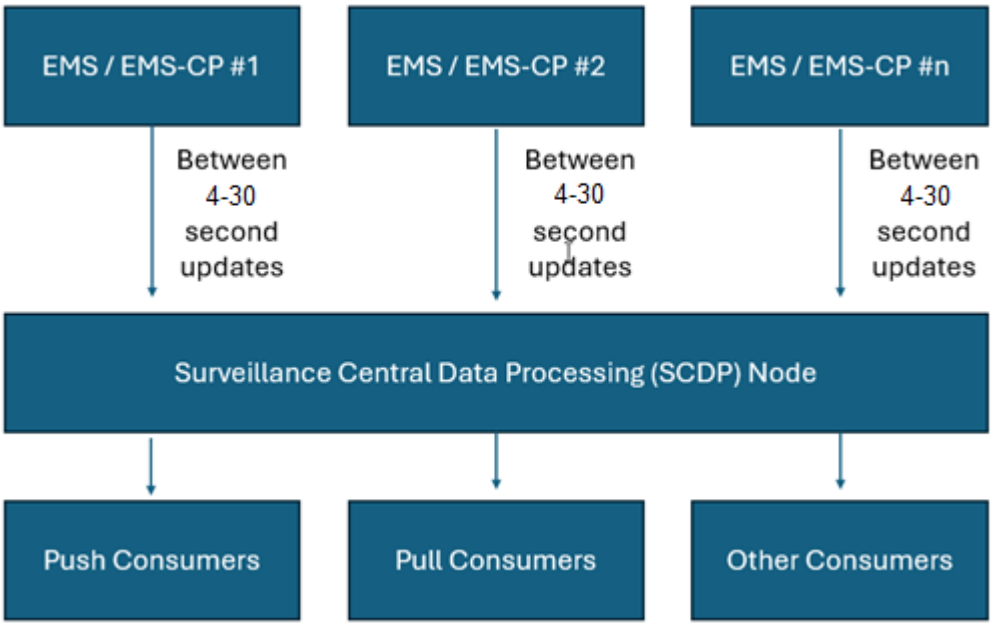
5.4. Key Performance Parameters

Parameter	Requirement
Update Rate	Between every **4 and 30 seconds** from all contributing EMSs to SCDP.
Latency	End-to-end delivery from EMS to consumer: **≤ 1 second** (nominal).
CRV Distribution Time	**200–400 ms**, subject to bandwidth; tolerance for up to 600 ms in constrained conditions.
Data Integrity	All messages must include verification (e.g., checksum, digital signature). Invalid or corrupted data shall be rejected.
Availability	99.9% availability (max 8.76 hours downtime per year).
Continuity	Surveillance data source shared via SWIM to maintain message delivery such that, for each individual source, no more than one consecutive expected message is missed within any rolling 24-hour period.
Timeliness	All surveillance data must be time-stamped to UTC with an accuracy of ±1 second.
Bandwidth Efficiency	Push models must implement flow control. Pull models must restrict volume by request scope and role-based access.
Scalability	Systems must scale to support a growing number of consumers (e.g., FIRs, ATFM units, adjacent ANSPs) without degradation in latency.

5.5. Quality Assurance and Monitoring

1. SWIM surveillance data services must implement continuous **performance monitoring** at key nodes (EMS, SCDP, CRV interface, consumer).
2. **Alerts** must be generated for:
    a. Missed updates.
    b. Latency exceeding defined thresholds.
    c. CRV congestion or message drops.
3. Logs must retain metadata for **audit and post-event analysis** for at least 30 days.

5.6.SWIM Surveillance Data Sharing Architecture



5.7. Key Components and Data Flow

1. **EMS / EMS-CP Nodes**:
    a. **Function**: Collect raw surveillance data (e.g., radar, ADS-B).
    b. **Data Transmission**: Send processed surveillance messages to the SCDP every 4 to 30 seconds.
    c. **Time Synchronization**: Ensure all messages are time-stamped using UTC (e.g., ISO 8601 format).
2. **Surveillance Central Data Processing (SCDP)**:
    a. **Function**: Aggregate, validate, and manage surveillance data from multiple EMS/EMS-CP sources.
    b. **Data Management**:
        i. Discard outdated messages beyond the 4-to-30-second refresh cycle.
        ii. Replace old messages with new ones to maintain data currency.
    c. **Data Distribution**:
        i. **Push Model**: Broadcast data to subscribed consumers.
        ii. **Pull Model**: Respond to specific data requests from consumers.
3. **Push Consumers**:
    a. **Examples**: Air Traffic Flow Management systems, situational awareness displays.
    b. **Data Reception**: Receive continuous data streams.

