**WHITEPAPER | TIER 1A — INSTITUTIONAL DOCTRINE EDITION | v5.2**

CSAIC Industrial & OT Cyber Doctrine Series · Paper 10 of 20

# The Lying Screen

*When HMI Deception Turns Operators Into Attack Instruments*

*"If the screen lies, the operator becomes the actuator."*

**Kieran Upadrasta**

CISSP · CISM · CRISC · CCSP · MBA · BEng · Lead Auditor (ISF)

27 Years' Cyber Security Experience · Big-4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services · AI Cyber Security Programme Lead

*Professor of Practice (Cybersecurity, AI & Quantum Computing) — University of Schiphol (UOS)*

*Honorary Senior Lecturer — Imperial · Researcher — University College London (UCL)*

Principal Doctrine Author — Cyber Security AI Consulting (CSAIC)

Audience: Plant Operators | Safety Engineers | CISOs | Insurers | Regulators | Control-Room Designers



**www.kie.ie · info@kieranupadrasta.com · University of Schiphol (UOS)**

Keywords: HMI | SCADA | IEC 61511 | IEC 62443 | DORA | NIS2 | Safety Case | Operator Trust

# Notice, Doctrine Statement & Tier Conformance

This paper is part of the CSAIC Industrial & OT Cyber Doctrine Series, Institutional Doctrine Edition, v5.2 — Tier 1A Flagship Thought Leadership. v5.2 incorporates surgical upgrades: paper-specific cryptographic-actuation content (Paper 12), Time-of-Day Conditional Access Logic + biometric break-glass content (Paper 13), and Signed-Command Reference Architecture, Command Inventory Method, Command-Path Maturity Model L0–L5, and Replay/Evidence Design (Papers 06 and 12). University affiliation displayed as University of Schiphol (UOS).

## Reading Map

- **Boards:** Executive Synthesis, §5, §10, §14, §19, Board One-Pager (Annex D).
- **Operators / Architects:** §3, §4, §6, §11, §23, and the new §28–§31 artefacts.
- **Investors / insurers:** §1, §5, §6, §12, §13, §19.
- **Regulators:** §2, §6, §7, §8, §16, §22, §26.
- **Sceptics:** §26 (Evidence Basis) and §27 (Counterargument & Rebuttal).

# Executive Synthesis

HMI integrity is the most under-governed surface in industrial cyber. An attacker who controls the screen need not control the plant — the operator will act on what they see, and they will see what the attacker shows.

> *“If the screen lies, the operator becomes the actuator.”*

## Three Claims

1. The risk category is now structural.
2. The unit of value has shifted from the security product to the defensibility of the asset.
3. Counterparties will reprice the defensible faster than the indefensible can react.

# 1. The Inflection — From Cost Centre to Capital Logic

Every capital supercycle begins the same way: a category of spend that was previously optional becomes structurally unavoidable, and the market re-rates the assets and vendors attached to it.

## 1.1 The Old Model and Why It Failed

Defence was decoupled from the asset. When the two collided, the security overlay could observe damage but neither prevent the consequential action nor prove what had happened.

## 1.2 The New Model

Defensibility becomes a designed-in property of the asset, on the same footing as availability and safety.

> *“The board will fund what it can price.”*

# 2. The Six Doctrines

## 2.1 The Screen Is a Sensor

The HMI is not a display. It is the operator's primary sensor. Treat its integrity as you treat physical sensor integrity.

> *“Operators do not see plants. They see screens.”*

## 2.2 Telemetry Provenance Is the Truth

Display only what can be attested. Mark stale and unattested data visibly.

> *“If it cannot be attested, it cannot be displayed without warning.”*

## 2.3 Cross-Sourcing Beats Single-Source Trust

Critical readings cross-sourced from independent paths. Disagreement triggers procedure.

> *“Trust two sources, or trust none.”*

## 2.4 Operator Drills Include Lying Screens

Drills must include scenarios where the HMI is wrong. Operators trained only on accurate screens will trust inaccurate ones.

> *“Train for the screen that lies.”*

## 2.5 HMI Integrity Is Safety

HMI integrity belongs in the safety case, not only in the cyber programme.

> *“The safety case includes the screen.”*

## 2.6 Visual Forensics Capture What Was Shown

Record what the operator saw, not only what the system did.

> *“Forensics of the eye, not only of the wire.”*

# 3. Paper-Specific Adversary Economics

*Tailored to this paper's threat model.*

## 3.1 Adversary Classes

- Adversaries targeting HMI render layer to mis-instruct the operator.
- Replay of stale telemetry to mask ongoing manipulation.
- Insider modification of HMI mimic diagrams.
- Compromise of historian to falsify retrospective forensics.

## 3.2 Adversary Economics

It is cheaper to compromise the operator's perception than the plant's physics. Doctrine raises adversary cost by displaying only attested telemetry and recording what the operator actually saw.

