ChatGPT

Modular multi-vendor sUAS detection common-operating-picture: Standards and protocols

This briefing summarises existing open standards and widely adopted protocols that can underpin a modular “adapter/plugin” ecosystem for a national multi-agency drone/sUAS detection common operating picture (COP). The goal is to combine radar, RF, remote-ID, acoustic and electro-optical (EO) sensors from multiple vendors into a unified map-based interface and to enforce role-based access to detections and historical tracks. Where possible, the report leans toward open standards used in **Modular Open Systems Architecture (MOSA)** and **Sensor Open Systems Architecture (SOSA)**, along with protocols already adopted by Anduril’s Lattice platform (open integration of third-party sensors) [1]. Citations are provided to give authoritative references for each standard.

1. System architecture baseline

1.1 Network and multicast

Area	Standards & recommendations	Why they matter
IP segmentation & multicast	**Source-specific multicast (SSM)** from **RFC 4607** designates IPv4 addresses `232.0.0.0/8` and IPv6 prefix `FF3x::/32` for SSM groups [2]. **IGMPv3** and **MLDv2** allow hosts to inform routers about their desire to receive multicast traffic and support filtering by source [3]. Use PIM-SSM routing with IGMPv3 (IPv4) or MLDv2 (IPv6) to ensure receivers request traffic only from specific sensor sources; avoid any-source multicast to limit cross-delivery [4].	Segregating multicast traffic by vendor and sensor type reduces noise and simplifies access control. SSM ensures an (S,G) channel for each sensor feed and eliminates the need for rendezvous points, making it attractive for real-time video and radar streams.
Campus TSN & QoS	**Time-Sensitive Networking (TSN)** set in IEEE 802.1 standards: 802.1Qbv (Time-Aware Shaper) schedules deterministic transmission, 802.1Qbu/802.3br enable frame pre-emption to reduce guard-band delays, 802.1CB adds Frame Replication and Elimination for reliability, and 802.1Qci provides per-stream filtering and policing [5]. **TSN** leverages **802.1AS** (gPTP) for precise clock synchronisation, and other resource-reservation standards like 802.1Qav (credit-based shaper) now consolidated in **802.1Q-2022** [6].	TSN ensures bounded latency and zero-congestion loss for sensor video, radar and control traffic. Using TSN with VLAN segmentation and per-flow scheduling allows mixing deterministic sensor streams with best-effort IT traffic on the same network without interference.

Area	Standards & recommendations	Why they matter
WAN backhaul & resilience	For WAN or backhaul links, leverage open streaming protocols such as **Reliable Internet Stream Transport (RIST)** or **Secure Reliable Transport (SRT)**. **RIST** main profile defines levels: baseline features (GRE tunnelling, periodic keep-alives), optional features such as null-packet deletion and tunnel bonding [7]. The **DTLS level** provides end-to-end encryption via Datagram TLS and supports server- and client-side certificates [8]; the **PSK level** supports pre-shared keys and key rotation [9]. **SRT** is an emerging IETF draft that provides reliability and security over UDP; it introduces control packets, improved flow/congestion control and optional encryption for low-latency streaming [10].	RIST and SRT are open specifications widely adopted in broadcast. They combine adaptive retransmission (ARQ) and optional FEC for robust streaming over lossy networks. Choosing open protocols avoids vendor lock-in; RIST has explicit profiles for PSK and DTLS encryption, which are attractive for national-level deployments, while SRT is an active IETF work with similar goals.
Backhaul encryption & port admission	**MACsec (IEEE 802.1AE)** provides line-rate encryption and integrity at the Ethernet layer; it uses AES-GCM and relies on 802.1X/EAP for key exchange. MACsec protects frames from eavesdropping and tampering and supports hardware-accelerated encryption [11]; it can be combined with 802.1AR device identities and 802.1X port access control, which requires clients to authenticate before receiving network access [12].	Because sensors will be deployed across agency networks, link-layer security ensures confidentiality and integrity even if higher-layer security is disabled. Port-based network access prevents rogue devices from injecting false tracks.

1.2 Precision timing and synchronisation

Area	Standards & recommendations	Why they matter
Precision Time Protocol (PTP)	**IEEE 1588 (PTP)** synchronises clocks across devices to the sub-microsecond level. PTP uses a hierarchical structure (grandmaster, boundary/transparent clocks), exchange of sync and delay messages, and precise time stamping [13]. Profiles tailored for telecommunications, industrial automation and AI exist.	With multiple radars and RF sensors, accurate time stamping is vital to fuse tracks and determine velocities. Deploy grandmasters and boundary clocks across networks; evaluate PTP High-Accuracy or White Rabbit for sub-100-ns triggers if required.
PTP security	IEEE 1588d extends PTP with security features (Prong A AUTH TLV, GDOI key distribution). MACsec or TLS at the transport layer (Prong B) and architectural hardening (Prongs C & D) remain mandatory for critical infrastructures.	Prevents spoofing or delay attacks that could corrupt track fusion. Use PTP AUTH TLV when vendor support is available; otherwise, rely on MACsec to protect PTP packets.