   c. **Bandwidth Consideration**: High bandwidth usage, especially during peak operational hours.
4. **Pull Consumers**:
   a. **Examples**: Analytical tools, post-event analysis systems.
   b. **Data Access**: Request specific data subsets based on criteria (e.g., geographic area, time frame).
   c. **Access Control**: Governed to ensure consumers receive only relevant and authorized data.
5. **CRV (Common Regional Virtual) Network**:
   a. **Function**: Facilitate data transmission between EMS/EMS-CP nodes and the SCDP.
   b. **Performance**:
      i. Typical distribution time: 200–400 milliseconds.
      ii. Potential for increased latency if bandwidth is constrained.
6. **Performance Parameters Summary**
   a. **Surveillance Refresh Rate**: Between every 4 and 30 seconds.
   b. **Message Validity**: Messages older than 4-to-30 seconds are discarded and replaced.
7. **Push Model**:
   a. **Bandwidth**: High during peak hours.
   b. **Latency**: Target end-to-end delivery within 1 second.
8. **Pull Model**:
   a. **Access Control**: Consumers receive only data pertinent to their role and authorization.
   b. **Latency**: Response time should not exceed 2 seconds.
9. **CRV Network**:
   a. **Distribution Time**: 200–400 milliseconds under optimal conditions; may increase with bandwidth limitations.

6. Annexes

6.1. Annex 1 – Message Headers for the Joint Event

Header Name	Values	Descriptions	Mandatory / Optional	Data Type
APAC_SOURCE	VH_HKCAD	Hongkong ASP (Contibutor & Consumer)	Mandatory	String
	RJ_JCAB	Japan ASP (Contibutor & Consumer)		
	WM_CAAM	Malaysia ASP (Contibutor & Consumer)		
	RK_KAC	ROK ASP (Contibutor & Consumer)		
	WS_CAAS	Singapore ASP (Contibutor & Consumer)		
	VT_AEROTHAI	Thailand ASP (Contibutor & Consumer)		
	VA_AAI	India (Contributor & Consumer)		
	RJ_JAL	Japan Airlines		
	VH_PCCW	PCCW		
APAC_RECIPIENT_LIST	ZB_ATMB	China ASP (Observer)	Mandatory	String
	VH_HKCAD	Hongkong ASP (Contibutor & Consumer)		
	RJ_JCAB	Japan ASP (Contibutor & Consumer)		
	WM_CAAM	Malaysia ASP (Contibutor & Consumer)		
	RK_KAC	ROK ASP (Contibutor & Consumer)		
	WS_CAAS	Singapore ASP (Contibutor & Consumer)		
	VT_AEROTHAI	Thailand ASP (Contibutor & Consumer)		
	VA_AAI	India (Contributor & Consumer)		
	WI_CAI	Indonesia ASP (Observer)		

Header Name	Values	Descriptions	Mandatory / Optional	Data Type
	VL_LPDR	Laos ASP (Observer)		
	NZ_AIRWAYS	NZ ASP (Observer)		
	OP_CAAPK	Pakistan ASP (Observer)		
	RP_CAAP	Philippines ASP (Observer)		
	YM_ASA	Australia (Consumer)		
	NF_FIJI	Fiji (Consumer)		
	RJ_JAL	Japan Airlines		
	VH_PCCW	PCCW		
APAC_CATEGORY	FIXM	All FIXM Messages	Mandatory	String
	AIXM	All AIXM Messages		
	IWXXM	All IWXXM Messages		
	ASTERIX	Surveillance Messages		
	GEOJSON	Meteorological Report Messages		
	JSON	Surveillance Messages in JSON Format		
APAC_CATEGORY_VERSION	FIXM_4_1	FIXM v4.1.0	Mandatory	String
	FIXM_4_1_APAC	FIXM v4.1.0 APAC Extension		
	FIXM_4_2	FIXM v4.2.0		
	FIXM_4_2_FF_ICE	FIXM v4.2.0 (for FF-ICE R1 and R2)		
	FIXM_4_2_APAC	FIXM v4.2.0 APAC Extension		
	AIXM_5_1	AIXM v5.1		
	IWXXM_2_0	IWXXM v2.0		

