ODA3 INSTITUTE

SECTOR CALIBRATION PACKAGE

PAI-SF™ Smart Infrastructure and Physical AI Sector Guide

Physical AI Security Framework v1.0 — Sector Calibration Package

ODA3-2026-07-SCP-PAISF-016 | Public-Facing — Sector Calibration Package

Document Control

Doc ID	ODA3-2026-07-SCP-PAISF-016
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™ Smart Infrastructure and Physical AI Sector Guide

Physical AI Security Framework v1.0 — Sector Calibration Package

Sector Position

This guide calibrates PAI-SF™ v1.0 for smart infrastructure and other physical AI deployments where AI-enabled sensing, decision support, autonomy, or control logic may influence buildings, utilities, transportation systems, public spaces, campuses, facilities, or critical operational environments. It is sector guidance, not regulatory approval, building-code compliance, 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 smart buildings, smart-city systems, campuses, transport corridors, public venues, utility-facing automation, facility automation, physical security systems, intelligent traffic or mobility infrastructure, and distributed edge-AI systems where model behavior can affect physical operations. It is intended for infrastructure operators, CISOs, OT/security architects, facility owners, AI governance teams, compliance officers, and assurance teams preparing an initial PAI-SF scoping exercise.

Included	Use With Care	Out of Scope
AI-enabled infrastructure systems with physical sensing, automation, operator decision support, or actuator consequence.	Existing OT, facility, public-safety, emergency-management, and safety-case artifacts used as supporting evidence. Managed-service, integrator, and vendor-controlled systems where infrastructure owners may not directly control every update or model change.	Pure IT analytics, dashboards, or reporting systems with no credible effect on physical command, operating environment, or human safety. Replacement of infrastructure regulation, building code, utility approval, fire safety, public safety, or operational authorization.

Included	Use With Care	Out of Scope
Security conditions that may affect public spaces, facility access, traffic flow, utilities, buildings, emergency routes, or operational continuity.		

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 smart infrastructure because they sit closest to distributed sensing, operator authority, physical commands, degraded operation, and public-facing consequence.

Cluster	Primary PAI-SF Controls	Sector Interpretation
Public-space sensing and environment	PAI-SF-SEN-001 to SEN-003; ENV-001 to ENV-003	Camera, lidar, access-control, traffic, occupancy, environmental, utility, and site sensors must be reviewed against lighting, weather, crowding, occlusion, sensor disagreement, and changing physical conditions.
Autonomy boundary and operator authority	PAI-SF-AUT-001 to AUT-004; HOV-001 to HOV-003	Automation scope, operator handoff, human override, municipal or facility command authority, emergency escalation, and cross-operator responsibilities must be explicit.
Physical actuation and safe-state behavior	PAI-SF-ACT-001 to ACT-003; SAF-001 to SAF-004; DEG-001	Traffic signals, barriers, gates, elevators, HVAC, power controls, water controls, lighting, alarms, and robotic subsystems require bounded commands and degraded-mode definitions.
Edge compute and update assurance	PAI-SF-ATT-001 to ATT-003; SUP-001 to SUP-003	Field controllers, edge AI nodes, gateways, model packages, firmware, dependencies, integrator components, and managed-service updates require provenance and staged rollout evidence.
Runtime monitoring and incident reconstruction	PAI-SF-TEL-001 to TEL-004; IRP-001 to IRP-003	Telemetry must preserve sensor state, autonomy mode, operator action, physical command, override, degradation, and recovery events across distributed infrastructure.
Safety interface and validation	PAI-SF-FSI-001 to FSI-004; TST-001 to TST-003	AI-security findings must be routed into facility safety, OT safety, emergency management, public-safety, maintenance, and validation processes without claiming code or regulatory approval.

3. Domain Calibration

This table translates the 12-domain PAI-SF architecture into smart-infrastructure review language. It does not change the canonical control catalogue.