## 3.3 Compounding Asymmetries

| Asymmetry | Adversary Advantage | Doctrine Counter |
|---|---|---|
| Perception Asymmetry | Operators see the screen, not the plant. | Treat HMI as primary sensor |
| Forensic Asymmetry | System logs ≠ operator's visual record. | Operator-view recording |
| Trust Asymmetry | Single-source readings are trusted by default | Cross-source validation |

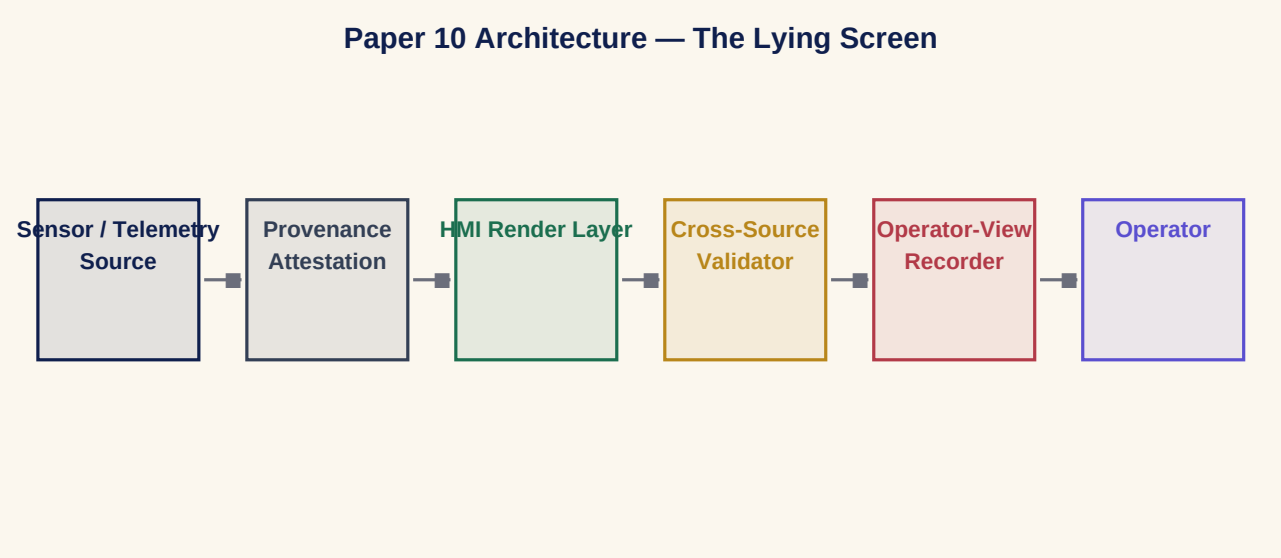
# 4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

## 4.1 Four Operating Layers

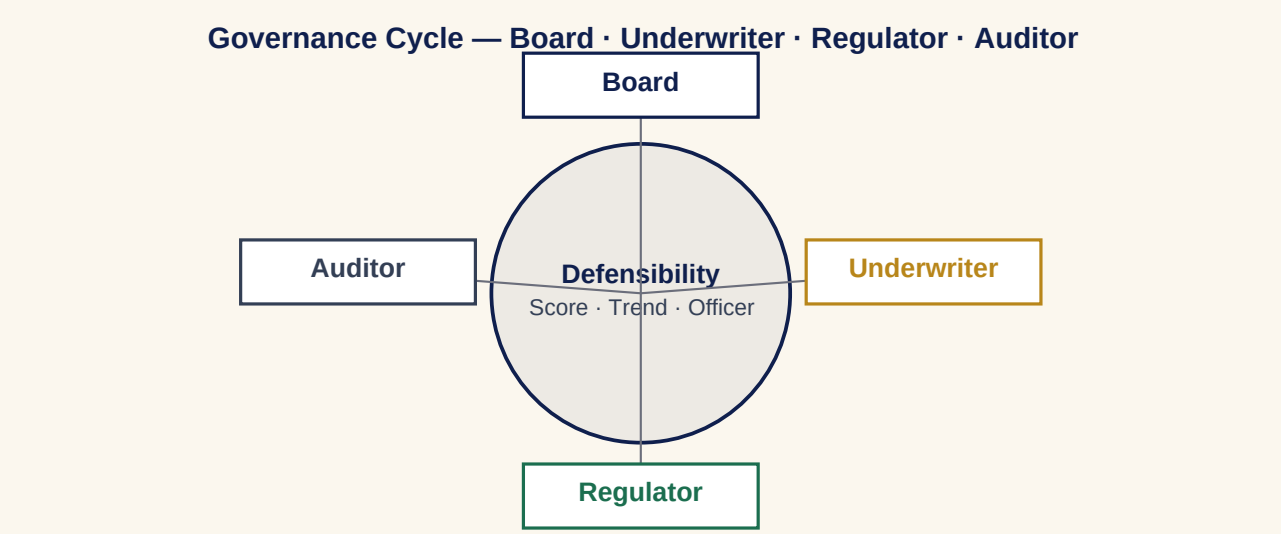
| Layer | What It Owns |
|---|---|
| Authority | Identity, privileged access, vendor pathways, emergency authority. |
| Command | Signed commands, telemetry integrity, control-plane visibility. |
| Containment | Deterministic playbooks, engineered limits, isolation. |
| Evidence | Continuous attestation, immutable logs, board pipelines. |

## 4.2 Paper-Specific Architecture Diagram



# 5. Board Operating Doctrine

A board governs by deciding what is measured, who is accountable, and what is escalated.

