TESSURE · TECHNICAL WHITEPAPER

Fusion Architecture

A reference architecture for civilian-enterprise edge sensor fusion at fixed critical-infrastructure sites. Multi-modal detection, on-site processing, cryptographically signed evidence, overlay integration with the VMS and access-control systems you already run.

VERSION 0.1 TESSURE SYSTEMS, INC. APRIL 2026

1. Executive summary

Physical security at high-risk fixed sites — power substations, data-center campuses, pipelines, logistics yards, private estates — is drowning in false alarms. Industry studies place standalone motion and analytics false-positive rates at **94–99%**. Operators in GSOCs become desensitized. When real events arrive, they hide in the noise.

The category's response for the last decade has been "more AI video". That has failed: single-modality camera systems bottom out at ~85% accuracy on outdoor perimeters because rain, fog, wildlife, and shadows all defeat them. Adversaries defeat them by choosing conditions.

Tessure's bet is architectural: **fuse multiple sensor modalities at the edge, corroborate on-site, verify before alerting, package evidence cryptographically, and overlay the VMS the customer already owns.** This paper is the reference for how.

<5% False-positive rate after 30-day tune (design target)	**~30s** Detect → verify latency at the edge
24h Continuous offline operation during WAN loss	**$900** Fusion Node BOM at 100-unit scale

1.1 Who this paper is for

Security architects, VP Security roles, GSOC leads, IT/Sec integrators, insurance loss-control officers, and the investigator or regulator who has to audit a physical-security incident after the fact. It is technical but not ML-specialist; every non-obvious claim ties to a measurable outcome.

1.2 What this paper is not

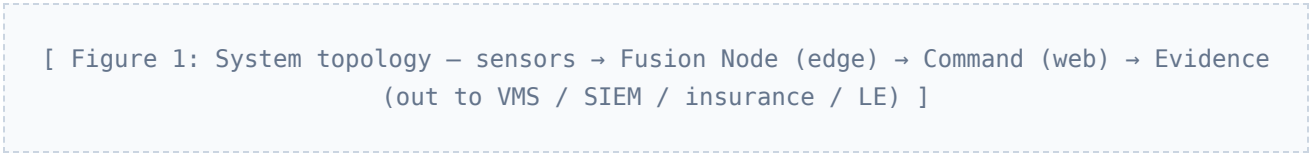
A marketing document, a defense-tech pitch, or a prescriptive VMS-replacement plan. Tessure is an overlay on existing infrastructure, not a rip-and-replace. See §6 for the integration surface.

2. System overview

Three things compose the Tessure platform:

1. **Fusion Node** — a ruggedized edge appliance installed at the site. Does all perception, fusion, verification, and signing. 24-hour offline autonomy.
2. **Tessure Command** — a thin operator UI. Surfaces only verified events. No raw video streaming by default.
3. **Tessure Evidence** — the pipeline that hashes, signs, and ships events downstream. Insurance-grade audit trail.

Optional: Tessure Cloud Assist for fleet management, cross-site aggregation, and model distribution. Edge-first means Cloud Assist is additive, not required.



2.1 What the Fusion Node does locally

- Ingests video (ONVIF / RTSP / SRT / USB), thermal (GigE-Vision), radar (vendor SDK), acoustic (MQTT / UDP), and optional RF spectrum.
- Runs perception models on GPU (object detection, thermal classification, radar tracking, acoustic classification).
- Aligns detections across modalities in a shared spatiotemporal frame.
- Runs the fusion engine (§4) to produce verified events.
- Packages, hashes, and signs evidence.
- Queues events locally during WAN outage; flushes on recovery.

2.2 What stays off-edge

Identity recognition (face, plate) is **opt-in per site** and disabled by default. Raw sensor streams do not leave the site. Cloud Assist receives only signed event metadata and, if explicitly enabled, redacted artifacts for fleet-wide analytics.

3. Fusion Node — hardware reference

Dual-sourced compute so supply volatility does not stall deployment.

COMPONENT	PRIMARY	FALLBACK
Compute	NVIDIA Jetson Orin NX 16GB (100 TOPS)	Hailo-8L + Intel N100 x86 mini-PC
Storage	512 GB NVMe + 64 GB eMMC	—
Network	2× GbE + 4× PoE+	+ LTE modem option
Wireless	Wi-Fi 6	—
Enclosure	IP54 indoor / IP67 outdoor (same PCB)	—
Power	12–48 V DC, 40 W typical, 80 W peak	PoE++ compatible
Cooling	Passive heatsink, fanless	—
Security	TPM-anchored crypto, tamper switch, signed boot	—

Target BOM: **$900 at 100-unit scale, $600 at 1,000-unit scale.** Hardware is shipped included as part of the SaaS tier and refreshed every four years.