Area	Standards & recommendations	Why they matter
gPTP/ 802.1AS for TSN	For layer-2 TSN networks, gPTP/802.1AS provides synchronisation with nanosecond-level accuracy and reduces packet delay variation [5].	gPTP ensures determinism required by TSN scheduling and can integrate with 1588 boundary clocks over WAN.

1.3 Logging, telemetry and configuration

Area	Standards & recommendations	Why they matter
Syslog and secure transport	**RFC 5424** defines the modern syslog message format with structured data and vendor-specific extensions [14]. **RFC 5425** specifies transporting syslog over **TLS**, describing how TLS secures syslog messages and mitigates threats such as eavesdropping [15]. **RFC 6587** defines framing for syslog over TCP. Use default port 6514 for syslog-TLS and restrict cipher suites per RFC 9662.	Collect sensor logs, detection events and auditing records in near real-time. Secure transport ensures logs remain confidential and tamper-proof across agency boundaries.
Model-driven telemetry	**NETCONF (RFC 6241)** provides secure, transaction-oriented configuration management over SSH/TLS, supports multiple datastores and uses YANG models [16]. **RESTCONF (RFC 8040)** offers a RESTful API to access YANG data via HTTP methods, using JSON or XML [17]. **gNMI** (gRPC Network Management Interface) from OpenConfig uses gRPC/HTTP2 and protocol-buffers and supports streaming telemetry and atomic transactions [18].	Standardising configuration and telemetry across heterogeneous sensors simplifies integration and auditing. YANG models can define common capabilities (e.g., track output rate, antenna orientation) and allow adapters to map vendor-specific parameters to a common schema.

1.4 Quality of Service (QoS)

Quality of Service is critical to ensure that control messages and high-rate sensor data do not impact each other. **DSCP** values in IP headers request different per-hop behaviors. Cisco's documentation lists **Expedited Forwarding (EF)** (DSCP 46) for high-priority low-latency traffic, **Voice-Admit** (DSCP 44) for voice-controlled flows, and **Assured Forwarding (AF)** classes (e.g., AF41, DSCP 34) for video streams [19] [20]. The **NQB draft** defines DSCP 45 for non-queue-building flows that need low latency but minimal bandwidth, recommending that network devices queue DSCP 45 traffic separately [21]. Apply DSCP markings consistently across sensors and networks and map them to TSN schedules or priority queues.

2. Sensor interfaces and data standards

2.1 Radar

- **EUROCONTROL ASTERIX** is a widely used set of open interface definitions for aviation surveillance. The ASTERIX library contains over seventy message categories; Category 062 (CAT-062) provides system track data and is used for non-cooperative radar tracks [22]. Category 033 carries ADS-B messages, and Category 129 can encode Remote-ID information [23].

ASTERIX data formats include exact bit-level definitions, making them interoperable across vendors. Use CAT-062 for radars and GMTI sensors, ensuring that packet sizes avoid IP fragmentation.

- **STANAG 4607 (GMTI)** is a NATO standard for Ground Moving Target Indicator data; it defines a flexible message format that can be tailored to send detailed data for targeting or minimal data for situational awareness, promoting interoperability [24].
- **STANAG 4609** is the NATO digital motion imagery standard for Full-Motion Video. It encapsulates H.264/H.265 video in MPEG-TS with MISB Key-Length-Value (KLV) metadata (e.g., platform position, sensor orientation, timestamps) [25]. Use MISB ST 0601/0603/0604 for KLV metadata and ST 0903 for Video Moving Target Indicator (VMTI) metadata [26]. Ensuring adherence to STANAG 4609 allows video streams to interoperate across coalition partners.
- **STANAG 4676** defines the data model and message formats for exchanging tracks among ISR systems; it aims to promote interoperability in the production, exchange and exploitation of tracking data [27]. Use STANAG 4676 for inter-system track exchange between the COP and external defence/aviation networks.

2.2 RF and signal intelligence

- **ANSI/VITA 49.2 (VRT)** defines VITA Radio Transport for radio frequency (RF) signal transport. It structures sample payloads with context packets that carry metadata such as bandwidth, centre frequency and timestamps. Adopt VRT for SDR front ends and ensure timestamping is synchronised via PTP.
- **SigMF** (Signal Metadata Format) provides an open standard for recording and sharing RF signal captures. It separates binary I/Q data from JSON metadata, making it easier to share datasets across agencies. Use SigMF for archival and forensic RF data.

