SKY SHADOW SYSTEMS

# AI-Enabled Offshore Security Monitoring

AI-enabled monitoring should prioritise review, surface uncertainty and support accountable decisions in offshore environments.

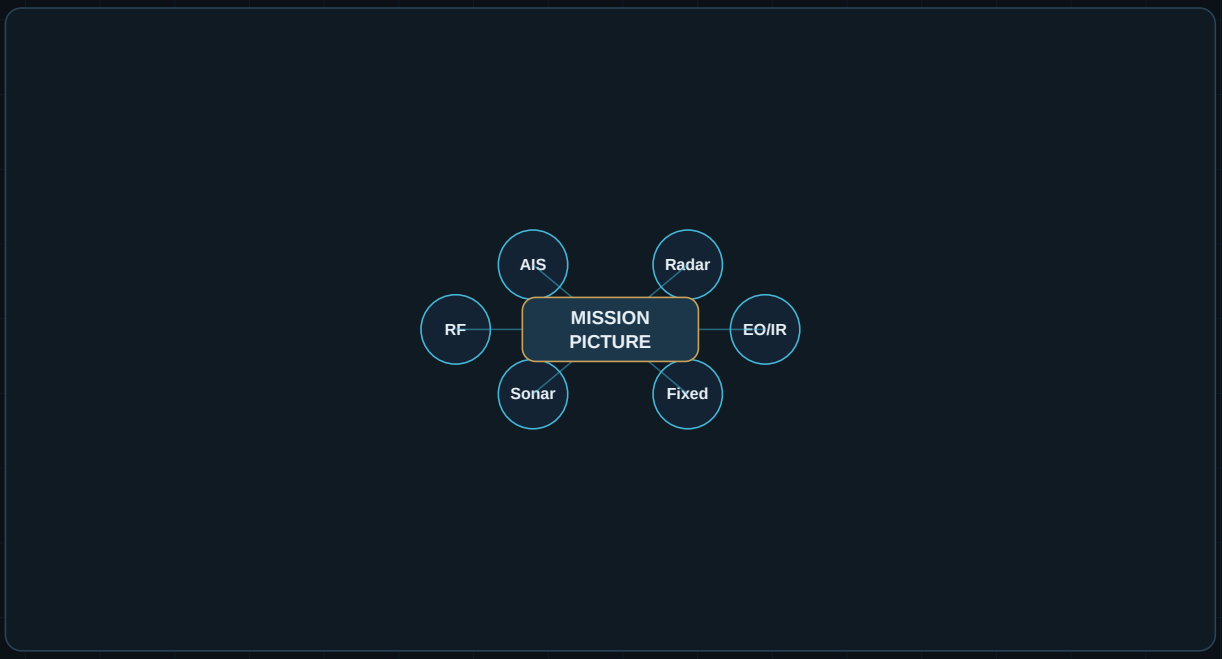
| | |
|---|---|
| Document type | Whitepaper |
| Audience | Investors, ports, offshore operators, infrastructure owners, integrators and approved public-sector stakeholders |
| Disclosure level | Public-level strategic material. Detailed specifications and deployment-sensitive information reserved for approved private review. |
| Version | Draft v1.0 - 29 May 2026 |

## Disclosure boundary

This document is intentionally written at public strategic and procurement level. It avoids controlled technical details, exact performance values, deployment-sensitive parameters, offensive capabilities, bypass methods, targeting instructions, and site-specific configuration data. The aim is to support investor and stakeholder understanding of system architecture, governance, pilot design and commercial positioning.

# Abstract

AI-enabled monitoring should prioritise review, surface uncertainty and support accountable decisions in offshore environments. The paper frames the issue as an architecture, governance and operator-workflow problem rather than a platform-only problem. It is intentionally public-safe and avoids detailed engineering parameters.




# Problem statement

Maritime and infrastructure operators increasingly face a signal-to-decision gap: sensors, public maritime data, platform feeds and human reports are available, but the operational value depends on how these inputs are fused, reviewed, prioritised and preserved as evidence.