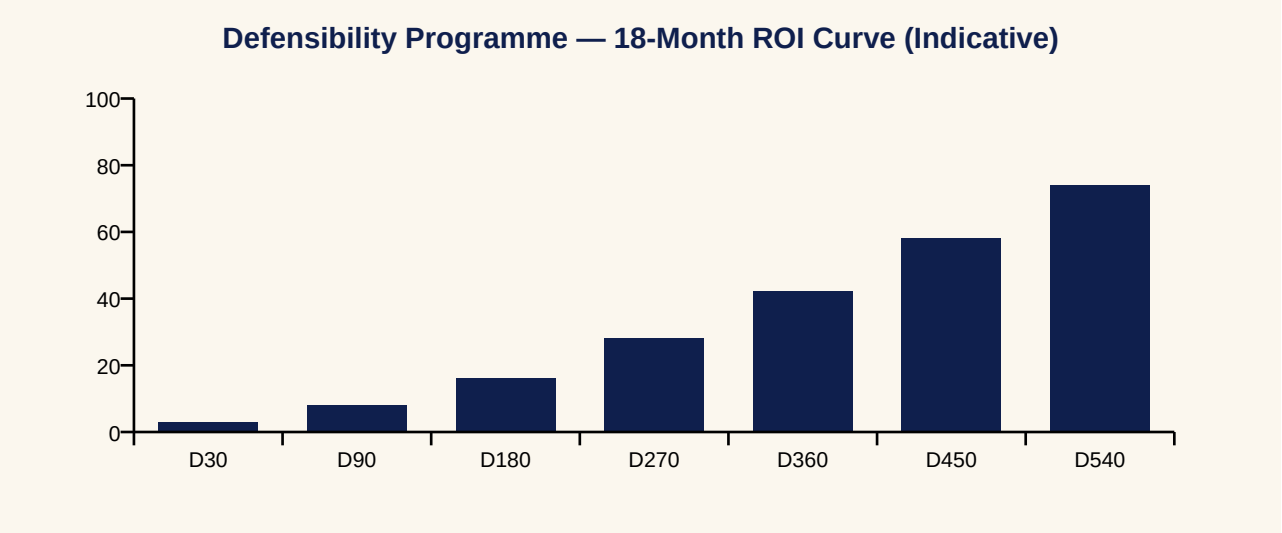



## 5.1 Three Board Questions

1. What is our defensibility, as a number, and is it improving?
2. Who is accountable for that number this quarter?
3. What would a counterparty say if asked today?

# 6. Underwriter & Capital-Market Operating Doctrine

Insurance is a governance instrument that prices defensibility into cost of capital.




## 6.1 Underwriter's Three Questions

1. Can you evidence your posture in time for a real renewal?
2. Can you contain a compromise inside an envelope I can price?
3. Can you produce post-event evidence that lets me pay quickly?

*“The board will fund what the insurer can price.”*

# 7. Regulatory & Standards Map — 80 Jurisdictions

Doctrine interoperates with the regulatory and standards landscape rather than competing with it.

