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

CSAIC Industrial & OT Cyber Doctrine Series · Paper 05 of 20

The Machine-Speed Operator

Governing AI Agents Before They Touch Industrial Control

"When AI gets tools, the plant gets a new class of operator."

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: Boards | CISOs | OT Architects | AI Governance Leads | Safety Engineers | Regulators

Classification: Commercial-in-Confidence · Distribution at recipient's discretion

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

Keywords: ISO 42001 | NIST AI RMF | EU AI Act | IEC 61511 | IEC 62443 | AI Governance | Functional Safety

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

Tool-using AI agents are entering industrial environments faster than the governance to constrain them. Treated as a new operator class — with authority, training, supervision, and accountability — they are an asset. Treated as a feature, they are a category-defining risk.

> *“When AI gets tools, the plant gets a new class of operator.”*

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 Agents Are Operators, Not Features

An AI agent that can issue an industrial command holds operator authority and must be governed as such — competence-checked, role-bounded, supervised, and revocable.

“If it can act, it must be sworn in.”

2.2 Determinism in Containment, Generativity in Advice

Generative reasoning is permissible at the periphery. Containment, isolation, and recovery actions must remain deterministic and pre-approved.

“The model may suggest. The playbook decides.”

2.3 Authority Is Scoped, Time-Bounded, Logged

No agent holds standing privileges. Every agent action is scoped, time-bounded, attested, and logged at the same standard as a privileged human session.

“Agents earn authority for a task, not for a tenure.”

2.4 Safety Cases Include the Model

The functional safety case must include the agent's failure modes — hallucination, prompt injection, drift, capability creep — alongside hardware failure modes.

“The model is part of the safety case, or it is part of the incident.”

2.5 Tool Use Is the Attack Surface

It is not the model that is dangerous. It is the tool the model can invoke. Govern the tool inventory with the rigour of a control-system inventory.

“Govern the tools. The model follows.”

2.6 Procurement Is the First Defence

Most AI risk is contracted in. The most powerful intervention is the procurement question that prevents the dangerous capability from being acquired in the first place.

“The cheapest control is the procurement question.”

3. Paper-Specific Adversary Economics

Tailored to this paper's threat model.

3.1 Adversary Classes

- Prompt-injection content authored to abuse tool-use APIs (MCP, function calls).
- Model drift induced by adversarial fine-tuning data in supply chain.
- Capability creep introduced by vendor over time without ECC oversight.
- Hallucination weaponised: agent confidently issues plausible but harmful command.

3.2 Adversary Economics

Adversary economics shift from exploit development to data and prompt manipulation — cheaper, harder to attribute, longer-dwell. Doctrine forces agents into deterministic envelopes for any action with consequential authority.

3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Speed Asymmetry	Agents act faster than human supervision.	Deterministic envelopes for consequential actions
Scope Asymmetry	Capability creep extends authority silently.	Capability inventory + ECC for every change
Provenance Asymmetry	Model lineage and tool lineage rarely traced.	Vendor attestation of model + tool provenance

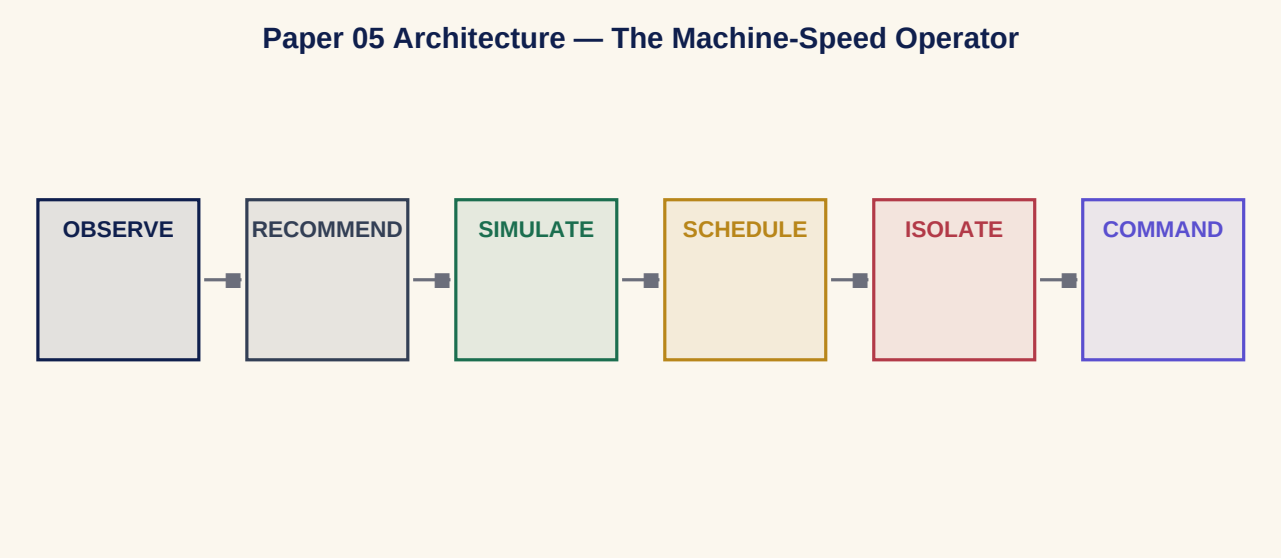
4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

