

ODA3 INSTITUTE

CHEAT SHEET / OPERATOR REFERENCE

PAI-SF™ Cheat Sheet and Operator Reference

Physical AI Security Framework v1.0 — Public Operator Reference

ODA3-2026-07-CHT-PAISF-020 | Public-Facing — Public Operator Reference

© ODA3 Pvt Ltd

Document Control

Doc ID	ODA3-2026-07-CHT-PAISF-020
Doc Type	Cheat Sheet / Operator Reference
Framework Tag	PAI-SF™ v1.0
Audience	Operator, assessor, security lead, safety lead, AI governance lead, incident lead
Companion Document	ODA3-2026-07-NOR-PAISF-005; ODA3-2026-07-CAT-PAISF-006; ODA3-2026-07-AIQ-PAISF-017; ODA3-2026-07-ERL-PAISF-018; ODA3-2026-07-ARC-PAISF-019
Governing Licence	GAISSF Ecosystem Licence (GEL v1.0)
Access Classification	Open / Public reference; scoring, certification, auditor procedures, and controlled scenarios remain Controlled
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 — Public Operator Reference

PAI-SF™ Cheat Sheet and Operator Reference

Physical AI Security Framework v1.0 — Public Operator Reference

Use

Use this reference during first-pass scoping, operator briefing, intake preparation, and evidence triage for physically embodied AI systems. It summarizes how to think with PAI-SF™; it does not replace the Framework Standard, Control Catalogue, Evidence Request List, or controlled assessment materials.

The one-line version of PAI-SF: does this system's AI decide *and* act physically without an independent check? If yes, **Kinetic Zero Trust** applies — the AI's own confidence is never sufficient authorization for physical action on its own.

1. Fast Triage

Rule	Operator Cue
Use PAI-SF	AI-enabled sensing, inference, autonomy, or command logic can affect movement, access, process state, infrastructure state, environment state, or human proximity.
Use GAISSF beside it	The system also has ordinary AI governance, cybersecurity, privacy, data, cloud, identity, model, vendor, or enterprise assurance concerns.
Use sector rules beside it	Aviation, medical-device, vehicle, machinery, infrastructure, workplace, building, telecom, or public-safety obligations may apply independently.
Escalate before review	The team cannot describe the physical consequence

Rule	Operator Cue
	path, command path, override path, degraded mode, update route, or telemetry needed for incident reconstruction.

2. 12-Domain Desk Reference

Read domains as a physical-effect chain: perception, edge identity, autonomy boundary, command, safe state, human intervention, telemetry, recovery, supplier update, validation, safety interface, and operating environment.

ID	Domain	Ask First	Evidence Cue
1	Sensor / Perception	Can the system trust what it sees?	Calibration, drift, spoofing, disagreement, blind spots.
2	Actuator / Command	Can commands create unsafe physical effects?	Bounds, timing, replay, interlocks, divergence.
3	Edge / Attestation	Can field compute be identified and trusted?	Firmware, model package, device identity, local updates.
4	Autonomy Boundaries	What may the system decide or do alone?	Modes, operating domain, limits, escalation.
5	Safe / Degraded Mode	What happens when conditions degrade?	Fallback, safe state, manual mode, recovery trigger.
6	Human Override	Can people intervene reliably?	Authority, stop, handoff, reset, training.
7	Runtime Telemetry	Can events be reconstructed?	Sensor, mode, command, override, safety events.
8	Incident / Recovery	Can physical recovery be governed?	Containment, custody, return-to-service, lessons.
9	Supply / Updates	Can updates alter physical behavior?	Supplier, provenance, rollout, rollback, regression.
10	Testing / Validation	Have realistic scenarios been tested?	Simulation, HITL, adversarial cases, sim-to-real limits.
11	Safety Interface	Where does AI security meet safety?	Safety-case links, gaps, owners, exceptions.
12	Operating Environment	What world does the system assume?	Zones, routes, occupancy, weather, lighting, obstacles.

3. Evidence Shortlist

Area	Starter Evidence Prompt
Scope	System/version, deployment stage, operator role,

Area	Starter Evidence Prompt
	physical boundary, autonomy modes, physical consequence path.
Behavior	Task envelope, command path, override route, safe-state triggers, degraded-mode behavior, reset and return-to-service steps.
Assurance	Sensor tests, model/package identity, edge attestation, scenario validation, telemetry coverage, update regression evidence.
Operations	Incident playbooks, operator training, maintenance state, environment-change handling, supplier responsibilities, evidence custody.

4. Quick Red Flags

Red Flag	Why It Matters
Unknown command path	AI-influenced behavior may affect physical state, but the organization cannot explain where commands originate, transform, authorize, execute, or stop.
Untested degraded mode	There is no evidence for response to perception loss, model drift, communication loss, power loss, operator loss, or unsafe environment change.
Weak override	Emergency stop, human handoff, remote/local intervention, reset, or return-to-service controls are undocumented or cannot be demonstrated.
Telemetry gap	Logs cannot reconstruct sensor state, autonomy mode, command path, override, safety-interface event, physical effect, and recovery action.
Silent behavior-changing updates	Model, firmware, map, ruleset, controller, or vendor updates can alter behavior without approval, rollback, or regression evidence.

5. Notably Absent

Absent Claim	Clarification
No certification claim	This reference does not produce PAI-SF certification, conformance, compliance status, maturity rating, or public assurance language.
No scoring logic	It does not publish thresholds, weighting, pass/fail criteria, maturity levels, auditor procedures, controlled scenarios, or certification decision logic.
No regulatory approval	It is not a substitute for safety certification, medical-device approval, aviation approval, road authorization, building-code compliance, or legal review.
No complete audit request	It is a quick operator reference. Use the intake questionnaire, evidence request list, and controlled assessment materials for formal assessment planning.

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 artifact.