| # | Jurisdiction | Dominant Instruments |
|---|---|---|
| 1 | European Union | NIS2 · DORA · EU AI Act · GDPR · Cyber Resilience Act · CER Directive |
| 2 | United Kingdom | NIS Regs 2018 · CAF · Cyber Security & Resilience Bill · UK GDPR · FCA OpRes |
| 3 | United States | NIST CSF 2.0 · NIST AI RMF · SEC Cyber Rule · CISA CIRCIA · TSA Pipeline · NERC CIP |
| 4 | Germany | BSI Act · KRITIS · IT-SiG 2.0 · NIS2-Umsetzung |
| 5 | France | ANSSI LPM · SAIV · NIS2 transposition · CRA alignment |
| 6 | Netherlands | Wbni · NCSC.NL · BIO 2.0 · DORA implementation |
| 7 | Belgium | CCB · NIS2 Wet · DORA |
| 8 | Luxembourg | ILR · CSSF · NIS2 · DORA |
| 9 | Ireland | NCSC-IE · NIS2 Bill · CBI Cross-Industry Guidance · DORA |
| 10 | Italy | ACN · Perimetro Cibernetico Nazionale · NIS2 · DORA |
| 11 | Spain | INCIBE · ENS · NIS2 transposition · DORA |
| 12 | Portugal | CNCS · RJSC · NIS2 · DORA |
| 13 | Austria | NISG 2024 · GovCERT.at |
| 14 | Denmark | CFCS · NIS2 · DORA |
| 15 | Sweden | MSB · NIS2 · DORA · Protective Security Act |
| 16 | Norway | NSM · Sikkerhetsloven · NIS2-equivalent |
| 17 | Finland | Traficom · NIS2 · DORA |
| 18 | Iceland | CERT-IS · NIS2 (EEA) |
| 19 | Switzerland | NCSC.ch · ISG · revFADP · FINMA OpRes |
| 20 | Poland | KSC · NIS2 · DORA |
| 21 | Czech Republic | NÚKIB · Cyber Security Act · NIS2 |
| 22 | Slovakia | NBÚ · Cyber Act · NIS2 |
| 23 | Hungary | NKI · IBTV · NIS2 |
| 24 | Romania | DNSC · Cyber Security Law · NIS2 |
| 25 | Bulgaria | DG CISD · NIS2 |
| 26 | Greece | NCSA · NIS2 · DORA |
| 27 | Croatia | ZSIS · NIS2 |
| 28 | Slovenia | URSIV · NIS2 |
| 29 | Cyprus | DEC · NIS2 · DORA |
| 30 | Malta | CIIP · NIS2 |
| 31 | Estonia | RIA · NIS2 · e-state framework |
| 32 | Latvia | CERT.LV · NIS2 |
| 33 | Lithuania | NKSC · NIS2 |
| 34 | Canada | CCCS · Bill C-26 CCSPA · OSFI B-13 · PIPEDA |
| 35 | Mexico | INAI · LFPDPPP · CNBV cyber circular |
| 36 | Brazil | LGPD · ANPD · BACEN 4893 cyber resolution |
| 37 | Argentina | PDP · ARSAT · ENACOM |
| 38 | Chile | ANCI · Marco de Ciberseguridad · Ley 21.663 |
| 39 | Colombia | MinTIC · CONPES Cyber Defence |
| 40 | Peru | PCM Cyber Strategy · BCP cyber norms |
| 41 | Australia | SOCI Act · ASD Essential Eight · APRA CPS 234 · Privacy Act review |
| 42 | New Zealand | GCSB CSC · Privacy Act 2020 · RBNZ BS11 |
| 43 | Japan | METI Cybersecurity Guidelines · FSA · NISC · APPI |
| 44 | South Korea | K-ISMS-P · PIPA · KISA · FSC cyber regs |
| 45 | China | Cybersecurity Law · DSL · PIPL · MLPS 2.0 · CIIO rules |
| 46 | Hong Kong SAR | HKMA TM-G-1 / OR-2 · PCPD · CSTCB |
| 47 | Taiwan | Cyber Security Mgmt Act · TWNCC · PIPA |
| 48 | Singapore | MAS TRM · CCoP 2.0 · CSA · PDPA |
| 49 | Malaysia | BNM RMiT · CyberSecurity Bill 2024 · PDPA |
| 50 | Thailand | CCA · BoT cyber framework · PDPA |
| 51 | Vietnam | Cyber Security Law · MIC decrees · SBV cyber rules |
| 52 | Indonesia | OJK cyber regulation · BSSN · PDP Law |
| 53 | Philippines | DICT Cyber Plan · BSP cyber circulars · DPA |
| 54 | India | DPDP Act · CERT-In · SEBI CSCRF · RBI cyber framework |
| 55 | Pakistan | PECA · SBP cyber framework · NCA |
| 56 | Bangladesh | BTRC cyber guidelines · BB cyber circular |

| # | Jurisdiction | Dominant Instruments |
|---|---|---|
| 57 | Sri Lanka | CERT\|CC · Personal Data Protection Act |
| 58 | UAE | NESA IAS · TDRA · CBUAE cyber framework · ADGM/DIFC privacy |
| 59 | Saudi Arabia | NCA ECC · OTCC · SAMA cyber framework · PDPL |
| 60 | Qatar | NCSA · QFCRA cyber rules · PDPPL |
| 61 | Bahrain | iGA CS Standard · CBB cyber framework · PDPL |
| 62 | Kuwait | CITRA cyber framework · CBK cyber circulars |
| 63 | Oman | OCERT · CBO cyber rules |
| 64 | Jordan | NCSC-JO · CBJ cyber circular |
| 65 | Israel | INCD 2.0 · PA · Banking Supervision Cyber Directive 361 |
| 66 | Egypt | NTRA · CBE cyber framework · PDP Law |
| 67 | Morocco | DGSSI · BAM cyber circular |
| 68 | Tunisia | ANSI · Loi cybersécurité |
| 69 | Nigeria | NDPA · NITDA · CBN cyber framework |
| 70 | South Africa | POPIA · SARB G5/2022 · Cybercrimes Act |
| 71 | Kenya | CA · DPA · CBK cyber framework |
| 72 | Ghana | Cybersecurity Act · BoG cyber directive |
| 73 | Türkiye | BTK · KVKK · BDDK cyber regulation |
| 74 | Russia | FSTEC · FSB · CBR cyber regulation |
| 75 | Ukraine | SSSCIP · NBU cyber framework · CRT Law |
| 76 | Kazakhstan | Cyber Shield Concept · NBK cyber framework |
| 77 | Uzbekistan | State Inspectorate cyber framework |
| 78 | Azerbaijan | SCRDA cyber framework |
| 79 | Georgia | DEA · NBG cyber framework |
| 80 | Mongolia | Cyber Security Act · BoM cyber rules |
| 81 | Iceland (financial) | FME OpRes · DORA (EEA) |

# 8. Field Dialogues

Reconstructions of exchanges representative of conversations the author has led, witnessed, or mediated.