4.1 Four Operating Layers

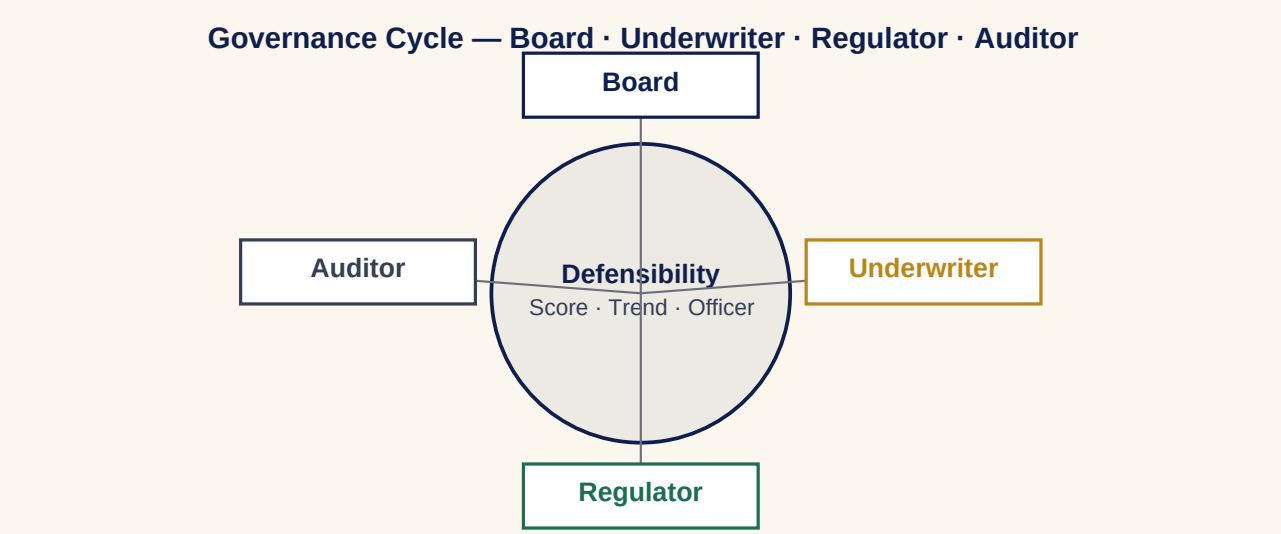
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

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.

