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

CSAIC Industrial & OT Cyber Doctrine Series · Paper 16 of 20

The Poisoned Simulator

How Digital Twins Could Mis-Train the Next Control-Room Crisis

"Poison the simulator today. Mis-train the crisis tomorrow."

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: Utilities | Aviation | Rail | Manufacturers | Digital Twin Vendors | Regulators | Insurers

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

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

Keywords: Digital Twin | Simulator | IEC 62443 | NIS2 | DORA | Operator Training | ISO 42001

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

Training simulators and engineering digital twins are now part of the control-system attack surface. A compromised twin trains operators to perform the wrong actions, confidently, in real crises.

> *“Poison the simulator today. Mis-train the crisis tomorrow.”*

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 Twin Is a Control System

If the twin can mis-train an operator, it can damage the plant. Treat it accordingly.

“The twin is the plant in waiting.”

2.2 Twin Integrity Is Attested

Twin integrity is signed, attested, and reproducible.

“If you cannot reproduce the twin, you cannot trust the training.”

2.3 Operator Drills Include Twin Failure

Drills include scenarios where the twin disagrees with the plant.

“Train for the twin that lies.”

2.4 Twin Updates Are Engineering Changes

Twin updates flow through engineering change control, not vendor patch cycles.

“Twin patches are engineering changes.”

2.5 Twin Data Is Asset Data

Twin telemetry is asset telemetry. Govern it accordingly.

“Twin data leaves no asset.”

2.6 Vendors Attest Twin Provenance

Vendors attest twin provenance: data, models, updates, dependencies.

“No attestation, no twin.”

3. Paper-Specific Adversary Economics

Tailored to this paper's threat model.

3.1 Adversary Classes

- Slow data poisoning of training scenarios for delayed mis-training.
- Vendor compromise propagating to twin via patch cycles.
- Insider modification of training scenarios.
- Supply-chain compromise of twin platform vendor.

3.2 Adversary Economics

Cheap to corrupt training data; expensive to attack live plant. Doctrine forces twin updates through ECC and requires daily attestation so mis-training is detected before crisis.

3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Dwell Asymmetry	Mis-training surfaces only in crisis.	Daily twin attestation
Change Asymmetry	Twin updates evade plant ECC.	Twin-update-as-engineering-change
Provenance Asymmetry	Vendor data lineage unverified.	Vendor twin provenance attestation

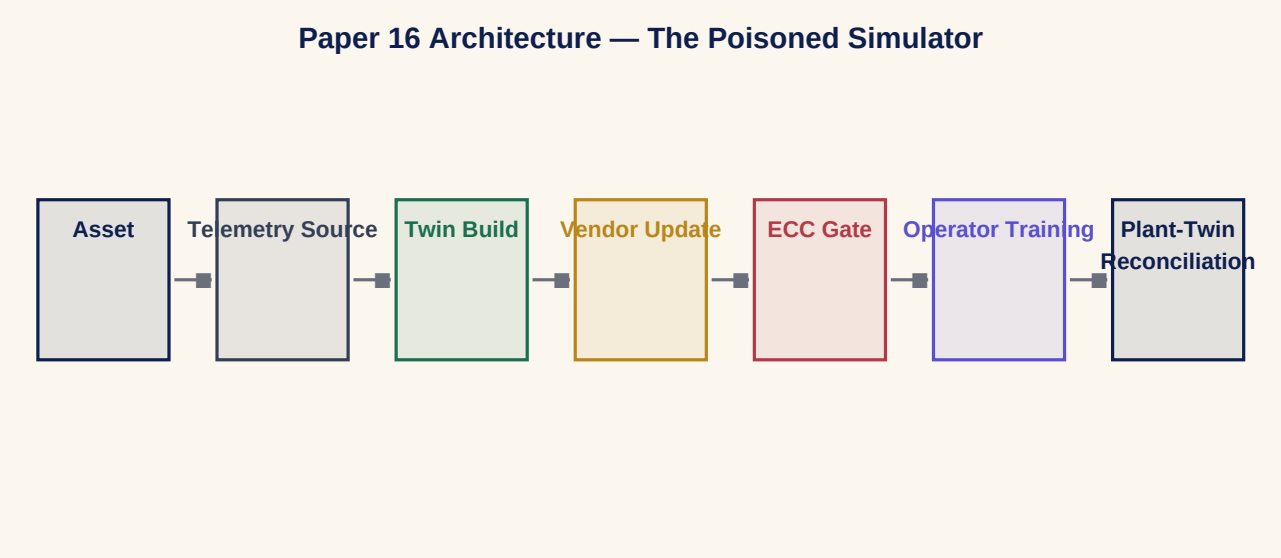
4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

