ONEDGE ENERGY

Threat → Mitigation Coverage Matrix

THREATMTX-1.0.0

Normative; under STANDARD axis S-0.0.4

Issuer:	IKKUNA SpA (StandardCo)
Document Type:	Normative threat coverage matrix
Version:	THREATMTX-1.0.0
Parent:	S-0.0.4
Status:	Initial coverage table
Intended Audience:	SDK implementers, auditors, regulators, lender diligence teams
Date:	May 18, 2026

1. Purpose and Status

The v0.0.2 whitepaper enumerates seventeen distinct threats but does not bind each threat to a specific mitigation in the technical, cryptographic, or governance surface. This document closes that gap. For each enumerated threat THREATMTX-1.0.0 specifies the canonical mitigation, the artifact in which the mitigation is defined, and the residual risk that remains after the mitigation is applied.

THREATMTX-1.0.0 is normative for conformance assessment. RFC 2119 / RFC 8174 conventions apply to the residual-risk column where requirements are stated.

2. Mitigation Surface Abbreviations

Tag	Surface
PT-τ	Provenance Tier criterion (Hardening Note v0.0.3 §4; $\tau \in \{0, 1, 2, 3, 4\}$)
PRED-T	Parametric predicate $P_T(y_k)$ requirement (Hardening Note v0.0.3 §5)
SDK-In	SDK Security Invariant I1–I7 (SECURITY_MODEL.md I-1.0)
GRS-RULE-k	GRSCHEMA-1.0.0 consistency rule k (§9 of the schema)
GRS-ERR	GRSCHEMA-1.0.0 reason code (§8 of the schema)
TEE-Vk	TEEATTEST-1.0.0 verification step k (§5.2 of the attestation chain)
TEE-ARL	TEEATTEST-1.0.0 Authoritative Revocation List (§6)
OPR-CONT	Oracle-problem mitigation continuity invariant (Oracle paper §2)
ZK-π	ZK proof artifact π_k verification under P-1.0.0
ECME-CR	ECME specification consensus rule (cross-runtime canonicalization)
XAM-Ix	XAM protocol invariant (XAM.md I-1.0)
G-§n	Governance addendum §n (G-1.3.3)
G-SCHED-L	Addendum Schedule L
GOV-CHARTER	StandardCo charter (pending; tracked open item)

3. Coverage Matrix

The seventeen v0.0.2 threats are enumerated below in their original order. Each row lists the canonical mitigation set, the resulting forced Golden Record outcome (where applicable), and the residual risk.

Threat	Canonical mitigation	Forced σ_k	Residual risk
T01 Missing telemetry	The required component vanishes from required(y_k), so $\tau(y_k) = 0$ and PRED-T fails for any $T \geq 1$. Verifier emits ERR_TELEMETRY_MISSING.	Opacity	Loss of certifiability for the affected event; no false-positive risk.
T02 Corrupted telemetry	GRS-RULE-1 (tier-predicate) plus GRS-ERR ERR_CODEC_INVALID for malformed bytes; if syntactically valid but cryptographically corrupt, TEE-V7 (telemetry signature) fails with ERR_TEE_TELEM_BAD_SIG.	Opacity	Persistent corruption pattern MUST trigger Min-Cut Intervention Plan under G-SCHED-C.8.