Header Name	Values	Descriptions		Mandatory / Optional	Data Type
	IWXXM_3_0	IWXXM v3.0			
	ASTERIX _CAT021	ASTERIX ADS-B Data Category			
	GEOJSON_4	GEOJSON v4.0			
	JSON_1	JSON v1.0			
APAC_MESSAGE_TYPE	**Values**	**Descriptions**	**Format**		
	PRELIMINARY_FLIGHT_PLAN	Preliminary Flight Plan	FIXM_FF-ICE R1	Mandatory	String
	FILED_FLIGHT_PLAN	Filed Flight Plan	FIXM_FF-ICE R1		
	SUBMISSION_RESPONSE	Submission Response	FIXM_FF-ICE R1		
	FILING_STATUS	Filing Status	FIXM_FF-ICE R1		
	PLANNING_STATUS	Planning Status	FIXM_FF-ICE R1		
	FLIGHT_PLAN_UPDATE	Flight Plan Update	FIXM_FF-ICE R1		
	FLIGHT_ARRIVAL	Arrival	FIXM_FF-ICE R1		
	FLIGHT_DEPARTURE	Departure	FIXM_FF-ICE R1		
	FLIGHT_CANCELLATION	Flight Plan Cancel	FIXM_FF-ICE R1		
	TRIAL_REQUEST	Trial Request	FIXM_FF-ICE R1		
	TRIAL_RESPONSE	Trial Response	FIXM_FF-ICE R1		
	FLIGHT_DATA_REQUEST	Flight Data Request	FIXM_FF-ICE R1		
	FLIGHT_DATA_RESPONSE	Flight Data Response	FIXM_FF-ICE R1		
	TRACK_RAW	Track Raw Data	ASTERIX Binary Data		
	TRACK_JSON	Track JSON Message	ASTERIX JSON Data		
	TRACK	Track Message	FIXM APAC Extension		
	CTOT	Calculated Take Of Time	FIXM APAC Extension		
	NOTAM	Notices to Airmen	AIXM		
	SAA	Special Activity Airspace	AIXM		

Header Name	Values	Descriptions		Mandatory / Optional	Data Type
	METAR	Aviation Routine Weather Report	IWXXM		
	SPECI	Special weather report	IWXXM		
	TAF	Terminal Area Forecast	IWXXM		
	SIGMET	Significant Meteorological information	IWXXM		
	AIRMET	Meteorological Information	IWXXM		
	VAA	Volcanic Ash Advisory	IWXXM		
DEP_AIRPORT	4 Letter ICAO Code	Departure Airport (used for flight identification)		Optional	String
ARR_AIRPORT	4 Letter ICAO Code	Arrival Airport (used for flight identification)		Optional	String
AIRLINE	Use ICAO Airline	Name of Airline		Optional	String
ACID	FIXM-defined format for ACID	Aircraft Identification (Mandatory for Tracks and Flight Plans)		Conditional Mandatory	String
GUFI	GUFI from message	Globally Unique Flight Identifier		Optional	String
EOBT	EOBT from message	Estimated off-block time (used for flight identification)		Optional	String
FFICE_PHASE	PRELIM	Preliminary phase of FF-ICE		Optional	String
	FILED	Filed phase of FF-ICE (Filed Flight Plan has been sent)		Optional	String
APAC_TIMESTAMP	epoch time	Timestamp of the message out or in the system. The time is to be appended to this field whenever the message is posted into a message queue. This field is delimited with commas E.g. JAL_OUT:1675213637251, JCAB_IN: 1675213638200 Comma delimited string of 64-bit signed integer representing the number milliseconds since Jan 1, 1970 00:00:00.000 UTC		Mandatory	String

6.2.Annex 2 – Data Structure of Surveillance Data for the Joint Event

6.2.1. JSON Structures for Surveillance Data with Flight Plan Information

Data fields below are based on ASTERIX CAT 21 version 2.1 specifications.