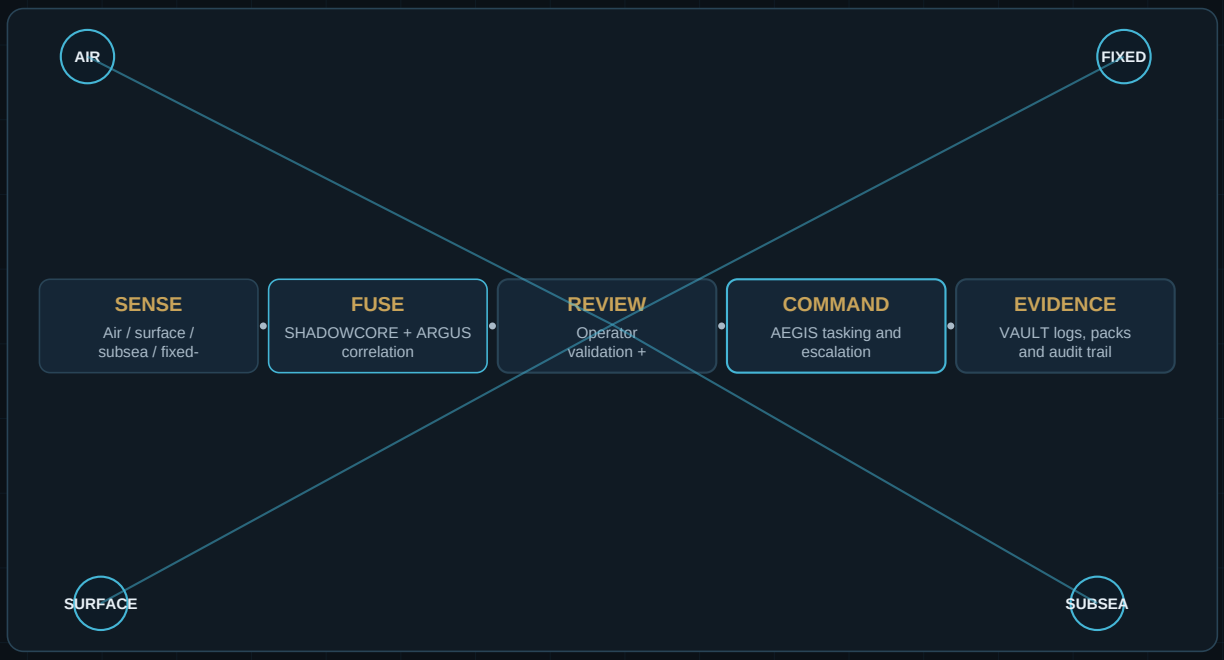
# System model

| Layer | Role | Design principle | Output |
|---|---|---|---|
| Collection | Gather authorised sensor, platform and contextual signals. | Domain-appropriate, bounded and auditable. | Raw observations and metadata. |
| Correlation | Associate events across sources and time windows. | Reduce fragmentation and false context. | Candidate events and confidence notes. |
| Review | Human operator evaluates relevance, ambiguity and actionability. | Human-commanded autonomy. | Validated event record. |
| Command | Route tasking, escalation and coordination. | Accountable authority and workflow clarity. | Task list and escalation log. |
| Evidence | Preserve records for briefing, audit and learning. | Structured, reviewable and retrievable. | Evidence pack and mission log. |

# Technical architecture themes

| | |
|---|---|
| **Multi-source ingestion**<br>Accept air, surface, subsea, fixed-site and external contextual data without binding the buyer to one platform. | **Confidence-aware review**<br>Present operators with confidence notes, source context and uncertainty rather than black-box declarations. |
| **Workflow separation**<br>Keep sensing, fusion, review, command and evidence as separate layers to improve governance. | **Pilot metrics**<br>Measure coverage, operator workload, event relevance, evidence quality and integration fit. |
| **Disclosure control**<br>Publish architecture and governance while keeping specifications, settings and deployment assumptions private. | **Scalable packaging**<br>Convert recurring use cases into repeatable pilot and deployment templates. |

# Operational model

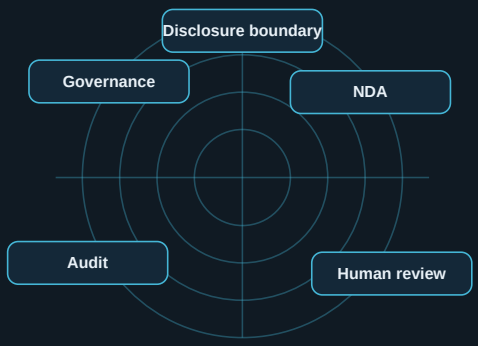



# Key performance indicators for evaluation

- Observation continuity within agreed zones.
- Time from event presentation to human review.
- Reduction in duplicate or irrelevant feeds presented to operators.
- Completeness of event records and audit trail.
- Operator confidence and workload ratings.
- Integration fit with existing reporting and escalation procedures.