3.1 Sensor inputs supported

MODALITY	PROTOCOL / INTERFACE	COUNTS PER NODE
Video (RGB)	ONVIF · RTSP · SRT · USB	4 (Small), 16 (Mid), 64 (Large distributed)
Thermal	ONVIF · GigE-Vision	1–4
Radar (ground + perimeter)	Echodyne, SpotterRF, TI mmWave	1–4
Acoustic	MQTT · UDP	1–8 (shot / glass / rotor)
RF spectrum (counter-UAS)	Aaronia SDR · Dedrone feed	0–1
Access control	Genetec SDK, Lenel OnGuard, CCURE 9000	event stream
SCADA / BMS	Modbus · BACnet · syslog	optional
Cyber events	Splunk · Elastic · Sentinel webhook	optional

4. Fusion engine

The differentiated core. Input: detection events from each modality. Output: **Fused Event** objects with confidence scores and evidence references.

4.1 Perception stack (edge, per-modality)

Video pre-processing	NVIDIA DeepStream / GStreamer
Object detection (video)	YOLO v11 + Grounding DINO for zero-shot refinement
Segmentation refinement	SAM 2 on detection hits
Thermal classifier	MobileNetV3 trained on thermal-persons + FLIR public sets
Radar processing	Vendor SDK + Kalman tracks + Doppler signature DB
Acoustic classifier	YAMNet + domain-adapted head
Face / plate redaction	RetinaFace + blur pipeline (on by default)

4.2 Fusion decision model

1. **Temporal clustering.** Detections within a rolling 3-second window at the same geo-cell are grouped into a Candidate Event.
2. **Spatial corroboration.** 2D detections project to a shared 3D site map via per-sensor calibration. Multi-modality hit in the same 1 m³ cell scores higher.
3. **Modality corroboration.** Separate confidence scores per modality combine via learned Bayesian weighting (tuned on per-site data during pilot).
4. **Signature matching.** Optional class-level signature DB (wildlife thermal profile, vehicle ALPR, drone RF).
5. **Policy playbook lookup.** Event classification → customer-configured response (log only / notify / dispatch / auto-action with operator approval).

4.3 Fused Event schema

```
{
  "event_id": "ev_abc123",
  "site_id": "site_xyz",
  "timestamp": "2026-04-14T02:47:13Z",
  "classification": "human_intruder",
  "confidence": 0.94,
  "corroborating_modalities": ["video_ptz_07", "radar_01", "thermal_02"],
  "geo_cell": "grid:12-07",
  "evidence_refs": ["clip_abc123_01.mp4", "radar_track_01.json",
"thermal_02.tiff"],
  "evidence_hash": "sha256:...",
  "proposed_response": "notify_operator + drone_dispatch",
  "auto_actions_taken": ["perimeter_lights_sector_3"],
  "requires_approval": ["drone_dispatch", "le_notify"]
}
```

4.4 Fusion weighting: Bayesian first, end-to-end only if it beats it

Start with interpretable Bayesian weighting tuned on site-specific data during the 30-day pilot. Add an end-to-end learned fusion head only when it beats the Bayesian model on held-out events across multiple sites. Interpretability is a brand-aligned property: customers and regulators can inspect the decision for any given event.

5. Evidence pipeline

Every confirmed event produces an **Evidence Package**. This is load-bearing for insurance ROI and a significant competitive moat versus camera-only products.

5.1 What's in a package

- Raw clips with redaction baked in — 30-second pre-roll + full event duration.
- Radar tracks (JSON).
- Thermal frame captures.
- Environmental telemetry.
- Acoustic recordings.
- Fusion decision log (why this event was classified).
- Operator actions (who approved what, when).

5.2 Chain of custody

- SHA-256 hash of each artifact.
- Root hash aggregated into a Merkle tree per event.
- Signed with site-specific Tessure key rooted in a per-customer Tessure signing authority.
- Stored locally (edge) + replicated to customer-chosen cloud (Tessure Cloud, customer S3, Azure Blob, GCS).
- Exportable as a signed PDF report for insurance, legal, and law enforcement.