2.3 Electro-optical/Infra-red (EO/IR) and acoustic

- STANAG 4609 and MISB standards apply to EO/IR video streams (see above). For audio and acoustic sensors, use **AES67** for interoperability; AES67 interoperates with PTP-synchronised audio transport and ties into SMPTE ST 2059-2 timing guidelines. Ensure PTP parameters match across AES67 and SMPTE profiles to maintain lip-sync and cross-sensor timing alignment.

2.4 Remote-ID

- **ASTM F3411-22a** defines UAS Broadcast and Network Remote-ID. The broadcast message includes unique identifiers, location, altitude, speed and operator information. The standard is widely adopted by regulators (FAA/ EASA). Sensors should ingest ASTM broadcast messages and network Remote-ID messages to populate the COP.
- **IETF DRIP** adds trust to remote-ID. **RFC 9374** introduces **Hierarchical Host Identity Tags (HHITs)** – self-asserting IPv6 addresses providing trustable identifiers with explicit hierarchy to facilitate registry discovery [28]. **RFC 9575** defines authentication formats that allow observers to verify that broadcast Remote-ID messages are signed by the registered owner of the device [29]. Implement DRIP validation in the ingestion pipeline to accept only remote-ID messages with valid signatures and accepted registries.

3. Security and access control

- **Network admission** – Deploy **802.1X** for port-based access control so that only authenticated sensors join the network. 802.1X uses AAA servers (often RADIUS) to authenticate clients and can provide authorization and accounting [12]. Use **MACsec** for per-hop link encryption to ensure confidentiality and integrity across switches [11].

- **Transport security** – For control channels (NETCONF/gNMI) and syslog, use TLS 1.3 (RFC 8446) with mutual authentication. For streaming data, select RIST DTLS level or PSK level for encryption [8] [9]. Avoid legacy protocols such as SSL or IPsec unless mandated.
- **Role-based visibility** – The COP should enforce attribute-based access control. Role definitions can be maintained in an identity management system; sensor outputs can be tagged with sensitivity levels. For example, defence sensors may mask precise coordinates when displayed to civilian operators while still providing aggregated coverage zones.
- **Audit and logging** – Use RFC 5424 syslog with TLS transport for every action on the COP. Keep audit logs for at least the regulatory retention period. Structured data elements (e.g., user ID, action, track ID) enable post-incident investigations. Consider using Message Bus events (e.g., AMQP 1.0 or MQTT 5) with persistent topics for streaming logs.

4. Modular integration (“adapter/plugin” model)

A modular COP should accept sensor feeds through adapters that translate vendor-specific formats into a normalised track/event schema. Design guidelines:

1. **Define a canonical data model** for detections and tracks. Use STANAG 4676 or a custom YANG-derived schema for the canonical model. Adapters map vendor fields (e.g., radar SNR, RF frequency) into this schema and drop unsupported fields. This decouples the core system from vendor updates.

2. **Use open transport protocols and message buses**. Consider DDS/RTPS for real-time publish/subscribe within the mission network; define topics for tracks, video frames and alerts with quality-of-service parameters matching DSCP and TSN priorities. For web-based clients, deliver summarised data via web sockets or gRPC, enforcing the same access-control rules.

3. **Implement dynamic plugin registration**. Each adapter should declare its capabilities via a YANG or JSON manifest (supported message categories, update rate, authentication requirements). When a new sensor is added, its adapter is deployed and registered with the COP; the system automatically subscribes to its (S,G) multicast channels and maps its outputs to the canonical model.

4. **Test interoperability**. Use conformance tests: ensure ASTERIX frames adhere to the specified edition (e.g., CAT-062 Ed 1.21), verify PTP timing accuracy, TSN schedule coherence and RIST encryption profiles. Accept only sensors that pass baseline and security tests.

5. **Support scalability**. Use load-balanced ingest clusters to handle bursts of detections, replicate data using 802.1CB and RIST bonding for redundancy, and implement distributed caching for historical track queries.

5. Adoption considerations and pitfalls

Benefits of open standards

- **Interoperability and vendor diversity** – SOSA and MOSA frameworks emphasise open standards to permit rapid integration of new sensors and effectors. Anduril’s Lattice platform demonstrates this by integrating third-party sensors through an open architecture [1]. Aligning with widely adopted standards (ASTERIX, STANAG 4676, IEEE 802.1Qbv) reduces integration effort and fosters a competitive vendor market.

- **Future-proofing** – Standards such as TSN and PTP are actively evolving; aligning early ensures compatibility with next-generation sensors (e.g., high-bandwidth phased-array radars). RIST and SRT are community-driven and likely to remain relevant in broadcast and defence streaming.
- **Security** – Adhering to MACsec, TLS, 802.1X and DRIP provides defence-in-depth. Standardised logging and telemetry facilitate audits.

