ChatGPT

Technical Standards for Multi-Vendor sUAS Detection COP

Figure: A small unmanned aerial system (DJI Mavic 2) in flight – the type of UAS target a national detection network must track. This document defines open-standards-based interfaces and protocols for a **multi-vendor, multi-agency UAS detection Common Operating Picture (COP)**. The system follows a plug-in **Adapter architecture**, where each sensor's proprietary output is translated (via software "gateways") into canonical, open formats before entering the COP. This avoids vendor lock-in and enables the central COP to rely solely on open protocols. The COP must integrate radar, RF, EO/IR, acoustic and Remote ID data, fuse them in real time, and display a unified situational picture while enforcing role-based data sharing. It uses a layered approach with clear interfaces: sensor networks on one side, a core processing/fusion engine in the middle, and user displays on the other. All components use defense-grade cybersecurity (authentication, encryption, logging) and precise time-stamping for data correlation.

Summary: The COP collects diverse sensor data into one system. It uses an "Adapter" model to translate all inputs into open formats. The goal is unified awareness and modular interoperability. Data is time-synchronized and securely exchanged, with fine-grained access control for multi-agency use.

2. Network Infrastructure

IP Networking: The system uses **dual-stack IPv4/IPv6** networks. IPv6 is essential for the large address space needed by hundreds of sensors, but IPv4 is kept for backward compatibility. All network devices (switches, routers) must support both stacks. Sensors are grouped by function and sensitivity: e.g. radar

in one VLAN, EO cameras in another, with strict segmentation. No “flat” network allowed – inter-VLAN routing is strictly controlled by firewalls to enforce domain isolation.

- **Rationale:** IPv6’s 2^128 address space lets every sensor and endpoint have a unique address without NAT, simplifying large-scale deployments. Network segmentation (using 802.1Q VLANs) enforces security boundaries between agencies or sensor types. This “defense-in-depth” restricts lateral movement if one segment is compromised.

Multicast for Sensor Feeds: Real-time sensor data (radar plots, video streams) is distributed via **Source-Specific Multicast (SSM)**. In SSM, a receiver subscribes to a specific source IP and group; this prevents a rogue node from injecting bogus data. We use **PIM-SSM** routing with IGMPv3 (for IPv4) and MLDv2 (for IPv6) on hosts. By default the IPv4 SSM range 232.0.0.0/8 is used and IPv6 SSM uses FF3x::/32 [1]. All receivers must implement IGMPv3/MLDv2 to filter to legitimate (S,G) streams [2]. Any-Source Multicast (ASM) is disallowed except for legacy exceptions.

- **Rationale:** SSM’s (S,G) model means receivers explicitly name the trusted source of data, greatly reducing spoofing risk. The IANA-reserved SSM ranges (IPv4 232/8 and IPv6 FF3x::/32) ensure interoperability [1]. Using multicast is much more efficient for live video and radar (one-to-many) than duplicating unicast streams. (If multicast is impossible, a brokered pub/sub like MQTT can be used as a less-efficient alternative.)

Quality of Service (QoS) and TSN: Sensor traffic is classified and prioritized using **Differentiated Services (DiffServ)** and, where possible, **Time-Sensitive Networking (TSN)**. Critical control messages (radar alarms, user “drone detected” alerts) are marked with **DSCP EF (46)** for Expedited Forwarding (low delay/jitter) [3]. High-bandwidth video (EO/IR, radar) uses Assured Forwarding (e.g. AF41/34) for reliable throughput. Audio streams use Voice-Admit (VA/44) for low-latency. Telemetry and best-effort data get a standard or “Non-Queue-Building” (CS6/48 or NQB/45) class. On switches with TSN support, IEEE 802.1Qbv **Time-Aware Shaping** enforces scheduled delivery for EF flows [4]. All devices must honor and queue-mark DSCP consistently.

- **Rationale:** This prevents a single heavy stream (like 4K video) from overwhelming low-latency signals. EF (Expedited Forwarding) is known to give sub-50ms delay for critical packets [3]. TSN scheduling (802.1Qbv/Qbu) can reserve time slots for the most time-critical flows (e.g. control commands or synchronized video frames) [4]. In short, QoS ensures “Drone Detected” alerts or track updates outrank bulk video.