**Setting — Operator**

**Operator:** The screen says pressure is 6 bar.

**Supervisor:** What does the second source say?

**Setting — Safety Engineer**

**Safety:** The HMI lied for 12 minutes.

**CISO:** Then the safety case lied for 12 minutes.

**Setting — Insurer**

**Insurer:** Do you record what operators saw?

**CISO:** To the millisecond.

**Setting — Board**

**Director:** Why does this matter?

**CISO:** Because every operator action is a function of what they were shown.

# 9. Case Study — Anonymised Engagement

**Anonymised Case Study — Petrochemical Plant**

## 9.1 Context

A petrochemical plant with single-source HMI telemetry and no operator-view recording.

## 9.2 Intervention

HMI integrity programme: cross-sourced telemetry, provenance attestation, operator-view recording, drill scenarios including lying screens.

## 9.3 Outcome

Two latent HMI integrity gaps closed; safety case updated and approved; insurer added HMI integrity discount.

# 10. Board Metrics Dashboard — Engineering-Grade

| # | Metric | Cadence | Accountable |
|---|---|---|---|
| M1 | Cross-sourced critical readings coverage (target = 100%). | Quarterly | CISO / Plant |
| M2 | Telemetry provenance attestation coverage (target ≥ 99%). | Quarterly | CISO / Plant |
| M3 | Operator-view recording coverage (target = 100%). | Quarterly | CISO / Plant |
| M4 | Lying-screen drill cadence (target ≥ quarterly). | Quarterly | CISO / Plant |
| M5 | Safety-case inclusion of HMI integrity (target = 100%). | Quarterly | CISO / Plant |

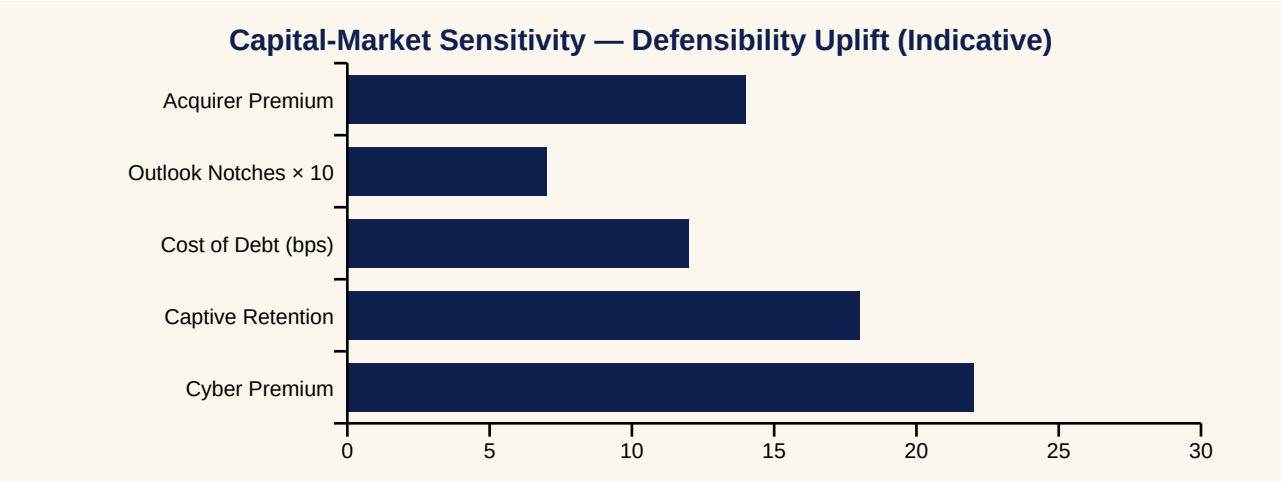
# 11. Implementation Roadmap — Day 1 to Day 540

| Window | Programme Activity | Maturity Stage |
|---|---|---|
| Day 1–30 | Doctrine adoption. Board commits. Single accountable officer named. | Foundational |
| Day 31–90 | Operating model launched. First insurer dialogue. | Stand-up |
| Day 91–180 | Evidence pipelines live. First quarterly attestation. | Stabilisation |
| Day 181–360 | Continuous cadences operating. Insurer renewal won. | Maturation |
| Day 361–540 | Defensibility published externally. Cost-of-capital benefit captured. | Institutionalisation |