# Investor implications

The investment value lies in repeatable mission packages, evidence-led pilots, private stakeholder relationships and software-supported workflows. The strongest near-term proof points are not extreme performance claims, but credible pilots, buyer engagement, validated reporting outputs and disciplined governance.



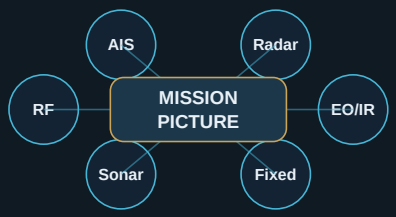

# Conclusion

Sky Shadow should continue to communicate at public strategic level while building private, evidence-rich technical packs for approved stakeholders. This supports credibility, protects sensitive detail and gives investors a cleaner route to assess maturity.

# Technical appendix A - mission data model

This technical appendix defines the public-safe information architecture used throughout the resource pack. It is suitable for investor and buyer understanding, but excludes implementation details, exact sensor settings, deployment parameters and controlled configuration data.

| Data class | Examples | Treatment | Business value |
|---|---|---|---|
| Observation metadata | Time, zone, source class, event identifier | Normalised into a reviewable event record. | Enables audit, search and comparison. |
| Sensor context | EO/IR, radar, AIS, RF, acoustic or fixed-site context | Stored as source context, not as a definitive conclusion. | Improves confidence and reduces false interpretation. |
| Operator review | Human assessment, confidence note, escalation decision | Preserved in VAULT as part of event history. | Supports accountability and stakeholder trust. |
| Mission output | Briefing pack, event log, anomaly register, summary report | Exported to approved users and governance channels. | Creates board-level and investor-visible evidence. |
| Disclosure control | NDA status, public/private classification, site sensitivity | Controls what can be reused publicly or commercially. | Protects customers and company IP. |



# Technical appendix B - system layer interfaces

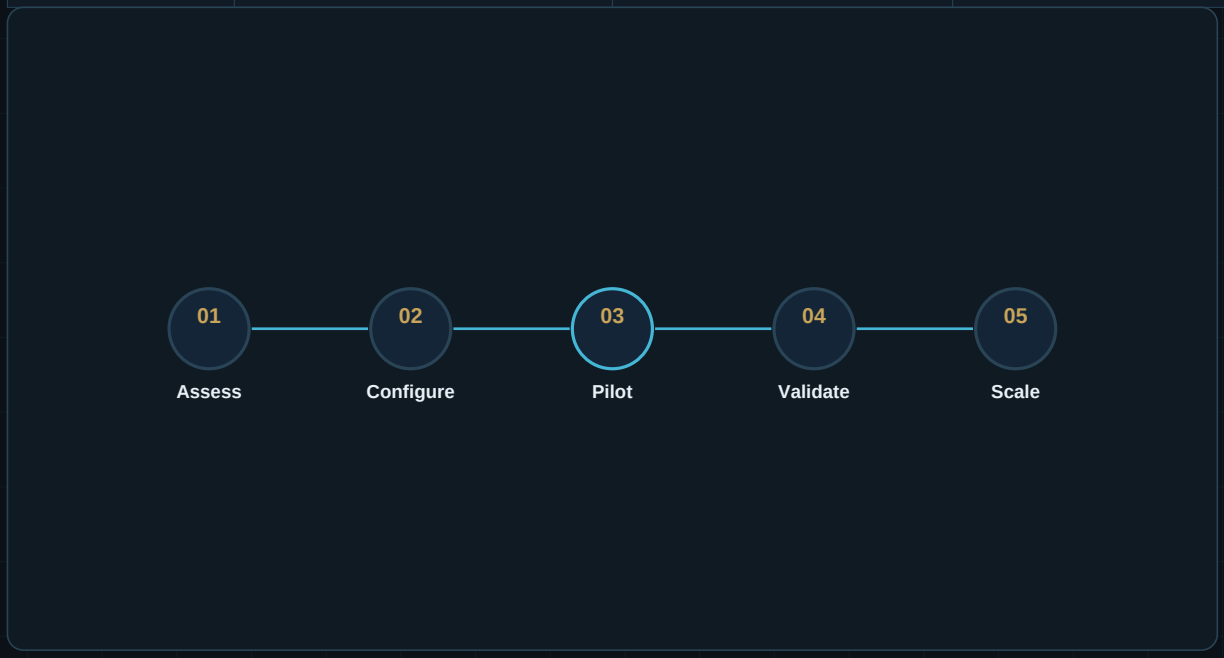
Sky Shadow should present itself as a modular mission architecture. Each layer can be explained as an interface boundary. This gives investors confidence that the company is building a repeatable system, not merely a collection of disconnected visual concepts.