Threat	Canonical mitigation	`Forced` σ_k	Residual risk
T03 Inconsistent BMS / SCADA / meter values	Provenance-tier stratification: SCADA-relayed values without silicon root are at most $\tau = 2$; BMS-TEE-signed values are $\tau = 3$. Inconsistencies between tier-2 and tier-3 channels for the same physical quantity downgrade $\tau(y_k)$ to the minimum and emit `ERR_GR_TELEMETRY_ORDER` or `ERR_TEE_TIER_DOWNGRADED`.	`Opacity or Breach (if envelope clearly violated under tier-3 root)`	Operator may strategically withhold silicon-rooted channels; mitigated by Tier-4 ZK continuity if enabled.
T04 Unverified data origin	TEE-V1 / V2 (chain registration + signature verification) reject any entry whose Layer-1 or Layer-2 cert is unregistered; `ERR_TEE_L1_UNREGISTERED` or `ERR_TEE_L2_BAD_SIG`.	`Opacity`	A compromised OEM root could mint apparently valid certs; mitigated by TEE-ARL and Requirement R5 (rotation).
T05 Unexplained data gaps	Per-channel freshness window (TEEAT-TEST §5.1). Sample outside window triggers `ERR_TELEMETRY_STALE`. Gap is recorded as Opacity (no false-positive certification).	`Opacity`	Repeated gaps without proximate cause trigger Min-Cut Intervention Plan (G-SCHED-C.8).
T06 Sensor drift beyond tolerance	Detected by the Tier-4 continuity invariant OPR-CONT inside ZK-π. Drift outside ϵ_{sensor} produces `ERR_TEE_CONTINUITY_FAIL`.	`Opacity for Level-4 statements; not detected at Levels 1-3`	Level-3 statements remain blind to slow drift; mitigation requires Level-4 deployment or scheduled OEM calibration audit.
T07 Delayed or non-sequenced telemetry	GRS-RULE: telemetry vector MUST be sorted ascending by $(channel\_id, sample\_h)$. Violation: `ERR_GR_TELEMETRY_ORDER`. Late samples outside freshness window: `ERR_TELEMETRY_STALE`.	`Opacity`	A reorganized chain could cause legitimate samples to fall outside the window; mitigated by adequate Δ_{fresh} sizing.
T08 Manipulated sensor feeds	Defense in depth: TEE-V7 catches non-silicon-signed manipulation; OPR-CONT catches physics-violating manipulation; envelope evaluation catches policy-violating commands.	`Opacity (if signature broken) or Breach (if signed but envelope violated)`	Manipulation inside the BMS-TEE silicon enclave is the residual physical-bypass risk; not mitigated by software.

Threat	Canonical mitigation	`Forced` σ_k	Residual risk
T09 Data replay	TEEATTEST §5.1 freshness anchors (block-height and/or VDF); SDK-I5 (XAM replay-protection invariant) for cross-runtime messaging; GRS-RULE-4 (parent-hash) for event-level replay.	`Opacity`	Replay within freshness window remains possible; bounded by Δ_{fresh}.
T10 Unauthorized schema modification	SDK-I6 (upgrade-authorization invariant) + threshold-signature gating; GRS-RULE: `manifest_root` mismatch triggers `ERR_GR_MANIFEST_ROOT_STALE`; CRYPTO-DOMAINS rule that label changes are consensus-breaking.	`Verifier rejects entire block`	Compromise of the upgrade-signing threshold; mitigated by GOV-CHARTER threshold policy (pending).
T11 Model drift	FINGERPRINT BASELINE registration: θ_a is hashed and revocable; drift between deployed θ and registered θ_a triggers `ERR_GR_FB_MISMATCH` or `ERR_FB_REVOKED`. `fb_hash` is committed inside GOLDEN RECORD.	`Opacity / Breach`	New FINGERPRINT BASELINE versions require StandardCo approval; uncontrolled fork = compliance disqualification.
T12 False curtailment claims	Candidate Extension (whitepaper §15) classifies curtailment-provenance events against authorized system / settlement / metering records; without those records, the claim is Opacity by construction.	`Opacity`	Settlement-record authority remains external; ONEDGE ENERGY does not adjudicate the records.
T13 False compliance claims	Three independent layers: silicon-rooted signing (TEE-V7), continuity (OPR-CONT), envelope evaluation. False compliance requires breaking at least one cryptographic primitive.	`Breach or Opacity`	Concerted multi-OEM compromise of Layer-1 keys; mitigated by Layer-0 audit cadence.
T14 False breach accusations	A Breach classification requires $P_T(y_k) = 1$ AND $E(x_k, u_k; \theta) = 0$ with non-zero `breach_mask`; the proof artifact π_k binds the inputs cryptographically. Fabricating a breach requires forging a Tier-T telemetry signature.	`--`	Compromise of silicon signing key; mitigated by TEE-ARL and Requirement R4.