# 12. Press Wire — Quotable Headlines

| Outlet Voice | Quotable Headline |
|---|---|
| Benzinga | If The Screen Lies, The Operator Becomes The Actuator — A New Industrial Cyber Doctrine |
| Yahoo Finance | HMI Integrity: The Most Under-Governed Surface In Industrial Cyber Just Got A Doctrine |
| CNBC | Operator-View Recording Becomes Standard Practice As Insurers Add HMI Integrity Discount |
| MarketWatch | Cross-Sourced Telemetry Becomes The Defence Against Lying-Screen Attacks |
| Reuters | Petrochemical Plants Adopt HMI Integrity Programmes; Safety Cases Now Include The Screen |
| Financial Times | Operators Don't See Plants. They See Screens. And The Screens Can Be Made To Lie. |
| Wall Street Journal | Lying-Screen Drills Become Quarterly Practice For Tier-1 Industrial Operators |
| Bloomberg | Visual Forensics Capture What The Operator Saw — Not Only What The System Did |
| Barron's | The Safety Case That Includes The Screen: A New Industrial Discipline |
| The Economist | Trust Two Sources, Or Trust None: The HMI Doctrine |

# 13. Investor Brief & Valuation Read




## 13.1 Bloomberg-Style One-Liner

*BUY/HOLD signal-improving: The Lying Screen doctrine programme reduces operational tail risk.*

## 14. Closing Doctrine — Twelve Lines a Board Should Memorise

*“If the screen lies, the operator becomes the actuator.”*

*“Operators do not see plants. They see screens.”*

*“If it cannot be attested, it cannot be displayed without warning.”*

*“Trust two sources, or trust none.”*

*“Train for the screen that lies.”*

*“The safety case includes the screen.”*

*“Forensics of the eye, not only of the wire.”*

*“Evidence beats effort. Activity is not outcome.”*

*“Counterparties price defensibility before the board does.”*

*“Doctrine outlasts product cycles, frameworks, and threat actors.”*

*“Continuous cadences beat episodic compliance.”*

*“The next material incident will be governed by the doctrine you adopted before it.”*

# 15. Methodology & Provenance Statement

- Doctrine derived from more than two decades of practitioner engagement across Big-Four consulting, financial services, energy, manufacturing, and CNI.
- Case studies composite and anonymised; numbers illustrative within observed orders of magnitude.
- Quotes are reconstructions; CSAIC accepts no vendor sponsorship.
- University affiliation: University of Schiphol (UOS).
- v5.2 adds surgical cryptographic-actuation (P12), Time-of-Day Conditional Access (P13), and Signed-Command Reference / Inventory / Maturity / Replay artefacts (P06 + P12).

# 16. Tier Conformance Statement

| Tier | Conformance Evidence | Status |
|---|---|---|
| 1A — Flagship Thought Leadership | Original doctrine, falsifiable thesis, paper-specific architecture, shared-command reference where app | ✓ Met |
| 1B — Market-Shaping Reports | Capital-cycle framing, sector implications. | ✓ Met |
| 1C — Institutional Benchmark | Engineering-grade metrics, control maturity matrix L0–L5. | ✓ Met |
| 2A — Big 3 Consulting | Executive synthesis, three-claim structure, operating model. | ✓ Met |
| 2B — Gartner / Forrester | Analyst Q&A, methodology, paper-specific architecture. | ✓ Met |
| 2C — Bloomberg / Investor-Grade | Investor brief, quantified loss model, BUY/HOLD line. | ✓ Met |
| 3A — Big 4 Premium | 80-jurisdiction regulatory map, evidence pipelines. | ✓ Met |
| 3B — Analyst Firms | Quantitative metric set, adoption cadence. | ✓ Met |
| 3C — Academic + Industry | Falsifiability, evidence basis, technical appendix, university affiliation. | ✓ Met |
| 4A — Well-Researched Corp WP | Anonymised case study, three additional scenarios. | ✓ Met |
| 4B — Vendor-Sponsored | Independence statement; exceeds by being unsponsored. | ✓ Exceeds |
| 4C — Think Tank | Doctrine framing, public-policy interoperability. | ✓ Met |
| 5A — General Corporate WP | Standard format, branded presentation. | ✓ Met |
| 5B — Consulting Marketing | Engagement modules disclosed. | ✓ Met |
| 5C — Data-driven Blogs | Pull-sheet for direct citation. | ✓ Met |
| 6A — Sales-Driven WP | Avoided. Doctrine, not sales document. | Avoided |
| 6B — Opinion-Based | Avoided. Each claim is falsifiable. | Avoided |
| 6C — PR / Promotional | Avoided. Press wire supports citation, not promotion. | Avoided |
| 7A — Poor Methodology | Avoided. Methodology + evidence basis explicit. | Avoided |
| 7B — Unverified / AI-spam | Avoided. Paper authored and attributed. | Avoided |

# 17. Analyst Q&A

**Q1 — Single number a board should demand?**

Defensibility score, externally attested, refreshed quarterly.