> WHY THIS MATTERS
>
> Single-modality camera systems produce footage. That is not evidence. Insurance underwriters, civil courts, and the police all require provenance, integrity, and chain of custody. Tessure ships evidence as a first-class product, not as an afterthought.

5.3 Five-stage pipeline

1. **Event** — sensor detection.
2. **Fuse** — cross-modality corroboration.
3. **Verify** — confidence score × policy playbook.
4. **Sign** — SHA-256 × Merkle × site key.
5. **Deliver** — VMS, SIEM, dispatch, insurance, LE.

6. Integration surface

Tessure overlays existing infrastructure. The integrations shipped as managed connectors:

TARGET	DIRECTION	NOTES
Genetec Security Center	Event out → incident	SDK-based
Milestone XProtect	Event out → bookmark + metadata	MIP SDK
Lenel OnGuard	Access events in, event out	OpenAccess
CCURE 9000	Access events in, event out	REST
TAK / CoT	Event out → tactical picture	CoT XML, UDP multicast
Splunk / Elastic / Sentinel	Event out → SIEM	HTTP Event Collector
PagerDuty / Opsgenie	Critical event → page	Webhook
ServiceNow	Evidence → record	REST
Slack / Teams	Alerts	Webhook

7. Privacy architecture

Privacy is not a compliance tax. It is a product feature.

- **On-site processing.** Raw sensor data does not leave the facility.
- **Redaction by default.** Faces and license plates are blurred before any storage.
- **Opt-in identity recognition.** Facial and plate recognition are disabled by default; customers must affirmatively enable per site with legal review.
- **Per-state compliance modes.** Tessure CA / IL / NY / EU modes auto-configure per local law (CCPA, BIPA, GDPR, AI Act).
- **Redacted-by-default exports.** Evidence packages ship redacted; unredacted originals available only with authorized access and audit log entry.
- **Signed evidence, inspectable.** The chain of custody is auditable without exposing any raw data to Tessure or a third party.

A detailed *Privacy Posture Brief* is available as a companion document.

8. Resilience & edge autonomy

- **24-hour offline operation.** Full detect / verify / record during WAN loss.
- **Event queue.** Offline events queue locally; flush + hash-verify on WAN recovery.
- **Firmware rollback.** Dual-slot A/B updates; failed update auto-rollback within 30 seconds.
- **Sensor fault detection.** Missing or degraded sensor triggers operator notice within 60 seconds; fusion adapts by down-weighting that modality.
- **Hardware watchdog.** Resets Node on stall (rare; mitigates kernel-level ML issues).

9. Security architecture

- **Per-site key pair** enrolled via out-of-band hardware attestation (TPM).
- **mTLS everywhere.** Node ↔ Cloud and Node ↔ Command.
- **Zero-trust posture.** Nodes cannot initiate connections to Cloud except through a signed channel.
- **Supply-chain integrity.** Firmware images signed; boot-time attestation.
- **Quarterly third-party pen-testing** (Bishop Fox or NCC Group); public disclosure of resolved findings after 90 days.

10. Deployment

Standard install is target **< 4 hours per site** by Month 9 once the install kit is standardized.

1. Site walk — identify gaps in existing coverage; place radar and thermal where needed.
2. Node install — mount, power, network.
3. Sensor enroll — ONVIF discovery for existing cameras; radar and thermal direct-attach.
4. Calibration — per-sensor geometric calibration to the shared 3D site map.
5. 30-day tune — collect baseline false-positive events; fine-tune Bayesian fusion weights per site.
6. Playbook configuration — operator-approved actions, response thresholds.
7. VMS / SIEM connector enable.
8. Operator training — half-day.

11. What Tessure chooses not to do

- No cloud-primary pipeline. Edge-first or no feature.
- No proprietary camera tie-in. ONVIF / RTSP only; no Tessure cameras.
- No identity recognition by default. Opt-in per site, legal-reviewed.
- No kinetic response. No pursuit drones, no projectile systems. Notify + evidence + customer-owned response only.
- No autonomy above human-in-the-loop risk thresholds. Document and publish thresholds.

This document is version 0.1 and reflects the Tessure thesis as of April 2026. The concept is archived; the thesis is public. If you are building in this category, the architecture is free to take. — sean.florez@colorado.edu · github.com/fl-sean03/tessure