Summary: The network uses IPv4/IPv6 with strict segmentation and VLANs. Sensor feeds use PIM-SSM multicast (addresses 232.0.0.0/8 or FF3x::/32 [1]) with IGMPv3/MLDv2 filters [2]. QoS (DSCP) and TSN shaping give priority to urgent control and detection traffic over bulk video.

3. Timing and Synchronization

Precision Time Protocol (PTP): All sensors and processing nodes must sync clocks via IEEE 1588-2019 PTP (v2.1) to microsecond accuracy. A grandmaster clock (with an OCXO oscillator) distributes time over the network. Intermediate switches operate as **boundary or transparent PTP clocks**, reducing delay jitter. End-to-end skew should be $\leq$1 microsecond on a site network. We use the telecom profile (ITU G.8275.1) for long backhaul links if needed. Redundant grandmasters run IEEE’s Best Master Clock Algorithm (BMCA) for failover.

- **Rationale:** When fusing data from multiple sensors, precise time correlation is vital. For example, matching a radar’s track at T=10.000s with a camera’s frame at T=10.001s requires sub-

microsecond sync. PTP routinely achieves ≈100 ns on LANs [5]. NTP (milliseconds) is too coarse. Using hardware clocks and boundary clocks makes delivery deterministic.

PTP Security: Timing is a critical attack vector. We apply IEEE 1588d-2023's security measures:
- *Authentication TLVs:* PTP packets carry cryptographic signatures (IEEE 1588 Prong A) [6].
- *Link Encryption:* All PTP messages on the LAN are inside MACsec (IEEE 802.1AE) links [7], preventing off-path attacks (Prong B). At minimum, enforce IPsec on any routed segments.
- *Filtering/HW Enforcement:* Network devices validate that only authorized masters speak PTP (Prong C). Any replayed or out-of-expected-path timing packets are dropped.
- *Monitoring:* Continuously monitor offset, delay, and BMCA state (Prong D) for anomalies.

- **Rationale:** A corrupted time source can desynchronize the COP, hide events, or spoof tracks. The four-pronged approach (auth TLV, encrypted transport, path validation, monitoring) is recommended by experts for PTP defense [6] [7]. For example, MACsec provides line-rate encryption of PTP on switches [7]. TLS or IPsec would be used for any PTP-over-IP tunnels.

Alternate gPTP (802.1AS): In segments with TSN (802.1Qbv switches), we may use IEEE 802.1AS (gPTP), which is a profile of 1588 optimized for nanosecond sync in bridged networks. gPTP would only be used for truly timing-critical streams (e.g. synchronized radar video) where TSN scheduling is in use.

Summary: All clocks use IEEE 1588 PTP (v2.1) with boundary clocks, achieving ≲1µs sync [5]. PTP packets are authenticated and encrypted (macsec/IPsec) to prevent attacks [6] [7]. A backup profile (gPTP) is available in TSN segments.

4. Security Standards

Device Authentication (802.1X & DevID): Every sensor and switch port uses IEEE 802.1X (EAP-TLS) for network admission. Each device must hold an IEEE 802.1AR *DevID* certificate (hardware root identity). On link-up, the device presents its certificate to the RADIUS/PKI server. Unauthenticated or failed devices are immediately quarantined. Management of certificates is centralized (enterprise PKI).

- **Rationale:** This enforces *zero-trust* at the network boundary: a bad actor physically plugging in a cable cannot join the network without a valid cert. The DevID (IDevID) ties identity to hardware. In effect, only pre-registered sensors or computers get network access.

Link-Layer Encryption (MACsec): All wired connections between edge and core switches (especially between agencies) must use IEEE 802.1AE (MACsec) with 256-bit keys. We use MKA (MACsec Key Agreement) to manage keys. Cipher suite: AES-GCM-256 (CHACHA20-Poly1305 is an option in newer revisions). Keys are rotated automatically at least daily; control vs data traffic use separate keys.