Threat	Canonical mitigation	`Forced` σ_k	Residual risk
T15 OEM data asymmetry	G-SCHED-C antitrust-safe conduct: StandardCo maintains the Fingerprint Baseline registry and the certificate chain; MarketCo cannot use exclusive arrangements to block OEM access to StandardCo channels (G-§7.4 anti-blocking). StandardCo data and outputs (StandardCo reserved rights) preclude OEM-side capture.	`--` `(governance threat)`	Antitrust-incompatible conduct caught only by quarterly C.2 reporting; depends on G-SCHED-C reporting discipline.
T16 Operator misreporting	Tier downgrade: any operator-rooted signature is at most $\tau = 1$; for any Level-$\ell \geq 2$ statement the operator's report cannot satisfy PRED-T.	`Opacity`	Operator collusion with downstream verifier; mitigated by independent reference validator.
T17 Dispatch-envelope mismatch	The envelope predicate $E(x_k, u_k; \theta) = 0$ produces a Breach classification with a specific `breach_mask`; the symmetric design protects both owner and OEM.	`Breach`	Envelope-evolution disputes resolved via G-§6B (Certification Use) + Schedule A acceptance criteria.
T18 "Opacity treated as Compliance"	GRS-RULE-1, GRS-RULE-2: the classification table forces $\sigma_k = 0$ (Opacity) whenever $P_T(y_k) = 0$; `ERR_GR_SIGMA_INCONSISTENT` rejects any record that attempts to assert $\sigma_k = 1$ under $P_T(y_k) = 0$.	`Opacity`	— (structurally prevented in the schema).
T19 Commercial misrepresentation	G-§§2C.1, 2C.2, 7A (Public Claims Protocol); MarketCo / JAXIAV may not claim StandardCo attribution without IKKUNA's written approval.	`--` `(governance threat)`	Enforcement via material-breach mechanics (G-§7C); detection via G-SCHED-F audit.

4. Coverage Summary

Mitigation surface	Threats covered	Count
Provenance Tiers + parametric predicate	T01, T03, T04, T08, T11, T16	6
GRSCHEMA-1.0.0 consistency rules	T02, T07, T10, T18	4
TEEATTEST-1.0.0 chain	T03, T04, T05, T07, T08, T13, T14	7
Oracle-problem continuity (Level 4)	T06, T08, T13	3
SDK Security Invariants	T09, T10	2
Fingerprint Baseline registration	T11	1
External authority deference	T12	1
Governance addendum + Schedules	T15, T17, T19	3
StandardCo charter (pending)	T10 (threshold policy), T15 (governance)	2 (partial)

A single threat MAY be covered by multiple surfaces (defense in depth). The intent is that every threat has *at least one* forced rejection path that the verifier can demonstrate with a specific reason code or a specific governance-channel obligation.

5. Open Items

The following items are tracked as open until a future release:

1. Numerical calibration of ϵ_{sensor} for the Tier-4 continuity test against at least one OEM reference asset (Tesla Megapack, LG ESS, Sungrow, CATL EnerC+).
2. Handling of legitimate physical discontinuities (breaker trips, BMS reinit, ambient step transients) so that they do not produce spurious Opacity events at Level 4.
3. Publication of the StandardCo charter (GOV-CHARTER), which is referenced by mitigations for T10 and T15.
4. Mapping each Schedule C reporting obligation to a per-threat audit cadence.

Disclaimer

This document is a normative threat-coverage matrix prepared by IKKUNA SpA. It does not constitute legal, financial, investment, regulatory, engineering, tax, or professional advice. ONEDGE ENERGY remains a proposed open standard and candidate specification in pre-TRL-7 validation status.