4.1 Four Operating Layers

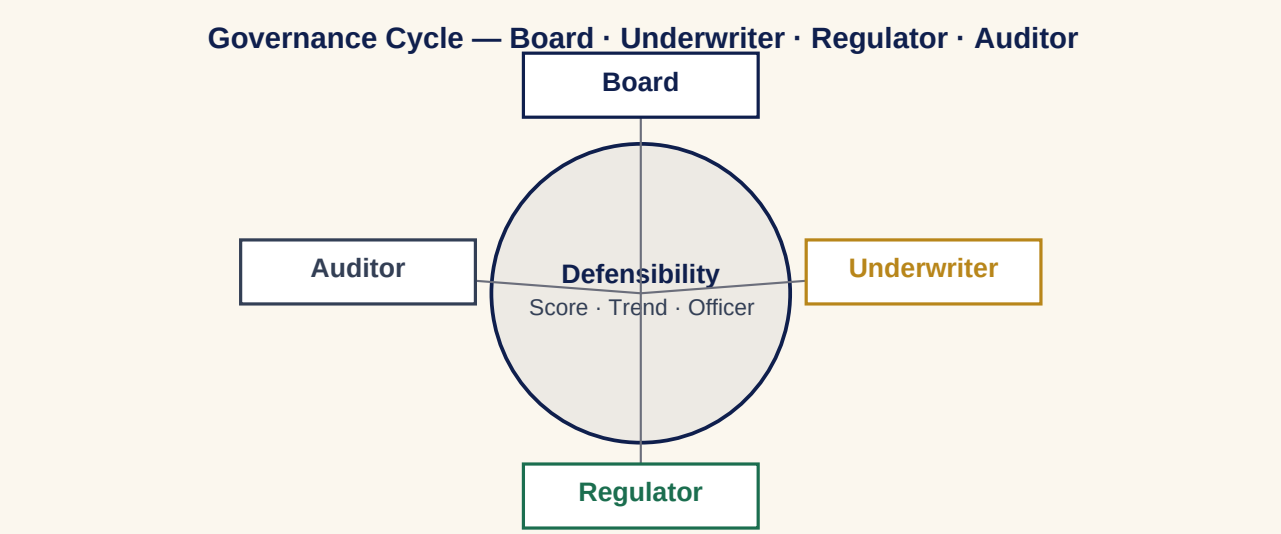
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

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.