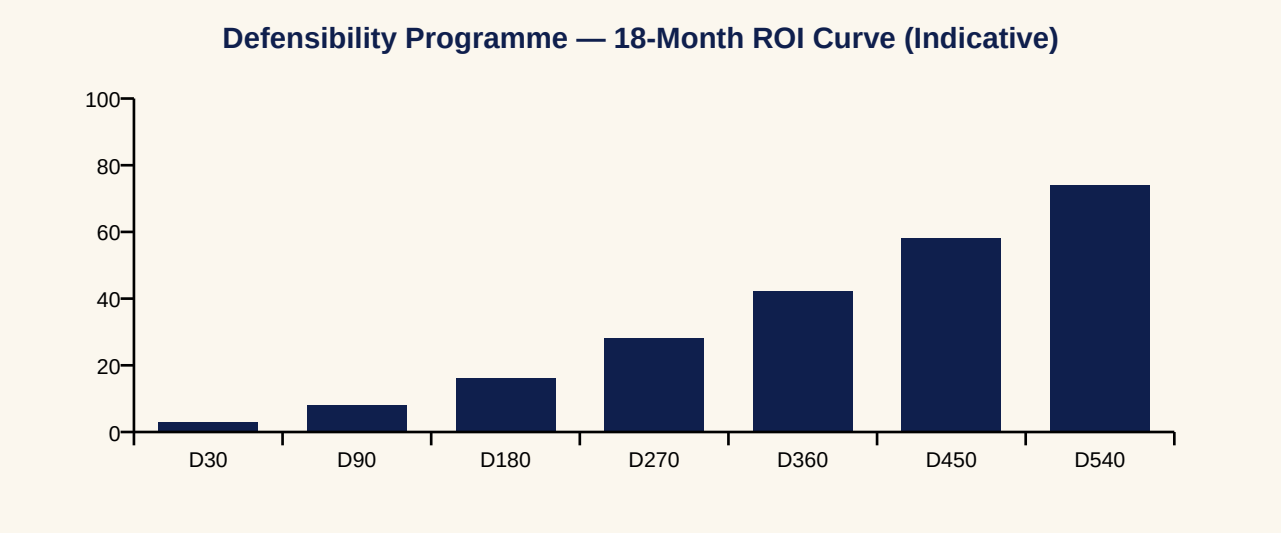


5.1 Three Board Questions

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 — Safety Engineer

Safety: What happens if the agent hallucinates a setpoint?

CISO: It cannot. The setpoint is bounded by deterministic envelopes, not by the model.

Setting — Board

Director: Can we revoke an agent in seconds?

CISO: Yes. Like any operator.

Setting — Regulator

Regulator: Who is accountable for the agent's action?

General Counsel: The same officer accountable for any operator's action.

Setting — Procurement

Procurement: The vendor wants tool-use enabled by default.

CISO: Then the vendor wants someone else.

9. Case Study — Anonymised Engagement

Anonymised Case Study — Tier-1 Refinery

9.1 Context

A refinery deployed AI agents into shift handover, alarm summarisation, and predictive maintenance with informal governance.

9.2 Intervention

Agent operator framework: capability inventory, scoped authority, deterministic envelopes around any action that crossed into control, safety-case update, agent attestation log integrated with control-room recording.

9.3 Outcome

Two latent prompt-injection paths closed; agent productivity preserved; regulator accepted updated safety case on first review; insurer added agent governance to the discount schedule.

10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	Agent inventory completeness (target = 100%).	Quarterly	CISO / Plant
M2	% agent actions executed inside deterministic envelopes (target = 100%).	Quarterly	CISO / Plant
M3	Mean time to revoke an agent (target ≤ 5 min).	Quarterly	CISO / Plant
M4	Agents with standing privileges (target = 0).	Quarterly	CISO / Plant
M5	Safety-case coverage of AI failure modes (target = 100% — hallucination, prompt injection, drift, capability creep).	Quarterly	CISO / Plant

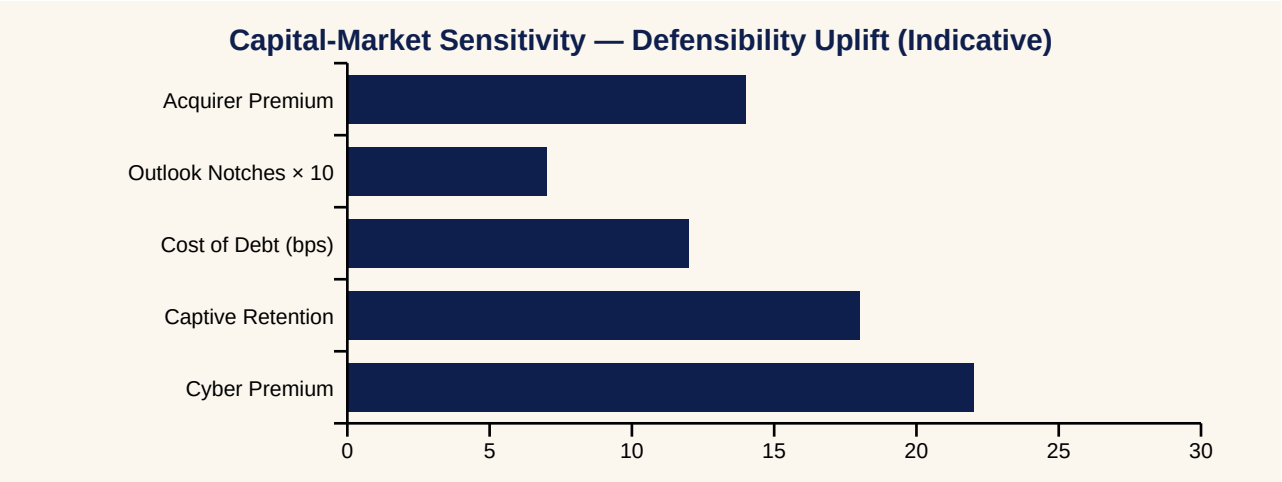
11. Implementation Roadmap — Day 1 to Day 540

