

ODA3 INSTITUTE

JSON SCHEMA PACKAGE

PAI-SF™ JSON Schema Notes

Physical AI Security Framework v1.0 — Machine-Readable Assessment Record
Schema

ODA3-2026-07-JSC-PAISF-025 | Public-Facing — Machine-Readable Schema Package

© ODA3 Pvt Ltd

Document Control

Doc ID	ODA3-2026-07-JSC-PAISF-025
Doc Type	JSON Schema Package (Documentation Note)
Framework Tag	PAI-SF™ v1.0
Companion Document	ODA3-2026-07-CAT-PAISF-006; ODA3-2026-07-CRT-PAISF-023; ODA3-2026-07-AMD-PAISF-022
Governing Licence	GAISSF Ecosystem Licence (GEL v1.0)
Access Classification	Open / Public — schema and example structure only; no scoring, certification, or assessor-calibration logic disclosed
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 — Machine-Readable Schema Package

PAI-SF™ JSON Schema Notes

Physical AI Security Framework v1.0 — Machine-Readable Assessment Record Schema

Purpose

This package provides a machine-readable schema for PAI-SF™ v1.0 assessment-support records. It is documentation for the schema, not the schema itself — the actual machine-readable artifacts are distributed alongside this note, unchanged.

This schema exists to make one thing checkable in structured form: whether a recorded assessment actually demonstrates **Kinetic Zero Trust** — PAI-SF's core assurance principle that AI-generated physical actions are validated against independent safety boundaries, not trusted on model confidence alone. The ``evidence_summary``, ``materiality``, and ``limitations`` fields on each domain record exist to capture that evidence in a form that can be queried and compared across assessments, not just read.

Included Files

- ``ODA3-2026-07-JSC-PAISF-025_PAI-SF-Assessment-Record-Schema-v1.0.schema.json`` — the JSON Schema (Draft 2020-12) defining the record structure. Verified: all 41 control IDs referenced in the schema's enum match the canonical PAI-SF control register exactly, with zero omissions or fabrications.
- ``ODA3-2026-07-JSC-PAISF-025_PAI-SF-Assessment-Record-Example-v1.0.json`` — a worked example instance. Verified: validates against every rule in the schema (required fields, type constraints, enum values, and field-length bounds), and its domain/control pairings are semantically correct (e.g., Domain 1's record only cites SEN-family controls, Domain 7's only cites TEL-family controls).

Intended Use

- Record in-scope physical-AI system boundaries.
- Map materially engaged PAI-SF domains and controls.
- Track evidence basis, freshness, source type, findings, limitations, and Notably Absent items.
- Support internal, partner, or controlled assessment workflows.

Known Schema Limitation — Recommended for v1.1

The schema does not currently enforce that a ``domain_record`s `domain_id`` and ``domain_name`` refer to the same canonical domain, or that its ``control_ids`` actually belong to that domain — these are independent enum fields with no cross-field validation. The included example is correctly filled in throughout, but the schema itself would not reject a record that paired, for instance, ``domain_id`: "1"` with ``domain_name`: "Actuator and Kinetic Command Safety"` and TEL-family control IDs. Closing this gap (via JSON Schema conditional validation, e.g. ``if`/`then`` keyed on ``domain_id``) is recommended before this schema is relied upon for automated cross-organization record comparison, where a human reviewer catching a mismatched pairing by inspection can't be assumed.

Notably Absent

- No scoring weights.
- No certification thresholds.
- No pass/fail formula.
- No assessor calibration method.
- No controlled test-scenario library.
- No public compliance, approval, endorsement, or certification grant.
- No regulatory substitution.

The schema preserves the PAI-SF public/controlled boundary: it supports structured evidence records while keeping certification and assessor-only logic outside the machine-readable artifact. Individual assessment records created using this schema may themselves be classified ``public-assessment-support``, ``controlled-assessment-support``, or ``partner-controlled`` depending on their content — that classification is a property of each record instance, not of the schema package itself, which is public.