

ODA3 INSTITUTE

STANDARDS CROSSWALK

PAI-SF Standards Crosswalk

Physical AI Security Framework v1.0 — Standalone Crosswalk Publication

ODA3-2026-07-CSX-PAISF-011 | Public-Facing — Standards Crosswalk Publication

© ODA3 Pvt Ltd

Document Control

Doc ID	ODA3-2026-07-CSX-PAISF-011
Doc Type	Standards Crosswalk Publication
Framework Tag	PAI-SF™ v1.0
Governing Licence	GAISSF Ecosystem Licence (GEL v1.0)
Access Classification	Open / Public — standards-positioning reference; not a Controlled asset
Publication State	Public reference v1.0
Publish Date / Review Cycle	01 August 2026 (content finalized); publication date to be confirmed
Classification	Public-Facing — Standards Crosswalk Publication

PAI-SF Standards Crosswalk

Physical AI Security Framework v1.0 — Standalone Crosswalk Publication

Purpose: This document extracts and matures the standards-mapping content from the PAI-SF Technical + Compliance Report into a standalone reference for scoping, evidence planning, and standards-body discussion.

1. Interpretation Rule

PAI-SF is positioned as an AI-security assurance layer for systems where sensing, inference, autonomy, and actuation can create physical consequences, governed by the **Kinetic Zero Trust** principle: AI-generated physical actions are validated against independent safety boundaries rather than trusted on model confidence alone. The crosswalk below describes analytical relationships only. It does not convert PAI-SF into a substitute for functional safety, product safety, sector compliance, or formal conformity assessment.

Source Basis	Use in This Document
Primary source basis	ODA3-2026-07-TCR-PAISF-001, Section 13 standards-mapping table and regulatory crosswalk tags.
Derived source basis	ODA3-2026-07-NOR-PAISF-005 and ODA3-2026-07-CAT-PAISF-006 for the canonical 12-domain / 41-control PAI-SF structure.
Evidence tiering	Analytical relationships in this document are ODA3 interpretation unless separately sourced to a published standard or public ODA3 framework text.

2. Standards Relationship Matrix

The following matrix preserves the standards set identified in the TCR and restates each relationship in publication-ready form.

Standard / Framework	Primary External Concern	What PAI-SF Adds	Boundary
ISO/IEC 42001	AI management system governance	PAI-SF adds physical-AI risk specificity beneath AI governance, accountability, operational control, and management-system evidence.	Complementary; not a certification substitute
ISO/IEC 23894	AI risk management guidance	PAI-SF extends AI risk identification and treatment with sensor, actuator, autonomy-boundary, degraded-mode, and physical-recovery controls.	Complementary risk-detail layer
NIST AI RMF	Govern / Map / Measure / Manage functions	PAI-SF provides physical-AI control detail that can support mapping, measurement, and management of cyber-physical AI risks.	Functional alignment only
IEC 62443	Industrial automation and control-system security	PAI-SF references OT security concepts for zones, conduits, component trust, update assurance, telemetry integrity, and actuation-layer protection.	Security complement
ISO 26262	Automotive functional safety	PAI-SF identifies AI-specific security and drift-related gaps that deterministic fault models do not fully address.	Does not replace automotive safety engineering
ISO 21448 (SOTIF)	Safety of intended functionality	PAI-SF complements intended-functionality safety with runtime trust verification, autonomy boundary controls, and physical telemetry evidence.	Security-assurance complement
IEC 61508	Functional safety lifecycle / SIL concepts	PAI-SF interfaces with lifecycle and safety-integrity concepts while addressing learned-model drift and adversarial influence.	Does not assign SIL or certify safety
ISO 10218 / ISO/TS 15066	Robot and collaborative-robot safety	PAI-SF extends traditional robot-safety concerns into AI-driven perception, autonomy decisions, actuator command validation, and recovery evidence.	Robotics safety complement

3. PAI-SF Domain Relevance Map

This map helps practitioners decide which external standards conversations are most likely to intersect with each PAI-SF domain. It is directional, not exhaustive. Domain numbers below match the canonical structure in the Framework Standard and Control Catalogue.

