ODA3 INSTITUTE

SECTOR CALIBRATION PACKAGE

PAI-SF™ Drones and Uncrewed Systems Sector Guide

Physical AI Security Framework v1.0 — Sector Calibration Package

ODA3-2026-07-SCP-PAISF-014 | Public-Facing — Sector Calibration Package

Document Control

Doc ID	ODA3-2026-07-SCP-PAISF-014
Doc Type	Sector Calibration Package
Framework Tag	PAI-SF™ v1.0
Governing Licence	GAISSF Ecosystem Licence (GEL v1.0)
Access Classification	Open / Public sector guidance; commercial delivery remains subject to GEL v1.0 licence terms
Publication State	Publication Candidate — pending formal publish action
Publish Date / Review Cycle	01 August 2026 (content finalized); publication date to be confirmed
Classification	Public-Facing — Sector Calibration Package

PAI-SF™ Drones and Uncrewed Systems Sector Guide

Physical AI Security Framework v1.0 — Sector Calibration Package

Sector Position

This guide calibrates PAI-SF™ v1.0 for drones and uncrewed systems where AI-enabled sensing, navigation, mission autonomy, payload control, and physical actuation may affect people, aircraft, infrastructure, property, or operating environments. It is sector guidance, not aviation approval, airworthiness certification, or an assessment-scoring method, and it operates under **Kinetic Zero Trust** — PAI-SF's core assurance principle that AI-generated physical action must be validated against independent safety boundaries, not trusted on model confidence alone.

1. Scope and Use

The guide applies to drones, uncrewed aerial systems, uncrewed ground or maritime systems where relevant, autonomous inspection platforms, delivery drones, AI-assisted remote-piloted systems, fleet or swarm operations, and payload-bearing systems whose behavior depends on models, perception components, navigation, sensor fusion, or adaptive autonomy. It is intended for security, aviation, autonomy, fleet, compliance, safety, and assurance teams preparing an initial PAI-SF scoping exercise.

Included	Use With Care	Out of Scope
AI-enabled drones and uncrewed systems with flight, mission, navigation, payload, or physical-environment consequence.	Remote-piloted drones where AI supports perception, route planning, or operator recommendations but does not directly command flight.	Replacement of aviation regulation, operational approval, airworthiness, pilot/operator qualification, or mission authorization.
Security conditions that may create or worsen physical consequences in air, ground, maritime, indoor, site, or fleet operations.	General aviation, airspace, or drone-cybersecurity issues with no AI-driven sensing, inference, autonomy, or physical command path. Existing flight-safety, maintenance, airworthiness, and operational-risk artifacts used as evidence for the AI-security	

Included	Use With Care	Out of Scope
	assurance layer.	

2. Priority Control Clusters

All 12 PAI-SF domains remain relevant to sector scoping. The following clusters should usually be treated as first-pass priorities for drones and uncrewed systems because they sit closest to the sensing, navigation, command, payload, and physical-consequence path.

Cluster	Primary PAI-SF Controls	Sector Interpretation
Perception, navigation, and environment	PAI-SF-SEN-001 to SEN-003; ENV-001 to ENV-003	Sensor calibration, GNSS/navigation confidence, obstacle perception, weather/lighting assumptions, geofence context, and environment-change response.
Autonomy boundary and mission control	PAI-SF-AUT-001 to AUT-004	Authorized autonomy level, mission envelope, geofence enforcement, command handoff, route/task change control, and escalation governance.
Flight command and kinetic safety	PAI-SF-ACT-001 to ACT-003; SAF-001 to SAF-004; DEG-001	Independent bounds on speed, altitude, heading, payload release, timing/replay, return-to-home, landing, loiter, and degraded flight modes.
Human override and remote intervention	PAI-SF-HOV-001 to HOV-003	Pilot/operator override, ground-control handoff, emergency command path, operator readiness, and reset integrity after intervention.
Telemetry, incident response, and recovery	PAI-SF-TEL-001 to TEL-004; IRP-001 to IRP-003	Tamper-evident flight logs, command/perception telemetry, custody of evidence, physical recovery, containment, and HITL return-to-service.
Supply chain, update, and validation	PAI-SF-ATT-001 to ATT-003; SUP-001 to SUP-003; TST-001 to TST-003; FSI-001 to FSI-004	Airframe/controller provenance, model/firmware updates, staged rollout, simulation-to-flight gap review, safety-interface escalation, and regression testing.

3. Domain Calibration

This table translates the 12-domain PAI-SF architecture into drone and uncrewed-system review language. It does not change the canonical control catalogue.