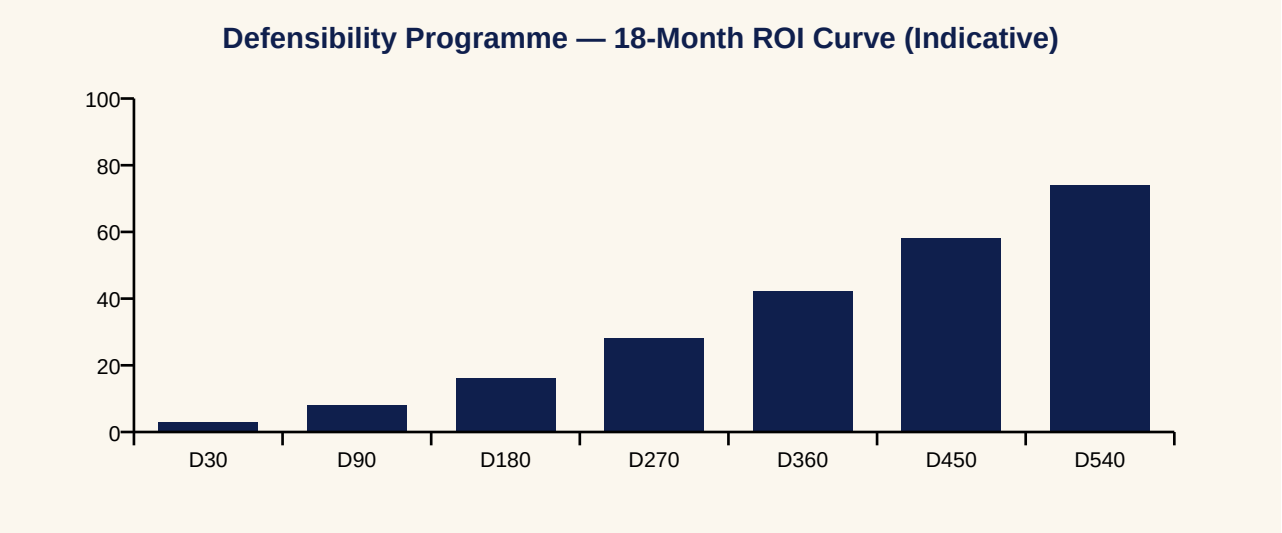


5.1 Three Board Questions

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 — Trainer

Trainer: The simulator and plant disagree.

CISO: Then one is wrong. Find which.

Setting — Board

Director: How would we know if the twin was poisoned?

CISO: Daily attestation, signed by the vendor and verified by us.

Setting — Vendor

Vendor: We push updates monthly.

CISO: Through engineering change control, or not at all.

Setting — Regulator

Regulator: Are operators trained on the real plant?

CISO: They are trained on an attested twin of the real plant.

9. Case Study — Anonymised Engagement

Anonymised Case Study — Rail Operator

9.1 Context

A rail operator with a vendor-managed training simulator updated independently of engineering change control.

9.2 Intervention

Twin integrity programme: attestation, ECC integration, drill scenarios with twin-plant disagreement, vendor attestation contracts.

9.3 Outcome

Two latent training drift issues closed; regulator accepted updated training case; insurer extended cyber-physical cover.

10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	Twin attestation cadence (target = daily).	Quarterly	CISO / Plant
M2	Twin updates through ECC (target = 100%).	Quarterly	CISO / Plant
M3	Twin-failure drill cadence (target ≥ quarterly).	Quarterly	CISO / Plant
M4	Vendor attestation coverage (target = 100%).	Quarterly	CISO / Plant
M5	Twin telemetry governance coverage (target = 100%).	Quarterly	CISO / Plant

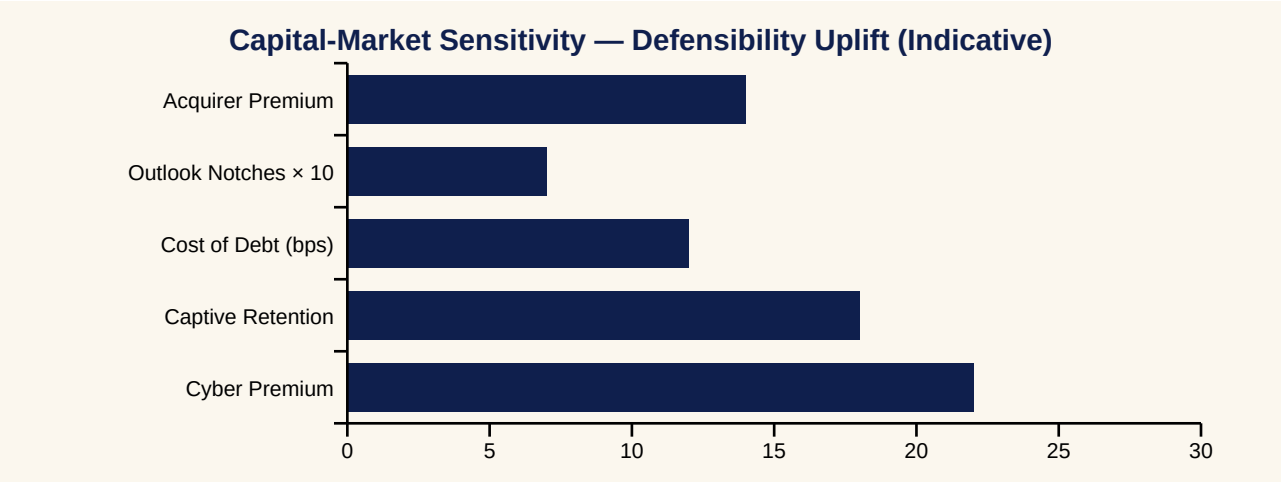
11. Implementation Roadmap — Day 1 to Day 540