Potential pitfalls and alternative perspectives

1. **Standards divergence** – Many standards exist with overlapping scope (e.g., ASTERIX vs. STANAG 4676 vs. custom vendor formats). Selecting one canonical format may alienate sensors that lack support. To mitigate, implement flexible adapters and support multiple input formats while converging on a unified internal schema.

2. **Latency vs. reliability trade-offs** – TSN and RIST provide deterministic timing and reliability but increase complexity and may require expensive switches. In some deployments, simple QoS with DSCP and DiffServ may suffice. Evaluate the cost/benefit before adopting full TSN across the network.

3. **Regulatory changes** – Remote-ID standards and UAS regulations are evolving. Investing heavily in ASTM F3411-22a and DRIP now may necessitate updates when regulators adopt new frameworks. Consider modular remote-ID ingest to adapt to future protocols.

4. **Vendor lock-in disguised as open** – Even with open standards, some vendors may implement proprietary extensions or licensing terms. Conduct thorough interoperability tests and demand open documentation to avoid hidden lock-in.

5. **Complexity of security management** – Implementing MACsec, 802.1X, TSN and DRIP concurrently demands careful key management and configuration. Automation (e.g., using NETCONF and gNMI) can help but also introduces new attack surfaces; maintain rigorous security hygiene and auditing.

By embracing the above standards and protocols, the multi-vendor sUAS detection COP can achieve a modular, vendor-agnostic architecture. Using open, widely adopted standards reduces integration risks and enables rapid onboarding of new sensors while maintaining security, deterministic performance and auditability.

---

1 Anduril Lattice to provide counter drone defence for Royal Australian Air Force – Unmanned airspace
https://www.unmannedairspace.info/counter-uas-systems-and-policies/anduril-lattice-to-provide-counter-drone-defence-for-royal-australian-air-force/

2 4 RFC 4607: Source-Specific Multicast for IP
https://www.rfc-editor.org/rfc/rfc4607.html

3 RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
https://www.rfc-editor.org/rfc/rfc4604.html

5 6 Guide to Time-Sensitive Networking (TSN) - Industry Collaboration on Risk Mitigation
https://www.windriver.com/resource/hitting-the-moving-target-with-time-sensitive-networking-white-paper

7 8 9 Microsoft Word - VSF_TR-06-2-levels-annex_2020_08_05.docx
https://static.vsf.tv/download/technical_recommendations/VSF_TR-06-2-levels-annex_2020_08_05.pdf

10 The SRT Protocol
https://haivision.github.io/srt-rfc/draft-sharabayko-srt.html

11 MACsec Explained: Security for Enterprise Networks
https://www.fs.com/blog/macsec-a-cool-security-option-for-your-enterprise-switch-449.html

12 What is 802.1X Authentication? | Auvik
https://www.auvik.com/franklyit/blog/802-1x-authentication/

13 What is Precision Time Protocol (PTP)? | Glossary | HPE
https://www.hpe.com/us/en/what-is/precision-time-protocol.html

14 RFC 5424 - The Syslog Protocol
https://datatracker.ietf.org/doc/html/rfc5424

15 RFC 5425 - Transport Layer Security (TLS) Transport Mapping for Syslog
https://datatracker.ietf.org/doc/html/rfc5425

16 17 18 Evolution of Management Protocols For Network Devices
https://codilime.com/blog/evolution-management-protocols-network-devices/

19 20 DSCP Options in Network Tests | ThousandEyes Documentation
https://docs.thousandeyes.com/product-documentation/tests/network-tests/dscp-options-in-network-tests

21 A Non-Queue-Building Per-Hop Behavior (NQB PHB) for Differentiated Services
https://www.ietf.org/archive/id/draft-ietf-tsvwg-nqb-14.html

22 23 Open Framework Standards for Combined Aircraft Sensor Network for the State of Ohio To Detect and Track Lower Altitude Aircraft. Volume 1 of 1
https://rosap.ntl.bts.gov/view/dot/73158/dot_73158_DS1.pdf

24 Evolution of Standard: The STANAG 4607 NATO GMTI Format
https://www.mitre.org/sites/default/files/pdf/05_0164.pdf

25 26 STANAG 4609 – ISR Video – ImpleoTV
https://impleotv.com/2025/03/11/stanag-4609-isr-video/

27 NISP Nation
https://nisp.nw3.dk/standard/nato-aedp-12-ed.a-v1.html

28 RFC 9374: DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)
https://www.rfc-editor.org/rfc/rfc9374.html

29 RFC 9575: DRIP Entity Tag (DET) Authentication Formats and Protocols for Broadcast Remote Identification (RID)
https://www.rfc-editor.org/rfc/rfc9575.html