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

CSAIC Industrial & OT Cyber Doctrine Series · Paper 12 of 20

Command Is the New Perimeter

Cryptographic Actuation, DNP3-SA, IEC 62351 and the Boundary Between the Supervisory Data Plane and the Physical Control Plane

"A signed command is the only fence the plant respects."

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: OT Architects | Protection Engineers | TSO/DSO Control-Room Leads | CISOs | Insurers | Regulators

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

Keywords: DNP3-SA | IEC 62351 | IEC 61850 GOOSE/SV | IEC 60870-5-104 | Cryptographic Actuation | Supervisory Data Plane | Physical Control Plane | DORA | NIS2

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

The defensible unit in industrial cyber is no longer the network perimeter and is not equivalent to IT Zero Trust. It is cryptographic actuation — every consequential write to a relay, breaker, or actuator is signed by an attested operator identity, validated at the field device, and replayable as evidence. The doctrine sits at the boundary between the Supervisory Data Plane (HMIs, EWS, historians) and the Physical Control Plane (DNP3, IEC 61850 GOOSE/SV, Modbus, IEC 60870-5-104) and treats the boundary as the asset.

> *“A signed command is the only fence the plant respects.”*

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 Cryptographic Actuation Is the Perimeter

Every consequential command — every breaker open/close, every setpoint write, every protective relay trip enable — carries a signature, an identity, a freshness window, and a replay record. The signature is verified at the field device, not at the SCADA. If the field device cannot verify, the command does not execute.

“A signed command is the only fence the plant respects.”

2.2 The Supervisory Plane and the Physical Plane Are Not the Same Plane

HMIs, engineering workstations, historians, and Active Directory live on the Supervisory Data Plane. Relays, RTUs, IEDs, IO modules, and protection devices live on the Physical Control Plane. Compromise of the first does not entitle the adversary to act on the second. The boundary is the doctrine.

“Defend the boundary between the screen and the actuator.”

2.3 Protocol Authentication Beats Network Segmentation

DNP3 Secure Authentication (IEEE 1815-2012), IEC 62351-5 (DNP3/T101 message authentication), IEC 62351-6 (GOOSE/SV authentication) and IEC 62351-9 (key management) are the operative controls. Segmentation slows lateral movement; protocol authentication denies the consequential action.

“If it speaks IEC 61850 and it is not signed, it is unauthenticated.”

2.4 Replay Windows Are Engineering Parameters

Freshness windows are tuned to grid physics, not to convenience. A protection trip can tolerate sub-second freshness; a tariff change can tolerate minutes. The window is a safety case parameter and signed off by the protection engineer, not the security architect.

“Time is part of the signature.”

2.5 Key Management Is a Substation-Engineering Discipline

Keys live in tamper-evident HSMs at the substation. Rotation is scheduled with planned outages. Compromise procedures are joint between protection and cyber. Key custody is RACI'd at board level.

“Keys are physical assets that happen to be numbers.”

2.6 Forensic Replay Is Court-Quality

Every accepted and every rejected command is logged with signer identity, time, freshness, command payload, device state before/after, and protection-relay context. The log is admissible in a regulator hearing and signed by the field device, not the SCADA.

“The relay attests the command, not the operator.”

3. Paper-Specific Adversary Economics

Tailored to this paper's threat model.

3.1 Adversary Classes

- Adversaries who already hold SCADA / EWS / AD authority and rely on the field device accepting any well-formed command.
- Vendor-side compromise pushing unsigned firmware or unsigned IED configuration changes.
- Insider abuse of unsigned engineering channels (IEC 61131-3 logic, ICCP, vendor-specific config tools).
- Replay attackers using captured legitimate commands outside their freshness window.
- Time-sync compromise (GPS / PTP) intended to widen the replay window invisibly.

3.2 Adversary Economics

Adversary economics for IT Zero Trust bypass are well-understood; cryptographic actuation breaks the bypass at a different layer. The adversary now has to compromise either the substation HSM (physical, tamper-evident) or the relay firmware-verification chain — both orders of magnitude more expensive than SCADA-level compromise. Doctrine relocates the defensive boundary from the network to the field device.