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	Poison The Simulator Today. Mis-Train The Crisis Tomorrow.
Yahoo Finance	Digital Twins Become A Control-System Attack Surface — Vendor Attestation Becomes Mandatory
CNBC	Rail Operators Add Twin Attestation To Daily Operational Routine
MarketWatch	Twin Updates Now Flow Through Engineering Change Control, Not Vendor Patch Cycles
Reuters	Insurers Extend Cyber-Physical Cover For Operators With Verified Twin Integrity
Financial Times	The Twin Is The Plant In Waiting — A Doctrine For Industrial Simulators
Wall Street Journal	Twin-Failure Drills Become Standard Quarterly Practice
Bloomberg	Vendor Twin Provenance Attestation Becomes A Contract Norm
Barron's	Aviation, Rail And Utilities Converge On Twin Integrity Programmes
The Economist	Train For The Twin That Lies: The New Operator Doctrine

13. Investor Brief & Valuation Read



13.1 Bloomberg-Style One-Liner

BUY/HOLD signal-improving: The Poisoned Simulator doctrine programme reduces operational tail risk.

14. Closing Doctrine — Twelve Lines a Board Should Memorise

“Poison the simulator today. Mis-train the crisis tomorrow.”

“The twin is the plant in waiting.”

“If you cannot reproduce the twin, you cannot trust the training.”

“Train for the twin that lies.”

“Twin patches are engineering changes.”

“Twin data leaves no asset.”

“No attestation, no twin.”

“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.

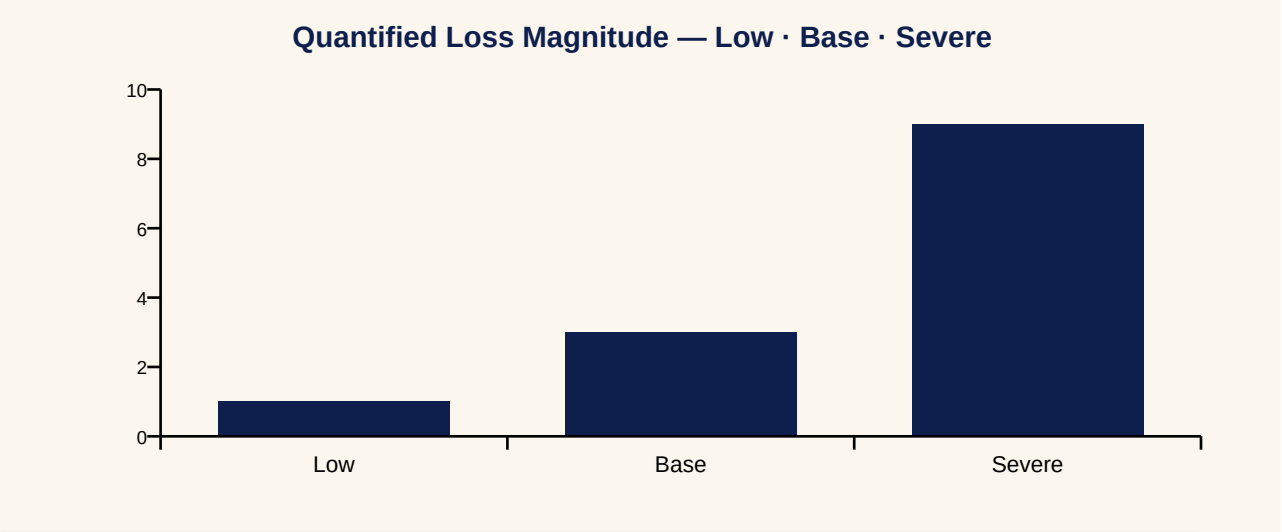
Q10 — Where does the doctrine fail?

See §24.

18. Contract Pull-Through & Commercial Engagement Model

- Digital twin integrity programme
- Twin-ECC integration design
- Twin-failure drill design and exercise
- Vendor twin attestation framework
- Twin telemetry governance

19. Quantified Loss Model — Low · Base · Severe



Scenario	Description	Operator Action	Direct Cost	Safety
Low	Twin-plant disagreement detected pre-crisis.	Recalibrate	€0.2-1 m	Nil
Base	Mis-trained operator makes wrong action under load.	Wrong action	€10-40 m	Near-miss
Severe	Crisis training poisoned; cascading mis-action.	Multiple errors	€100 m+	Safety event

20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0	Vendor-managed twin; no ECC.	Latent training drift.
L1	Twin inventory; ECC for major updates.	Partial coverage.
L2	Daily twin attestation pilot.	Drift observable.
L3	Twin-failure drills quarterly.	Operators train for twin that lies.
L4	Vendor attestation contractual.	Insurer extends cover.
L5	Twin telemetry governed as asset telemetry.	Sector exemplar.