Field Name	Type	CAT21 Data Item Reference	Compulsory	Values	Descriptions
GUFI	String	N/A	No	0248982c-4384-49f4-bdb3-7956bd553383	Globally Unique Flight Identifier (obtained from FF_ICE services)
ACID	String	N/A	Yes	TLM912	Aircraft Identification
ADEP	String	N/A	Yes	VTBS	Departure Aerodrome
ADES	String	N/A	Yes	ZGGG	Destination Aerodrome
ARCTYPE	String	N/A	No	A339	Aircraft Type
WKTRC	String	N/A	No	H	Wake Turbulence Category
LAT	Number	I021/130 or I021/131	Yes	18.6701799113899	Latitude (Degree) Use I021/131. If I021/131 does not exist, use I021/130
LONG	Number	I021/130 or I021/131	Yes	103.180853652939	Longitude (Degree) Use I021/131. If I021/131 does not exist, use I021/130
FL	Number	I021/145	Yes	310	Flight Level
GS	Number	I021/160	No	498	Ground Speed (Knot) Use I021/160 x 3600 because I021/160 provides Ground Speed in NM/s
HEADING	Number, Null	I021/152 or I021/160	No	34.2773437344	Heading (Degree) Use I021/152 If I021/152 does not exist, use I021/160 null, if both not exist.

Field Name	Type	CAT21 Data Item Reference	Compulsory	Values	Descriptions
ARCADDR	String	I021/080	Yes	883031	Aircraft Address (ICAO 24-bit Mode S address)
SSRCODE	String	I021/070	No	5035	Mode 3A Code
DT	String	I021/071 or I021/073 or I021/075	Yes	2022-09-13T15:41:3	Date and Time (Date from server date and Time from packet) Use I021/073 If I021/073 does not exist, use I021/075 If I021/075 does not exist, use I021/071 I021/071, I021/073 and I021/075 are time only value. Publishers have to add date themselves.
QITYPE	String	I021/210	Yes	NUCp or NIC	NUCp = Navigational Uncertainty Category for Position NIC = Navigational Integrity Category
QI	Integer	I021/090	Yes	6	Range is 0-11 for NIC and 0-9 for NUCp
SAC	Integer	I021/010	Yes	78	Data Source Identification (SAC)
SIC	Integer	I021/010	Yes	29	Data Source Identification (SIC)

6.2.2. JSON Structures for Surveillance Data only

Data fields below are based on ASTERIX CAT 21 version 2.1 specifications.

Field Name	Type	CAT21 Data Item Reference	Compulsory	Values	Descriptions
ACID	String	I021/170	Yes	TLM912	Target Identification in 8 characters, as reported by the target.
LAT	Number	I021/130 or I021/131	Yes	18.6701799113899	Latitude (Degree) Use I021/131. If I021/131 does not exist, use I021/130

Field Name	Type	CAT21 Data Item Reference	Compulsory	Values	Descriptions
LONG	Number	I021/130 or I021/131	Yes	103.180853652939	Longitude (Degree) Use I021/131. If I021/131 does not exist, use I021/130
FL	Number	I021/145	Yes	310	Flight Level
GS	Number, Null	I021/160	No	498	Ground Speed (Knot) Use I021/160 x 3600 because I021/160 provides Ground Speed in NM/s
HEADING	Number	I021/152 or I021/160	No	34.2773437344	Heading (Degree) Use I021/152 If I021/152 does not exist, use I021/160 null, if both not exist.
ARCADDR	String	I021/080	Yes	883031	Aircraft Address (ICAO 24-bit Mode S address)
SSRCODE	String	I021/070	No	5035	Mode 3A Code
DT	String	I021/071 or I021/073 or I021/075	Yes	2022-09-13T15:41:3	Date and Time (Date from server date and Time from packet) Use I021/073 If I021/073 does not exist, use I021/075 If I021/075 does not exist, use I021/071 I021/071, I021/073 and I021/075 are time only value. Publishers have to add date themselves.
QITYPE	String	I021/210	Yes	NUCp or NIC	NUCp = Navigational Uncertainty Category for Position NIC = Navigational Integrity Category
QI	Integer	I021/090	Yes	6	Range is 0-11 for NIC and 0-9 for NUCp
SAC	Integer	I021/010	Yes	78	Data Source Identification (SAC)
SIC	Integer	I021/010	Yes	29	Data Source Identification (SIC)