- **Rationale:** MACsec encrypts every packet on the wire (broadcast, multicast, unicast) at line rate, preventing eavesdropping and injection. It's more efficient than IPsec for local links. Modern hardware supports AES-GCM-256 for very low latency encryption [8].

Logging & Audit (Syslog/TLS): All components generate structured audit logs (in IETF syslog format, RFC 5424). Logs are forwarded in real time over TLS (RFC 5425 on port 6514 [9] [10]) to central collectors. TLS 1.3 with mutual authentication is used, and we follow cipher restrictions (RFC 9662). The

log stream uses RFC 6587 octet-counting framing. Each log entry includes user, action, timestamp and sensor/data provenance.

- **Rationale:** Using TLS-protected syslog centralizes auditing across agencies and vendors. RFC 5425 explicitly secures syslog with TLS [9], ensuring log confidentiality/integrity. Port 6514 is the standard port [10]. This meets compliance and forensics needs: any data or configuration change is recorded in a tamper-evident way.

Summary: Network ports enforce 802.1X/EAP-TLS with DevID certs so only authorized devices join. All Layer-2 links use MACsec (AES-256-GCM) to encrypt traffic [8]. Every action is logged in structured syslog over TLS [9] for audit and non-repudiation.

5. Sensor Interface Standards

Each sensor type has a standardized data output format (the “canonical model”) for the COP. Adapters/gateways perform any necessary conversion from proprietary formats into these standards. All timestamps on data are PTP-based.

5.1 Radar Sensors

5.1.1 Track Data

Standard: EUROCONTROL *ASTERIX Category 062* for System Track messages.
ASTERIX is an internationally adopted binary format for air-surveillance data [11]. CAT-062 defines track reports: each includes a unique Track ID, time, position (lat/long/alt), velocity, and classification. Mandatory fields for our use: System Area/ID code (SAC/SIC) to identify the radar site, Track ID, timestamp, and state (e.g. confirmed vs tentative). All fields must fit in a UDP packet without fragmentation. Time-of-track is taken from the synchronized PTP clock.

- **Rationale:** ASTERIX is the de-facto standard in civil/military radar networks [11]. It ensures any ASTERIX-capable fusion engine can read tracks from any vendor. It’s compact and extensible. (As an alternative for military settings, STANAG 4676/AEDP-12 is defined by NATO for tracking.)

5.1.2 Radar Video

Standard: EUROCONTROL *ASTERIX Category 240* for raw radar video.
Radar video (all returns) is sent as sequential data frames over UDP (multicast) with timestamps. ASTERIX CAT-240 specifies the format of each frame (range bins, azimuth, etc). Frames are tagged with a PTP-aligned timecode and sent via (S,G) multicast. MTU must be sized to avoid IP fragmentation.

- **Rationale:** Using a standard radar video format means visualization clients can natively display live video from any ASTERIX sensor. It also allows applying uniform preprocessing (e.g. CFAR) on the COP side. ASTERIX 240 is widely supported by air traffic radars.

Figure: A radar antenna (satellite dish form) – similar to those used in border surveillance. Radar sensors report tracks and video according to ASTERIX standards.

5.2 RF/Signals Sensors

5.2.1 Live Data Transport

Standard: *ANSI/VITA 49.2 (VITA Radio Transport, VRT)*.
RF sensors stream digitized spectrum (I/Q samples) and context in VRT packets. Each packet includes a high-precision timestamp (PTP-derived) and context fields for center frequency, bandwidth, gain, etc [12]. The transport is typically UDP (unicast or multicast) to the COP. Packet size must also avoid fragmentation.

- **Rationale:** VITA-49 is an open standard specifically for streaming RF data with metadata [12]. It is supported by many SDR and spectrum sensors. Using it allows the COP to perform cross-sensor correlation (e.g. matching a radar track to an RF signal) because all details of the RF stream are explicit.

5.2.2 Archived Data

Standard: *SigMF (Signal Metadata Format)*.
Offline I/Q captures from RF sensors are archived using SigMF: a JSON metadata file alongside the binary I/Q data. The metadata includes sample rate, center freq, time stamps, sensor ID, plus annotations.

- **Rationale:** SigMF is an emerging open format for signal data. It decouples metadata from raw payload, making long-term storage and analysis easier. It ensures analyses can be reproduced across tools.