No.	PAI-SF Domain	Drones / Uncrewed Systems Calibration
1	Sensor and Perception Integrity	Validate camera, lidar/radar where present, IMU, GNSS, altimeter,

No.	PAI-SF Domain	Drones / Uncrewed Systems Calibration
		compass, obstacle-detection, and sensor-fusion behavior under weather, lighting, interference, and occlusion conditions.
2	Actuator and Kinetic Command Safety	Treat thrust, attitude, speed, altitude, route, payload, timing, replay, and command-link behavior as security-assurance evidence because compromise can create physical consequence.
3	Edge Hardware and Model Attestation	Verify flight controller, companion computer, firmware, model, ground-control station, payload controller, and attestation-key provenance where flight behavior depends on local compute.
4	Autonomy Boundaries	Document and enforce mission envelope, autonomy level, geofence, altitude, airspace, route, payload, swarm/fleet, and operator-handoff boundaries.
5	Safe-State and Degraded-Mode Behavior	Define and test credible degraded states such as return-to-home, controlled landing, loiter, hover, operator handoff, payload inhibit, or mission abort.
6	Human Override and Intervention	Require independent operator or remote-pilot intervention paths, emergency controls, override training, and reset criteria after manual takeover.
7	Runtime Monitoring and Telemetry	Preserve tamper-evident telemetry for navigation confidence, perception state, autonomy mode, command link, payload state, override events, and incident reconstruction.
8	Incident Response and Physical Recovery	Prepare containment, landing/recovery, evidence preservation, damaged-device handling, software rollback, and human-in-the-loop revalidation procedures.
9	Supply Chain and Update Assurance	Control airframe, sensor, firmware, model, controller, payload, ground-station, dependency, and third-party update paths with staged regression evidence.
10	Simulation, Testing, and Validation	Use simulation, hardware-in-the-loop, tethered/controlled flight, adversarial physical-world, RF/navigation degradation, and mission-replay testing.

No.	PAI-SF Domain	Drones / Uncrewed Systems Calibration
11	Functional Safety Interface	Map AI-security findings into applicable aviation, product-safety, functional-safety, and operational risk processes without claiming airworthiness or regulatory compliance.
12	Physical Operating Environment	Maintain a validated account of airspace, operating site, weather, terrain, obstacles, people, infrastructure, launch/recovery zones, and emergency landing assumptions.

4. Starter Evidence Pack

A first-pass review should collect enough evidence to determine whether the aircraft, vehicle, fleet, payload, or mission system can be scoped for deeper PAI-SF assessment. The list below is intentionally a starter pack, not a complete audit request list.

Evidence Area	Examples to Collect
System and mission scope	Aircraft/platform inventory, autonomy level, mission types, operating site, geofence, altitude envelope, payload class, operator role, and physical operating assumptions.
Perception and navigation assurance	Sensor calibration records, GNSS/navigation confidence handling, obstacle-detection tests, weather/lighting limits, interference assumptions, and sensor-disagreement responses.
Command, safe-state, and override	Flight-command architecture, speed/altitude/route bounds, replay/timing controls, return-to-home/landing logic, emergency command path, and post-override reset criteria.
Telemetry and evidence readiness	Flight-log map, command-link telemetry, payload-state telemetry, tamper-evidence controls, retention/custody rules, and incident reconstruction procedure.
Update and component assurance	Firmware/model/payload provenance, ground-control software inventory, staged update process, physical regression suite, and third-party component assurance records.
Validation and safety interface	Simulation and controlled-flight evidence, mission-replay cases, RF/navigation degradation tests, safety-case mapping, and unresolved AI-security gap register.

5. Integration Notes

PAI-SF should be applied beside aviation safety, UAS operational risk, product safety, fleet management, maintenance, cybersecurity, and site-safety practices. For this sector, existing aviation or mission-approval artifacts may support evidence about operating limits, emergency procedures,

maintenance controls, and pilot/operator responsibilities. PAI-SF's role is narrower: it asks whether AI-specific sensing, inference, navigation, autonomy, command, payload, telemetry, update, and recovery conditions are adequately assured where conventional drone or aviation processes may not fully address learned, adaptive, or fleet-updated behavior.

Boundary Discipline: An operational approval package, maintenance record, safety case, flight test campaign, or airspace authorization may provide useful evidence, but it should not be treated as automatic PAI-SF coverage. The review must still test whether AI-specific perception drift, navigation degradation, autonomy boundary changes, command-link compromise, payload control, telemetry gaps, incident reconstruction, and return-to-service risks are addressed.

6. Notably Absent

Absent Claim	Clarification
No aviation or UAS regulatory approval claim	This guide does not establish airworthiness, type certification, BVLOS permission, airspace authorization, pilot/operator licensing, or compliance with civil aviation rules.
No flight-safety certification claim	The guide does not certify that a drone or uncrewed system is safe to operate, fit for a mission, or accepted by any aviation, defense, site, or safety authority.
No replacement for aviation safety engineering	Flight safety, operational risk assessment, product safety, maintenance, airspace management, and regulatory approval processes remain necessary and separate.
No scoring or certification logic	The guide does not publish assessment scoring, maturity thresholds, auditor procedures, test protocols, or certification-decision criteria.
No universal mission profile	Inspection drones, delivery drones, counter-UAS systems, swarms, defense systems, agricultural drones, maritime/ground uncrewed systems, and indoor drones require system-specific scoping.

On GAISSF Domain 9: GAISSF Domain 9 control titles are cited via the verified crosswalk (ODA3-2026-07-CSX-PAISF-004), not reproduced independently in this guide.

7. Next Use

This sector guide should be used with the PAI-SF Framework Standard, Control Catalogue, Quick Start Guide, and Standards Crosswalk. Assessment planning, scoring, maturity treatment, auditor qualification, flight authorization, operational approval, and certification language remain outside this guide and should be handled through the controlled assessment and conformance-documentation set when authorized.