6.2.3. Message Header for Surveillance Data with Flight Plan Information

Header Name	Values	Descriptions
APAC_SOURCE	RJ_JCAB	Name of message publisher
APAC_RECIPIENT_LIST	RJ_JAL,VT_AEROTHAI	Name list of recipients (comma delimited)
APAC_CATEGORY	ASTERIX	Name of information exchange model (ASTERIX)
APAC_CATEGORY_VERSION	ASTERIX _CAT021	Version of information exchange model (Data Category of ASTERIX)
APAC_MESSAGE_TYPE	TRACK_RAW or TRACK_JSON	Message type of information exchange model • TRACK_RAW for binary data • TRACK_JSON for JSON data
DEP_AIRPORT	RJAA	Departure Airport
ARR_AIRPORT	VTBS	Arrival Airport
AIRLINE	JAL	Name of Airline
ACID	JAL707X	Aircraft Identification
GUFI	0248982c-4384-49f4-bdb3-7956bd553383	Globally Unique Flight Identifier
EOBT	2023-02-01T03:00:00Z	Estimated Off-Block Time
APAC_TIMESTAMP	JCAB_OUT:1675213637251	Timestamp of the message out or in the system

6.2.4. Message Header for Surveillance Data Only

Header Name	Values	Descriptions
APAC_SOURCE	RJ_JCAB	Name of message publisher
APAC_RECIPIENT_LIST	RJ_JAL,VT_AEROTHAI	Name list of recipients (comma delimited)
APAC_CATEGORY	ASTERIX	Name of information exchange model (ASTERIX)
APAC_CATEGORY_VERSION	ASTERIX _CAT021	Version of information exchange model (Data Category of ASTERIX)
APAC_MESSAGE_TYPE	TRACK_RAW or TRACK_JSON	Message type of information exchange model • TRACK_RAW for binary data • TRACK_JSON for JSON data
ACID	JAL707X	Aircraft Identification
APAC_TIMESTAMP	JCAB_OUT:1675213637251	Timestamp of the message out or in the system

7. Acronyms and Abbreviations

2FA	Two Factor Authentication
ADS-B	Automatic Dependent Surveillance - Broadcast
ALG	Application Layer Gateways
AMQP	Advanced Message Queuing Protocol
ANSP	Air Navigation Service Provider
APAC	Asia Pacific
APANPIRG	Asia/Pacific Air Navigation Planning and Implementation Regional Group
API	Application programming interface
ASBU	Aviation System Block Upgrade
ASTERIX	All Purpose Structured EUROCONTROL Surveillance Information Exchange
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
bps	Bits per second
CA	Certificate Authority
CONOPS	Concept of Operations
CNS SG	Communications, Navigation and Surveillance Sub-group
CRV	Common aeRonautical Virtual Private Network
CRV OG	Common aeRonautical Virtual Private Network Operations Group
DoS	Denial of Service
DDoS	Distributed Denial of Service
EMS	Enterprise messaging system
FF-ICE	Flight and Flow Information for a Collaborative Environment
FIR	Flight Information Region
GANP	Global Air Navigation Plan
GRE	Generic Routing Encapsulation
HMI	Human Machine Interface
ICAO	International Civil Aviation Organization
IDS	Intrusion Detection System
IPSec	Internet Protocol Security

JSON	JavaScript Object Notation
MET	Aeronautical Meteorological Services
MTBF	Mean Time Between Failure
NIC	Navigation Integrity Category
NUC	Navigation Accuracy Category
PCCWG	PCCW Global
RBAC	Role-based Access Control
S3TIG	Surveillance Sharing in SWIM Trial Implementation Group
SAC	System Area Code
SCDP	Surveillance Central Data Processor
SHA	Secure Hash Algorithm
SIC	System Identification Code
SIM	Subscriber Identity Module
SIPG	SWIM Implementation Pioneer Group
SURICG	Surveillance Implementation Coordination Group
SURSG	Surveillance Study Group
SWIM	System Wide Information Management
SWIM TF	System Wide Information Management Task Force
TFP	Trust Framework Panel
TLS	Transport Layer Security
TOR	Terms of Reference