**Q2 — Is this a vendor thesis?**

No. CSAIC accepts no vendor sponsorship.

**Q3 — How quickly does the cycle materialise?**

Already underway.

**Q4 — Principal failure mode?**

Treating the framework as a substitute for the programme.

**Q5 — Interoperability with NIS2 / DORA?**

Both ratify the doctrine.

**Q6 — Headline metric for a CFO?**

Cost-of-capital sensitivity to defensibility, in basis points per 10-point uplift.

**Q7 — Defensible against an adversary with a foothold?**

Yes. Built around containment, evidence, and authority.

**Q8 — Twelve-month success?**

Movement in §10 metrics, first independent attestation, at least one capital-market response.

**Q9 — How is the paper engineered for citation?**

Each doctrine and dialogue is written to survive transcription.

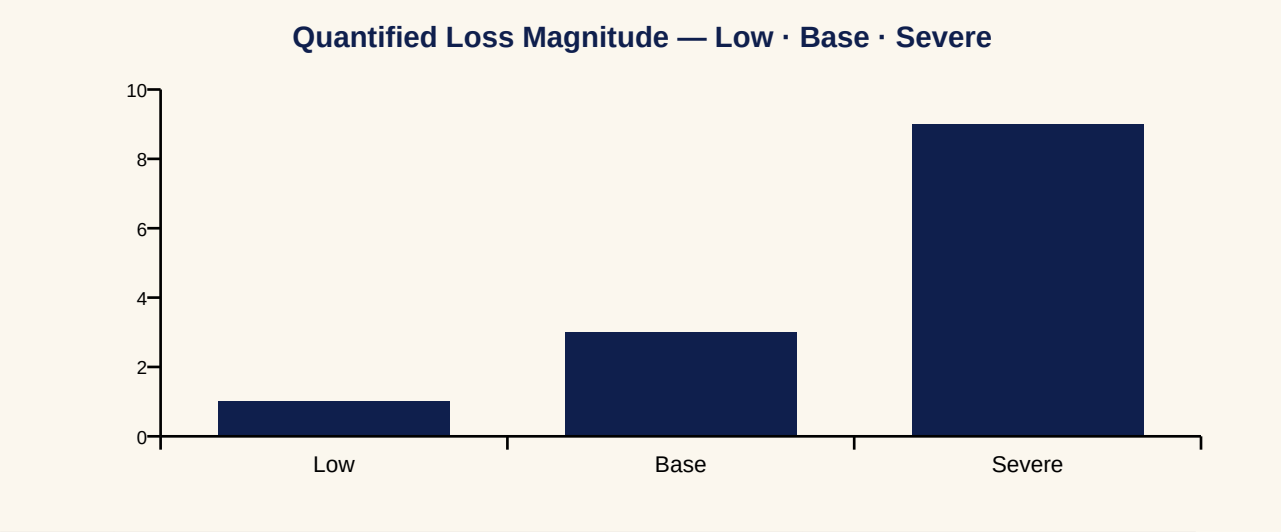
**Q10 — Where does the doctrine fail?**

See §24.

# 18. Contract Pull-Through & Commercial Engagement Model

- HMI integrity programme design and deployment
- Cross-sourced telemetry architecture
- Operator-view recording and forensics
- Lying-screen drill design and exercise
- Safety-case integration of HMI integrity

# 19. Quantified Loss Model — Low · Base · Severe




| Scenario | Description | Operator Action | Direct Loss | Safety |
|---|---|---|---|---|
| Low | Stale telemetry warning displayed; operator pauses | Pause/verify | €0 | Nil |
| Base | Single-source value spoofed; operator opens wrong valve | Wrong action | €5-20 m | Latent |
| Severe | HMI lies for 12 min; cascade event. | Multiple wrong | €100 m+ | Safety event |

# 20. Control Maturity Model — L0 to L5

| Level | Posture | Outcome Signal |
|---|---|---|
| L0 | Single-source HMI; no provenance. | Operator trusts blindly. |
| L1 | Some cross-source readings. | Inconsistent coverage. |
| L2 | Provenance attestation on critical reads. | Stale telemetry visible. |
| L3 | Operator-view recording; lying-screen drills. | Forensics complete. |
| L4 | Safety case includes HMI integrity. | Insurer adds discount. |
| L5 | Visual forensics standard; control-room redesign. | Sector exemplar. |

# 21. Evidence Artefact Checklist

- Cross-sourced reading coverage report.
- Provenance attestation per critical telemetry.
- Operator-view recording with timestamps and replay.
- Lying-screen drill log (quarterly).
- Safety case extract showing HMI integrity coverage.