5.3 EO/IR Video and Imagery

Standard: *STANAG 4609 FMV* with MISB KLV metadata (ST 0601/0603/0604/0903). Video streams from cameras (drones, towers, etc) use MPEG-TS encapsulated H.264 or H.265. Embedded in the transport stream are MISB KLV metadata packets: ST 0601 (UAS position and orientation), ST 0603/0604

(timestamp and frame sync), and ST 0903 (Video Moving Target Indicator, if available). Video frames are aligned to PTP time per SMPTE ST 2059-2 guidance.

- **Rationale:** STANAG 4609 is the NATO standard for full-motion video exchange, ensuring interoperability [13]. Its MISB metadata conveys camera geolocation and pointing, so the COP can georegister video: e.g. draw the camera's field-of-view on the map or triangulate targets. Standardizing on KLV means all EO data (from planes, UGVs, etc.) can be fused coherently.

Alternative Transport: For remote feeds over wide-area networks (e.g. between cities), RIST (VSF TR-06) or SRT can be used to convey the MPEG-TS reliably with ARQ/FEC. These protocols should be run over DTLS or SRT's encryption for confidentiality.

Figure: A high-resolution surveillance camera, typical of EO/IR sensors that feed the COP. EO/IR streams use STANAG 4609 (NATO FMV) with embedded metadata for geo-tagging.

5.4 UAS Remote ID

5.4.1 Message Format

Standard: *ASTM F3411-22a (UAS Remote ID)*.
The COP ingests broadcast and network Remote ID messages per F3411. This standard specifies what information a UAS (or operator) must broadcast over radio (or to internet) so authorities can identify it. The format includes UAV ID, location, velocity, system info, etc.

- **Rationale:** ASTM F3411 is the mandated specification by regulators (FAA, EASA, etc.) for drone identification. Using it ensures the COP can interface with any compliant UAS.

5.4.2 Authentication

Standard: *IETF DRIP (RFC 9434 & RFC 9575)*.
Remote ID alone is unauthenticated. We require the **Drone Remote ID Protocol (DRIP)** overlay to add digital signatures. DRIP Entity Tags and Host Identity Tags (HHIT) are used. The system validates

signatures in RFC 9575 AUTH messages against registries. Messages failing DRIP validation are flagged as “spoofed”.

- **Rationale:** Cryptographic signing prevents hostile actors from faking Remote ID signals. DRIP provides a trust framework (with IANA registries and RFC-defined formats) so that observers can verify a broadcast RID came from a genuine registered UAS [14] [15]. This lets the COP distinguish “blue” (friendly) drones from “red” (unknown/spoof) ones.

Summary: Radar data use ASTERIX 062/240 for tracks and raw video, ensuring full compatibility [11]. RF sensors stream VITA-49 formatted I/Q (with SigMF archives) [12]. EO/IR cameras use STANAG 4609/H.264+KLV metadata [13]. Remote ID uses ASTM F3411, augmented with IETF DRIP crypto for authenticity [15] [14].

6. Data Exchange and COP Functions

Track Fusion (STANAG 4676): Internally, the COP fuses tracks using the NATO STANAG 4676 format (AEDP-12). Each fused track record contains position, velocity, a covariance matrix, and provenance (which sensors contributed). The standard supports track splitting/merging and quality fields. All track updates include a unique Track ID.

- **Rationale:** STANAG 4676 is specifically designed for multi-sensor ISR tracking. It captures lineage (which sensors, times) and uncertainties, enabling downstream systems to trust and audit the fusion. Using an international tracking standard ensures interoperability between allied systems.

Role-Based Visibility (ABAC): Access to data in the COP is controlled by **Attribute-Based Access Control** with data tagging. Every data element (track, video, sensor origination) carries a classification tag (e.g. based on source agency). Policies then use user attributes (agency, clearance, role) plus context to grant or deny. For example, a battlefield sensor might tag location as “SECRET”; a border guard with lower clearance might see the track object (position/velocity) but without precise origin coordinates. Any time data is shared across agencies, “downgrading” or obfuscation (e.g. jitter or vague location) may occur per policy.