No.	PAI-SF Domain	Smart Infrastructure / Physical AI Calibration
1	Sensor and Perception Integrity	Validate public-space, facility, transportation, utility, and environmental sensors against occlusion, lighting, weather, crowd density, calibration drift, spoofing, disagreement, and operating-site changes.
2	Actuator and Kinetic Command Safety	Treat commands to gates, barriers, locks, signals, elevators, HVAC, lighting, alarms, pumps, valves, energy controls, and mobile infrastructure assets as security-relevant physical commands.
3	Edge Hardware and Model Attestation	Verify field controllers, gateways, edge AI nodes, embedded devices, model packages, firmware, integrator images, and managed-service components that influence physical behavior.
4	Autonomy Boundaries	Define the permitted automation envelope for facility, traffic, energy, water, security, building, public-space, and emergency-management functions, including who may expand or suspend it.
5	Safe-State and Degraded-Mode Behavior	Specify fail-safe, fail-secure, manual, degraded, isolation, local-control, emergency-open, emergency-stop, and service-continuity modes for each physical subsystem.
6	Human Override and Intervention	Require clear operator override, emergency services interface, local manual control, supervisory approval, reset criteria, and post-intervention accountability.
7	Runtime Monitoring and Telemetry	Collect tamper-evident records of sensor confidence, autonomy mode, operator actions, physical commands, safety interlocks, degraded states, overrides, and incident timelines.
8	Incident Response and Physical Recovery	Prepare procedures for isolating affected infrastructure, preserving evidence, coordinating operators, restoring manual control, validating physical recovery, and handling public-safety impact.

No.	PAI-SF Domain	Smart Infrastructure / Physical AI Calibration
9	Supply Chain and Update Assurance	Control vendors, integrators, OT suppliers, cloud/edge services, firmware, model, ruleset, and maintenance-update paths with staged rollout and rollback evidence.
10	Simulation, Testing, and Validation	Use digital twins where available, lab validation, site acceptance tests, tabletop exercises, degraded-mode drills, replay testing, and physical-world scenario validation.
11	Functional Safety Interface	Map AI-security findings into applicable OT safety, building safety, utility safety, public-safety, emergency-management, and maintenance processes without claiming compliance equivalence.
12	Physical Operating Environment	Maintain an up-to-date account of roads, buildings, utility assets, public spaces, weather, occupancy, emergency routes, maintenance zones, and dependency relationships.

4. Starter Evidence Pack

A first-pass review should collect enough evidence to determine whether the infrastructure 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 site scope	Inventory of infrastructure assets, AI-enabled functions, physical commands, operating sites, public-space exposure, operator roles, emergency dependencies, and subsystem boundaries.
Sensor and environment evidence	Sensor map, calibration records, physical environment assumptions, known blind spots, sensor-disagreement handling, and adverse-condition test results.
Command and safe-state evidence	Physical command paths, interlock design, command bounds, manual-control procedures, degraded-mode playbooks, emergency-control paths, and reset criteria.
Telemetry and response evidence	Event-log map, telemetry retention, operator-action logs, incident reconstruction procedure, evidence custody, physical recovery process, and cross-operator escalation contacts.
Supplier and update evidence	Vendor and integrator list, edge-device provenance, firmware/model/update records, maintenance windows, rollback process, and third-party service dependencies.
Validation and safety-interface evidence	Site acceptance testing, simulated or replay scenarios, emergency drills, safety-case linkages, unresolved AI-

Evidence Area	Examples to Collect
	security gap register, and responsible owner for each gap.

5. Integration Notes

PAI-SF should be applied beside OT cybersecurity, physical security, facility safety, public-safety coordination, emergency management, maintenance, privacy governance, and sector-specific operational-risk practices. For this sector, existing infrastructure artifacts may support evidence about operating limits, emergency procedures, asset dependencies, vendor responsibilities, and recovery processes. PAI-SF's role is narrower: it asks whether AI-specific sensing, inference, autonomy, command, update, telemetry, and recovery conditions are adequately assured where conventional infrastructure processes may not fully address learned, adaptive, or remotely updated behavior.

Boundary Discipline: A safety case, building-management procedure, OT cybersecurity review, service contract, maintenance record, or emergency plan 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, autonomy boundary changes, operator handoff, physical command compromise, telemetry gaps, supplier updates, incident reconstruction, and return-to-service risks are addressed.

6. Notably Absent

Absent Claim	Clarification
No critical-infrastructure approval claim	This guide does not establish approval by a regulator, authority, municipality, utility commission, emergency-services body, or infrastructure owner.
No building-code or safety-code compliance claim	The guide does not certify compliance with building codes, fire codes, electrical rules, industrial safety rules, public-safety obligations, or sector-specific regulations.
No replacement for OT and safety engineering	Existing OT cybersecurity, functional safety, physical security, emergency management, maintenance, and operational-risk 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 infrastructure model	Smart cities, campuses, hospitals, airports, factories, transport corridors, utilities, buildings, and public venues 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, regulatory submission, and certification language remain outside this guide and should

be handled through the controlled assessment and conformance-documentation set when authorized.