21. Evidence Artefact Checklist

- Twin attestation log (daily).
- Twin update ECC records.
- Twin-failure drill log (quarterly).
- Vendor provenance attestation per release.
- Twin telemetry governance evidence.

22. Three Anonymised Scenarios

Sector	Pattern	Outcome
Rail operator	Vendor-managed simulator updated independently of EOC.	Twin integrity programme; 2 latent issues closed; insurer extende
Refinery	Twin data drift from sensor calibration change.	Cross-reconcile twin and plant daily.
Aviation	Simulator vendor compromise via update channel.	Vendor provenance attestation per release.

23. Technical Appendix

- Simulator poisoning attack chain: data → model → scenario → operator training.
- Twin-update change-control model: ECC for any change; signed by vendor and operator.
- Operator mis-training drill: twin and plant intentionally disagree; operator response measured.
- Vendor provenance attestation template.

24. Where This Doctrine Fails (Cost of Implementation)

- Fails when twin is treated as IT, not OT.
- Fails when training scenarios are vendor-curated, not reviewed.
- Fails when twin-failure drills are never conducted.
- Costs: ECC integration, daily attestation, drill cadence, vendor contract uplift. Payback in single avoided mis-trained crisis.

25. Procurement & Tabletop Packs

25.1 Procurement Clause Pack

- Vendor must attest model, data, and code provenance per release.
- Vendor must accept ECC for any change touching the twin.
- Vendor must support daily attestation of twin state.
- Vendor must enable cross-reconciliation feeds with the live plant.
- Termination on any silent capability change.

25.2 Tabletop / Drill Pack

1. Drill: simulator and plant disagree by 10% on pressure.
2. Detect: cross-reconcile alarm within 1 hr.
3. Investigate: ECC log + vendor attestation reviewed.
4. Operator: trained-for-disagreement procedure activates.
5. Debrief: training case refreshed; insurer notified.

26. Evidence Basis — External References & Standards Anchors

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

- IEC 62443-4-1 (secure product development).
- ISO/IEC 42001 (AI management).
- NIST AI RMF.
- ISA TR84 functional safety considerations for digital twins.
- NIST SP 800-160 (systems security engineering).

27. Counterargument & Rebuttal

Tier 1A doctrine is testable against its strongest critique.

The counter is that digital twins are not safety-critical and that the doctrine over-engineers a training tool. The rebuttal is that operator action under crisis is a function of training, and training quality is a function of twin integrity. The chain is short and direct.

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

“Poison the simulator today. Mis-train the crisis tomorrow.”

“The twin is the plant in waiting.”

“If you cannot reproduce the twin, you cannot trust the training.”

“Train for the twin that lies.”

“Twin patches are engineering changes.”

“Twin data leaves no asset.”

“No attestation, no twin.”

Press Wire Drop-Quotes

Benzinga: Poison The Simulator Today. Mis-Train The Crisis Tomorrow.

Yahoo Finance: Digital Twins Become A Control-System Attack Surface — Vendor Attestation Becomes Mandatory

CNBC: Rail Operators Add Twin Attestation To Daily Operational Routine

MarketWatch: Twin Updates Now Flow Through Engineering Change Control, Not Vendor Patch Cycles

Reuters: Insurers Extend Cyber-Physical Cover For Operators With Verified Twin Integrity

Financial Times: The Twin Is The Plant In Waiting — A Doctrine For Industrial Simulators

Annex D — Board One-Pager

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

The Poisoned Simulator

How Digital Twins Could Mis-Train the Next Control-Room Crisis

> *“Poison the simulator today. Mis-train the crisis tomorrow.”*

- Thesis: digital twins are control systems waiting to be activated.
- Buy: twin attestation + ECC integration + twin-failure drills.
- Measure: twin attestation cadence = daily; twin updates via ECC = 100%.
- Win: regulator-accepted training case; insurer extended cover.
- Risk: twin updates flow vendor-to-operator without ECC.

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