- **Rationale:** Simple role-based schemes are too coarse. NATO’s STANAG 4774 provides XML/JSON labeling for data confidentiality [16]. By using ABAC, the COP can flexibly share just-enough data. (E.g., a police officer might see a “drone track” but not its exact flyover point.) All access decisions and data releases are logged.

Summary: The COP fuses sensor tracks into a unified track picture (e.g. using STANAG 4676 internally). Access to tracks and data is controlled by fine-grained ABAC policies with labeling (per STANAG 4774) [16], so agencies only see what they are allowed.

7. Backhaul and Resilience

Wide-Area Video Streaming: When relaying video or sensor feeds over public networks (WAN/4G/5G), we use **RIST (Main Profile)** or **SRT** protocols. Both add ARQ/FEC to UDP, recovering from packet loss. RIST (VSF TR-06) can natively bond multiple links and support multicast; it uses RTP/UDP underneath. SRT (IETF draft) is a uni-directional ARQ over UDT/UDP with AES-128/256 encryption. Configure ARQ

retransmit rates and FEC dynamically per link quality. Always use DTLS (RIST) or SRT encryption on these links. Failover between paths (e.g. LTE vs fiber) must be hitless (<500ms switchover).

- **Rationale:** Standard UDP will drop too many packets on lossy backhauls. RIST and SRT are open, industry-backed solutions. RIST especially (main profile) is preferred for multi-user broadcasts and bonding, while SRT is common for point-to-point streams. Both avoid proprietary "video-over-IP" protocols. Using DTLS/AES ensures confidentiality across public networks.

Redundant Delivery (802.1CB FRER): At network edges (before a WAN link), critical streams may be replicated on two independent paths to guarantee delivery. IEEE 802.1CB defines **Frame Replication and Elimination for Reliability (FRER)**. Each packet (e.g. a video frame) is tagged with a sequence number; an upstream switch multicasts duplicates along separate routes; a downstream node then drops duplicates, delivering a single sequence to the application. FRER runs over bridged networks (TSN). The COP must monitor path health and remove stale duplicates.

- **Rationale:** Some sensor feeds (radar video, live maps) cannot tolerate even a single lost packet. 802.1CB provides "zero-loss" transport without relying on application retries [17]. In essence, it achieves seamless hitless redundancy at Layer 2: if one path fails, the other has the frame. This is vital for deterministic delivery where latency of retries is unacceptable.

Summary: For WAN links we use RIST (preferred for multicast/backbone) or SRT (P2P) with ARQ/FEC and AES/DTLS. In LAN/TSN segments we use IEEE 802.1CB to replicate and drop duplicates, achieving lossless redundancy [17].

8. Configuration and Telemetry

Configuration Management: Devices and applications expose YANG models and are configured via **NETCONF** (RFC 6241) over SSH. Each managed device implements approved YANG schemas (e.g. interface, VLAN, PTP configuration). Changes are transactional (commit/rollback). For environments more suited to HTTP, **RESTCONF** (RFC 8040) is allowed as an alternative over TLS. All configuration actions are logged and audited.

- **Rationale:** NETCONF/YANG is the modern standard for network device configuration. It supports rollbacks and validation. Using YANG ensures parameters are typed and standardized. One could also use a controller (Ansible etc.) on top of NETCONF, but the key is structured config.

Telemetry (gNMI): For monitoring, devices stream operational metrics using **gNMI (gRPC Network Management Interface)** with OpenConfig YANG models. Metrics like CPU, temperature, interface counters, etc. are sent as streaming updates (on-change or periodic). gNMI uses HTTP/2 and Protobuf for efficiency. Subscription parameters (intervals) are configurable. All telemetry is sent over mutual-TLS-authenticated channels.

- **Rationale:** gNMI is more efficient and scalable than SNMP polls. It enables high-frequency, model-driven telemetry. Per Cisco: "Model-driven telemetry using protocols such as NETCONF... and gNMI [give] consistency, flexibility and a programmatic framework" [18].

Summary: Management uses standard YANG/NETCONF (or RESTCONF) for configs. Telemetry is via gNMI/OpenConfig streams over gRPC, providing efficient, structured monitoring [18]. Both use mutual-TLS for security.