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	AI Agents Just Became Operators — Now Industrial Cyber Has To Catch Up
Yahoo Finance	When AI Gets Tools, The Plant Gets A New Class Of Operator — And A New Class Of Risk
CNBC	Boards Are Being Asked: Can You Revoke An AI Agent The Way You Revoke A Login?
MarketWatch	Industrial AI Governance Becomes A Sellable Outcome As ISO 42001 And The EU AI Act Bite
Reuters	Functional Safety Cases Now Must Include AI Failure Modes — Hallucination, Prompt Injection, Drift
Financial Times	The Machine-Speed Operator: Why Industrial AI Needs Operator Discipline, Not Vendor Slogans
Wall Street Journal	Regulators Begin To Treat AI Agents As Accountable Operators In Industrial Settings
Bloomberg	Insurers Add AI Governance To The Discount Schedule For Industrial And Energy Operators
Barron's	Procurement Becomes The Most Powerful AI Control In The Industrial Stack
The Economist	Discipline, Not Improvisation: A Doctrine For AI In Plants

13. Investor Brief & Valuation Read



13.1 Bloomberg-Style One-Liner

BUY/HOLD signal-improving: The Machine-Speed Operator doctrine programme reduces operational tail risk.

14. Closing Doctrine — Twelve Lines a Board Should Memorise

“When AI gets tools, the plant gets a new class of operator.”

“If it can act, it must be sworn in.”

“The model may suggest. The playbook decides.”

“Agents earn authority for a task, not for a tenure.”

“The model is part of the safety case, or it is part of the incident.”

“Govern the tools. The model follows.”

“The cheapest control is the procurement question.”

“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.

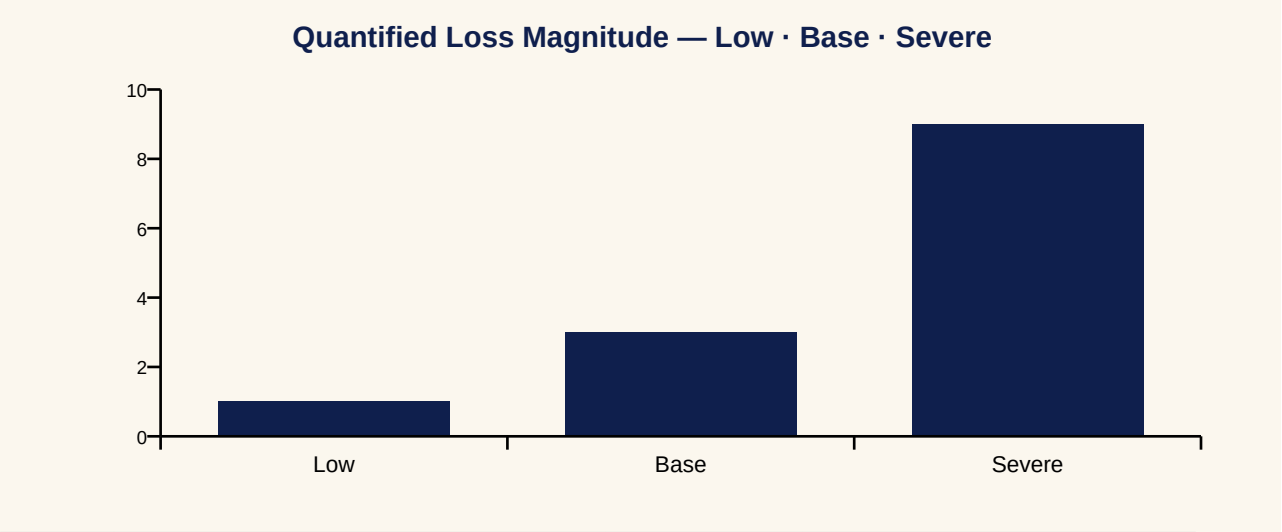
Q10 — Where does the doctrine fail?

See §24.

18. Contract Pull-Through & Commercial Engagement Model

- Industrial AI governance framework design
- Agent operator attestation programme
- Deterministic envelope architecture for AI-adjacent control
- Safety-case update integrating agent failure modes
- Procurement guardrail design and training

19. Quantified Loss Model — Low · Base · Severe



Scenario	Description	Direct Loss	Safety Impact	Regulator Actio
Low	Agent recommends invalid setpoint; rejected by envelope.	€0	Nil	None
Base	Agent executes within envelope but degrades cycling.	€2–8 k	Latent	Notification
Severe	Capability creep + prompt injection → consequential command.	€20–100 k	Safety event	Operator licence action

20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0	Agents deployed without inventory; tools enabled by default.	Latent incident paths.
L1	Agent inventory; advisory-only authority.	Productivity gains; risk uncatalogued.
L2	Scoped tool inventory; ECC for changes.	Risk catalogued; envelopes designed.
L3	Deterministic envelopes around all consequential actions.	Agent productivity preserved; risk bounded.
L4	Safety-case updated; agent attestation log integrated.	Regulator-accepted on first review.
L5	Continuous attestation; insurer discount scheduled; sector exemplar.	Sector exemplar agent governance.