Domain	Closest Standards Touchpoints	Reason for Relevance
D1 Sensor and Perception Integrity	ISO/IEC 23894; NIST AI RMF; ISO 21448	Perception failure, spoofing, blinding, and disagreement response.
D2 Actuator and Kinetic Command Safety	IEC 62443; ISO 10218 / ISO/TS 15066; ISO 26262	Command validation, motion/force bounds, and cyber-physical actuation integrity.
D3 Edge Hardware and Model Attestation	IEC 62443; ISO/IEC 42001	Edge trust, model provenance, hardware integrity, and deployment authorization.
D4 Autonomy Boundaries	NIST AI RMF; ISO/IEC 23894; ISO 21448	Autonomy-level authorization, ODD change control, and boundary enforcement.
D5 Safe-State and Degraded-Mode Behavior	IEC 61508; ISO 26262; ISO 21448	Safe-state triggers, degradation behavior, and recovery from unsafe confidence states.
D6 Human Override and Intervention	ISO 10218 / ISO/TS 15066; IEC 61508; ISO 21448	Human authority, emergency stop, intervention channels, and fallback accountability.
D7 Runtime Monitoring and Telemetry	NIST AI RMF; IEC 62443; ISO/IEC 42001	Runtime evidence, independent telemetry, and monitoring for physical consequence pathways.
D8 Incident Response and Physical Recovery	NIST AI RMF; ISO/IEC 42001; IEC 62443	Containment, forensic preservation, physical recovery, and return-to-service evidence.
D9 Supply Chain and Update Assurance	IEC 62443; ISO/IEC 42001; ISO/IEC 23894	Hardware, firmware, model, and update assurance for physical-AI systems.
D10 Simulation, Testing, and Validation	ISO/IEC 23894; NIST AI RMF; ISO 21448; ISO 10218 / ISO/TS 15066	Scenario testing, HIL/SIL, validation evidence, and environment-specific assurance.
D11 Functional Safety Interface	IEC 61508; ISO 26262; ISO 21448	Explicit boundary between AI-security assurance and established functional-safety practice.
D12 Physical Operating Environment	ISO 10218 / ISO/TS 15066; ISO 21448; IEC 61508	Operating-design assumptions, human proximity, and environment-change response.

4. Practical Use

Use Case	Recommended Treatment
Governance scoping	Use the standards matrix to identify which external regimes are relevant to a physical-AI assurance

Use Case	Recommended Treatment
	discussion.
Evidence planning	Use the domain map to decide which PAI-SF controls may generate evidence useful beside AI management, OT security, functional safety, robotics safety, or automotive safety work.
Gap communication	Use the relationship notes to explain where PAI-SF adds AI-security assurance detail rather than replacing established standards.
Future crosswalk work	Use this publication as the parent reference for deeper clause-by-clause crosswalks, once source standards and licensing constraints are reviewed.

5. Notably Absent

The following absences are part of the release record and should remain visible wherever this crosswalk is cited.

Absent Claim	Clarification
Clause-level equivalence	This document does not claim that PAI-SF controls satisfy any clause, requirement, annex, SIL, ASIL, or conformity-assessment obligation in the listed standards.
Regulatory recognition	No regulator, standards body, or certification body recognition is claimed.
Functional safety certification	PAI-SF does not replace functional safety standards, product safety standards, sector safety cases, or independent safety certification.
Implementation sufficiency	Use of this crosswalk does not by itself establish adequate implementation, assurance maturity, commercial delivery authorization, or certification readiness.

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

6. Follow-On Crosswalk Work

Future publications may develop clause-by-clause or control-by-control mappings for specific standards, sectors, or regulator-facing submissions. Those mappings should be separately numbered, source-reviewed, and labelled according to their evidence basis. This document should remain the parent standards-positioning reference unless the PAI-SF standard itself changes.

Release Discipline: A later detailed mapping should not remove the caveats in this publication unless the relevant external standard has been directly reviewed and the mapping has been independently checked.