| Interface boundary | Input | Processing posture | Output |
|---|---|---|---|
| Sensor to SHADOWCORE | Authorised observations and metadata | Prioritisation, anomaly triage and event shaping. | Candidate events with confidence context. |
| SHADOWCORE to ARGUS | Candidate events and source context | Cross-source correlation and duplicate reduction. | Composite operating picture. |
| ARGUS to AEGIS | Correlated events and uncertainty notes | Operator tasking, review and escalation workflow. | Human decision record and task queue. |
| AEGIS to VAULT | Reviewed events, decisions and notes | Evidence packaging, audit trail and reporting structure. | Briefing-ready records. |
| VAULT to stakeholder | Approved reports and logs | Controlled distribution and disclosure review. | Buyer, investor or governance evidence. |

# Technical appendix C - evaluation and assurance criteria

The most investor-attractive technical story is an evidence-led adoption model. A buyer should be able to test the mission system through metrics that demonstrate reduced uncertainty, improved review quality and repeatable operational value.

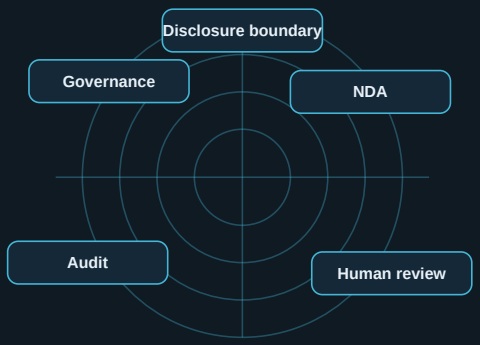
| Criterion | Measurement method | Evidence artifact | Investor signal |
|---|---|---|---|
| Coverage fit | Compare planned zones with reviewed observation windows. | Coverage map and gap note. | Shows practical utility. |
| Signal relevance | Measure useful events versus irrelevant raw inputs. | Event relevance dashboard. | Shows operator-value, not feed volume. |
| Review latency | Measure time from event surfacing to human review. | Workflow timing log. | Shows process efficiency. |
| Evidence integrity | Check completeness of logs and event traceability. | VAULT evidence sample. | Shows governance readiness. |
| Integration fit | Assess fit with existing security operations. | Integration review note. | Shows procurement pathway. |
| Repeatability | Compare whether same template can apply to another site. | Repeatable mission template. | Shows scalability. |



# Technical appendix D - governance and risk controls

For a defence-adjacent and infrastructure-focused company, credibility depends on disciplined public disclosure. The documents should create confidence without disclosing parameters that could create operational risk or regulatory issues.