21. Evidence Artefact Checklist

- Agent inventory: name, owner, model, tool set, authority scope, expiry.
- Capability change log via ECC, signed.
- Deterministic-envelope test results (out-of-bound rejection rate).
- Safety-case extension with AI failure modes covered.
- Vendor provenance attestation: model lineage, training data, dependencies.

22. Three Anonymised Scenarios

Sector	Pattern	Outcome
Tier-1 refinery	AI agents in shift handover, alarm summary, predictive maintenance with informal governance.	Operator-class framework; 2 lateral injection paths closed; safety
Utility control room	Copilot recommends switching action; envelope rejects out-of-bound suggestion.	Productivity preserved; risk bounded.
Pharma plant	Vendor enables tool-use by default in firmware update.	Procurement guardrail catches before deployment.

23. Technical Appendix

- Agent authority matrix: OBSERVE → RECOMMEND → SIMULATE → SCHEDULE → ISOLATE → COMMAND.
- Deterministic envelope: setpoint bounded by hard-coded physics constants, not model output.
- Tool-use control inventory (MCP / function-call) per agent, with capability sign-off.
- Safety-case failure-mode extension: hallucination, prompt injection, drift, capability creep.

24. Where This Doctrine Fails (Cost of Implementation)

- Fails when tool-use is enabled by default at the vendor level.
- Fails when safety case excludes AI failure modes.
- Fails when revocation is bureaucratic rather than instant.
- Costs: agent governance office, envelope tooling, safety-case refresh, procurement training. Payback in regulator and insurer recognition.

25. Procurement & Tabletop Packs

25.1 Procurement Clause Pack

- Vendor must disclose model lineage, training data sources, and dependencies.
- Vendor must enable tool-use only on opt-in with capability sign-off.
- Vendor must support deterministic-envelope enforcement at the integration boundary.
- Vendor must commit to ECC for any capability change; no silent capability extension.
- Vendor must provide attestation suitable for regulator and safety case.

26. Evidence Basis — External References & Standards Anchors

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

- ISO/IEC 42001 (AI management system).
- NIST AI RMF 1.0.
- EU AI Act (Regulation (EU) 2024/1689).
- OWASP LLM Top 10 / Agentic AI Top 10.
- IEC 61511 (functional safety, process industries).

27. Counterargument & Rebuttal

Tier 1A doctrine is testable against its strongest critique.

The counter-position is that AI in industrial control is a vendor fad and should be banned, not governed. The rebuttal is that productivity is already being captured; the doctrine question is whether the institution governs that productivity or absorbs the risk silently. The choice is not adoption vs. ban; it is governed adoption vs. ungoverned adoption.

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

“When AI gets tools, the plant gets a new class of operator.”

“If it can act, it must be sworn in.”

“The model may suggest. The playbook decides.”

“Agents earn authority for a task, not for a tenure.”

“The model is part of the safety case, or it is part of the incident.”

“Govern the tools. The model follows.”

“The cheapest control is the procurement question.”

Press Wire Drop-Quotes

Benzinga: AI Agents Just Became Operators — Now Industrial Cyber Has To Catch Up

Yahoo Finance: When AI Gets Tools, The Plant Gets A New Class Of Operator — And A New Class Of Risk

CNBC: Boards Are Being Asked: Can You Revoke An AI Agent The Way You Revoke A Login?

MarketWatch: Industrial AI Governance Becomes A Sellable Outcome As ISO 42001 And The EU AI Act Bite

Reuters: Functional Safety Cases Now Must Include AI Failure Modes — Hallucination, Prompt Injection, Drift

Financial Times: The Machine-Speed Operator: Why Industrial AI Needs Operator Discipline, Not Vendor Slogans

Annex D — Board One-Pager

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

The Machine-Speed Operator

Governing AI Agents Before They Touch Industrial Control

> *“When AI gets tools, the plant gets a new class of operator.”*

- Thesis: AI agents in industrial environments are a new operator class.
- Buy: agent operator framework + deterministic envelopes + procurement guardrails.
- Measure: agents with standing privileges = 0; envelope coverage = 100%.
- Win: regulator-accepted safety case; insurer governance discount.
- Risk: capability creep silently extends authority without ECC.

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