9. Testing and Conformance

All systems must pass acceptance tests to confirm compliance.

- **Timing Tests:** Verify end-to-end PTP offset ≤1µs. Check BMCA failover <1s. Use PTP YANG models to measure path delay. Simulate rogue master and ensure it is rejected by prong-C filters.

- **Multicast Tests:** Verify IGMPv3/MLDv2 join latency <1s. Confirm (S,G) filters work (unauthorized streams should never reach listeners). During single-link outages, FRER should prevent any packet loss (check sequence continuity).

- **Security Tests:** Follow NIST SP 800-115 methodology. Attempt VLAN hop, unauthorized 802.1X, MACsec break, PTP spoofing. Ensure logs capture all events and survive reboot (write-protect and verify log integrity).

- **Throughput/Latency:** Confirm QoS/TSN priority works by flooding the network with low-priority traffic and ensuring high-priority streams stay within latency bounds. Use hardware timestamping where possible.

Summary: Acceptance tests will use industry standard methods (e.g. NIST 800-115 for security). Key metrics: PTP skew ≤1µs, IGMP join <1s, FRER no-loss, and full audit log recoverability. Only devices meeting these criteria are approved.

Sources: Standards cited above (802.1X/AE/AR, PTP RFCs, ASTERIX, STANAGs, MISB, RFC 5424/5425, etc.) come from official publications [1] [2] [4] [3] [5] [6] [7] [19] [8] [9] [13] [20] [12] [16] [18] [11] [15] [14]. All interfaces and protocols listed above are open standards or widely supported specifications; vendors and agencies should ensure compliance with these specs when integrating sensors and systems.

---

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

2 Example: Configuring Source-Specific Multicast | Junos OS | Juniper Networks
https://www.juniper.net/documentation/us/en/software/junos/multicast/topics/topic-map/mcast-ssm.html

3 RFC 4594 - Configuration Guidelines for DiffServ Service Classes
https://datatracker.ietf.org/doc/html/rfc4594

4 Time-Aware Shaping — INET 4.5.4 documentation
https://inet.omnetpp.org/docs/showcases/tsn/trafficshaping/timeawareshaper/doc/index.html

5 Precision time protocol (PTP)
https://arubanetworking.hpe.com/techdocs/AOS-CX/10.12/HTML/fundamentals_6300-6400/Content/Chp_PTP/ptp.htm

6 7 Securing Critical Timing Infrastructure
https://ww1.microchip.com/downloads/aemDocuments/documents/FTD/ProductDocuments/WhitePaper/Securing-Critical-Timing-Infrastructure-White-Paper-00004262A.pdf

8 19 IEEE 802.1AE - Wikipedia
https://en.wikipedia.org/wiki/IEEE_802.1AE

9 10 RFC 5425 - Transport Layer Security (TLS) Transport Mapping for Syslog
https://datatracker.ietf.org/doc/html/rfc5425

11 ASTERIX - Wikipedia
https://en.wikipedia.org/wiki/ASTERIX

12 VITA - VITA 49 Overview
https://www.vita.com/page-1855484

13 20 STANAG 4609 – ISR Video – ImpleoTV
https://impleotv.com/2025/03/11/stanag-4609-isr-video/

14 RFC 9575 - DRIP Entity Tag (DET) Authentication Formats and Protocols for Broadcast Remote Identification (RID)
https://datatracker.ietf.org/doc/rfc9575/

15 thedroneprofessor.com
https://thedroneprofessor.com/wp-content/uploads/2022/11/F3411.40165-UAS-Remote-ID.pdf

16 Ensuring NATO STANAG 4774 and 4778 Compliance
https://www.archtis.com/achieving-nato-stanag-4774-and-4778-compliance/

17 P802.1CB – Frame Replication and Elimination for Reliability |
https://1.ieee802.org/tsn/802-1cb/

18 Telemetry in Action: NETCONF and gNMI with a Custom-Built Collector! - Cisco Blogs
https://blogs.cisco.com/datacenter/telemetry-in-action-netconf-and-gnmi-with-a-custom-built-collector