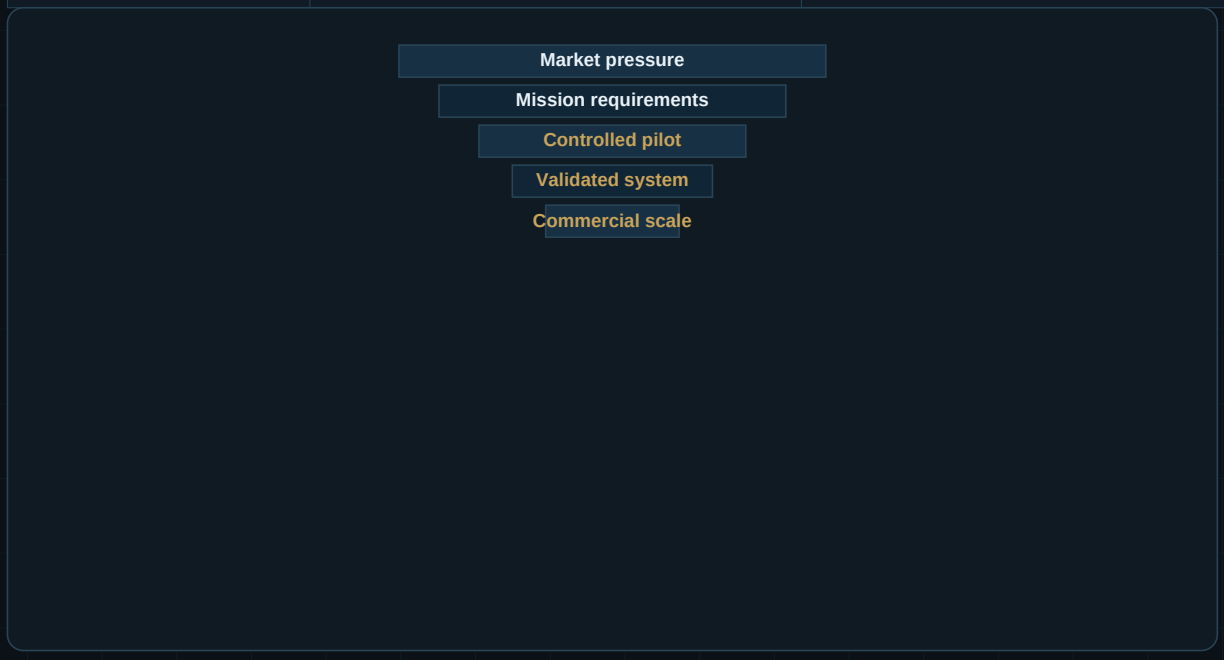
| | |
|---|---|
| **Public-safe architecture**<br>Describe system layers, buyer value and governance without exact technical settings. | **NDA technical review**<br>Route deeper technical discussions through private briefing and controlled diligence. |
| **Human authority**<br>Present autonomy as operator-supporting and human-commanded for sensitive contexts. | **Evidence integrity**<br>Use audit trails, logs and review histories as a core value proposition. |
| **Compliance posture**<br>Keep export-control, data protection and sector-specific review in the buyer process. | **Claim discipline**<br>Avoid unverified performance, customer, funding, contract or deployment claims. |



# Technical appendix E - investor conversion logic

The resource library should help a serious investor quickly understand the company as an architecture-led mission-systems venture. The best conversion pathway is from public credibility to controlled private review, then from private review to pilot design, stakeholder proof and commercial scale.

| Website asset | Investor purpose | What it should trigger |
|---|---|---|
| Capability statement | Quick credibility and scope assessment. | Private briefing request. |
| Whitepapers | Demonstrates doctrine, depth and market understanding. | Technical discussion under NDA. |
| Pilot programme brief | Shows practical route to validation. | Pilot scoping call. |
| Investor overview | Explains commercial thesis and roadmap. | Qualified investor diligence. |
| Case-style pilot report | Future proof artifact after approved trials. | Funding, partnership or customer conversion. |



# References and source basis

The documents use Sky Shadow public website content and public strategic references. Market figures are indicative third-party estimates and should be validated before investor use.


- Sky Shadow Systems website scan, 29 May 2026: homepage describes persistent maritime awareness, human-commanded autonomy and evidence-ready decisions.

- Sky Shadow Technology page: describes sensors, SHADOWCORE, ARGUS, AEGIS and VAULT as the public mission architecture.

- NATO Alliance Maritime Strategy, 29 Oct 2025: emphasises persistent maritime situational awareness and protection of critical maritime infrastructure.

- IMO SOLAS XI-2 / ISPS Code: mandatory port and maritime security framework for contracting governments, port authorities and shipping companies.

- UK National Protective Security Authority: provides protective security advice for critical national infrastructure owners and operators.

- Grand View Research maritime surveillance market summary: 2024 market estimate and 2025-2030 growth outlook.

- Precedence Research maritime surveillance market summary: 2025 estimate and 2035 forecast.

- ArXiv 2025 maritime AI / MDA literature used only for public-level themes: AIS/satellite fusion, adversarial AI resilience and explainable maritime autonomy.