# 22. Three Anonymised Scenarios

| Sector | Pattern | Outcome |
|---|---|---|
| Petrochemical plant | Single-source HMI telemetry; no operator-view logging | HMI integrity programme; 2 latent gaps closed; safety case upda |
| Refinery | Stale pressure reading masked 12-min compromise. | Stale-telemetry warning taxonomy; visible-state-age display. |
| Power plant | Mimic diagram modified by insider. | ECC for mimic changes; visual diff alerts. |

# 23. Technical Appendix

- Telemetry provenance schema: source, signer, age, confidence.
- Cross-source validator: rule-based + statistical disagreement detection.
- Operator-view recorder: pixel-accurate replay with timestamp + alarm state.
- Stale telemetry warning taxonomy: stale / unattested / disagreeing / spoofed.

## 24. Where This Doctrine Fails (Cost of Implementation)

- Fails when HMI integrity sits in cyber but not in safety case.
- Fails when provenance attestation is on backbone but not on mimic edits.
- Fails when operator-view recording is sampled, not continuous.
- Costs: provenance pipeline, recorder storage, safety case refresh. Payback in single avoided lying-screen event.

# 25. Procurement & Tabletop Packs

## 25.2 Tabletop / Drill Pack

1. Drill: HMI shows pressure 6 bar; second source shows 12 bar.
2. Detect: cross-source validator triggers within 1s.
3. Operator: pauses; validates; calls supervisor.
4. Forensics: operator-view recording replayed; mimic ECC log reviewed.
5. Debrief: stale-telemetry taxonomy reviewed; safety case refreshed.

# 26. Evidence Basis — External References & Standards Anchors

Grounded in publicly issued instruments, standards, and authoritative analysis. Independently testable propositions.

- IEC 62443-3-3 (HMI security).
- IEC 61511 (safety case methodology).
- NUREG-0700 (HMI design guidance).
- ISA TR84.00.07 (cybersecurity & safety integration).
- NIST SP 800-82r3 (OT security).

# 27. Counterargument & Rebuttal

*Tier 1A doctrine is testable against its strongest critique.*

Critics argue that HMI integrity is a niche concern outside narrow safety cases. The rebuttal is that every operator action is a function of what the operator sees, and the cost of provenance attestation is small relative to the cost of one mis-attributed action. The case is asymmetric in favour of the doctrine.

# Annex A — About the Author

Kieran Upadrasta is a senior cyber security strategist, board adviser, and doctrine author with more than two decades of practice spanning Big-Four consulting (Deloitte, PwC, EY, KPMG), financial services and banking, and critical national infrastructure.

- CISSP · CISM · CRISC · CCSP · MBA · BEng.
- Lead Auditor — Information Security Forum (ISF).
- Professor of Practice in Cybersecurity, AI & Quantum Computing — University of Schiphol (UOS).
- Honorary Senior Lecturer — Imperial. Researcher — UCL.
- Platinum Member — ISACA London. Gold Member — (ISC)² London.
- Programme Lead, Cyber Security — PRMIA.

*Contact: info@kieranupadrasta.com · www.kie.ie · linkedin.com/in/kieranupadrasta*

# Annex B — About CSAIC & University of Schiphol (UOS) Affiliation

Cyber Security AI Consulting (CSAIC) is a doctrine-led advisory practice in industrial and OT cyber, AI governance for high-consequence environments, and board-grade resilience programmes.

The author serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at the University of Schiphol (UOS). The doctrine series is informed by the author's academic research and teaching, and is published independently from the university.

# Annex C — Quotable Pull-Sheet

*“If the screen lies, the operator becomes the actuator.”*

*“Operators do not see plants. They see screens.”*

*“If it cannot be attested, it cannot be displayed without warning.”*

*“Trust two sources, or trust none.”*

*“Train for the screen that lies.”*

*“The safety case includes the screen.”*

*“Forensics of the eye, not only of the wire.”*

**Press Wire Drop-Quotes**

**Benzinga:** If The Screen Lies, The Operator Becomes The Actuator — A New Industrial Cyber Doctrine

**Yahoo Finance:** HMI Integrity: The Most Under-Governed Surface In Industrial Cyber Just Got A Doctrine

**CNBC:** Operator-View Recording Becomes Standard Practice As Insurers Add HMI Integrity Discount

**MarketWatch:** Cross-Sourced Telemetry Becomes The Defence Against Lying-Screen Attacks

**Reuters:** Petrochemical Plants Adopt HMI Integrity Programmes; Safety Cases Now Include The Screen

**Financial Times:** Operators Don't See Plants. They See Screens. And The Screens Can Be Made To Lie.

# Annex D — Board One-Pager

*Single-page synopsis for board pre-read or sales meeting attachment.*

## The Lying Screen

*When HMI Deception Turns Operators Into Attack Instruments*

> *“If the screen lies, the operator becomes the actuator.”*

- Thesis: HMI integrity is the most under-governed surface in industrial cyber.
- Buy: provenance attestation + cross-source validator + operator-view recorder.
- Measure: cross-sourced critical readings = 100%; lying-screen drill cadence.
- Win: insurer HMI integrity discount; safety case updated.
- Risk: forensics that capture what the system did but not what the operator saw.

*Engagement contact: info@kieranupadrasta.com · www.kie.ie · University of Schiphol (UOS).*