3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Layer Asymmetry	Adversary plans against IT/SCADA; defender must defend physics	Authentication at the relay, not the SCADA
Time Asymmetry	Captured commands have value beyond their freshness window	Freshness window as engineering parameter
Trust Asymmetry	Unsigned commands are trusted by default in legacy IEDs	Default-deny at the protocol layer
Custody Asymmetry	Keys treated as IT secrets; not physically secured	Substation HSMs with joint custody

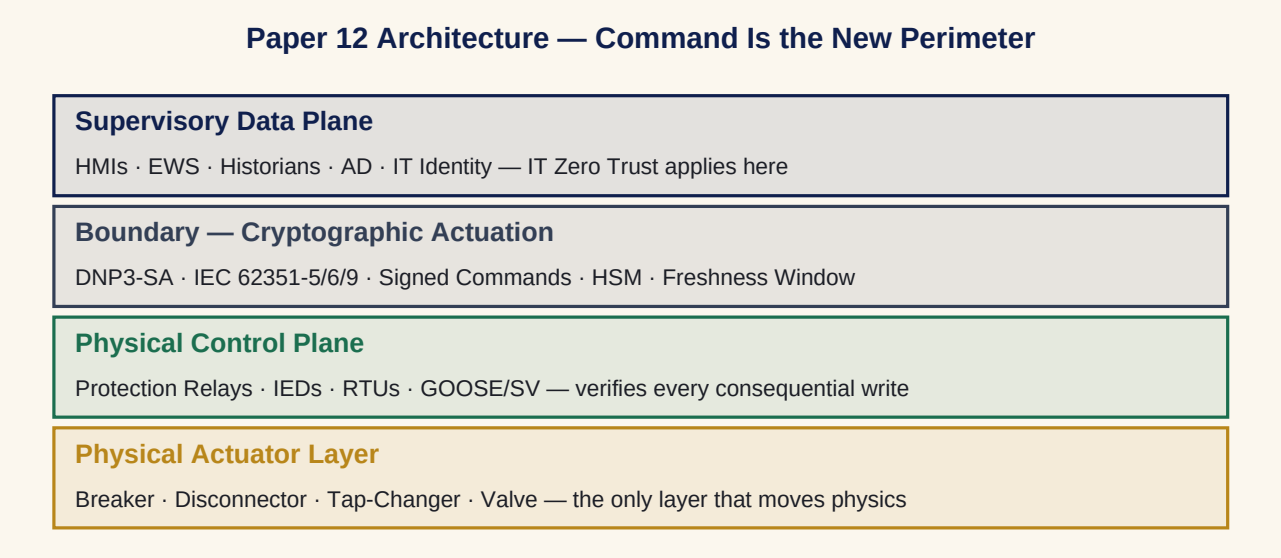
4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

4.1 Four Operating Layers

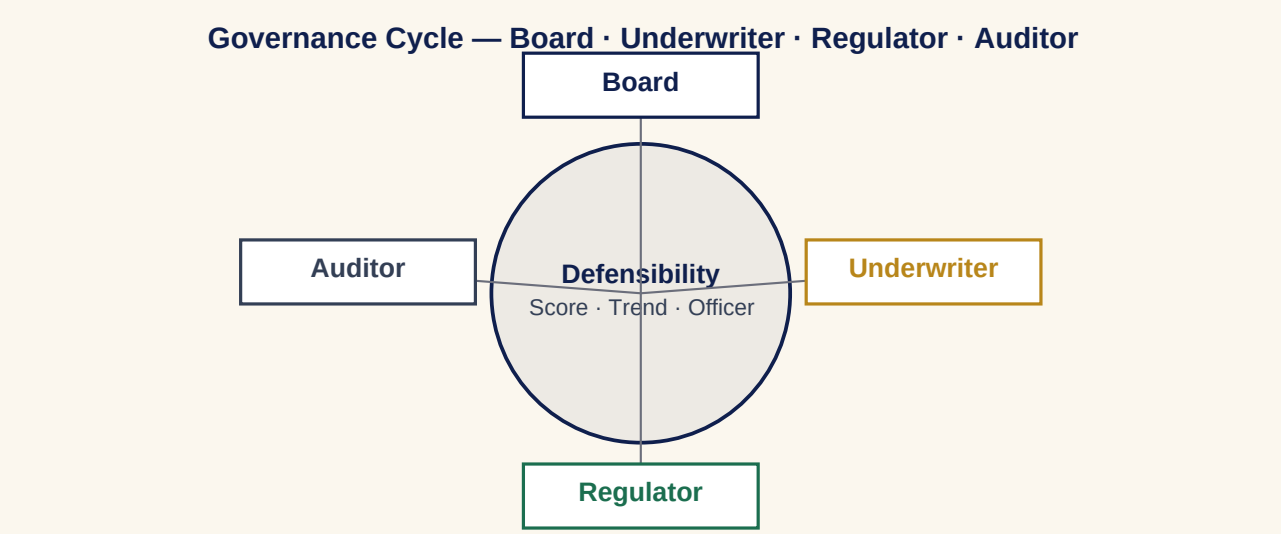
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

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.

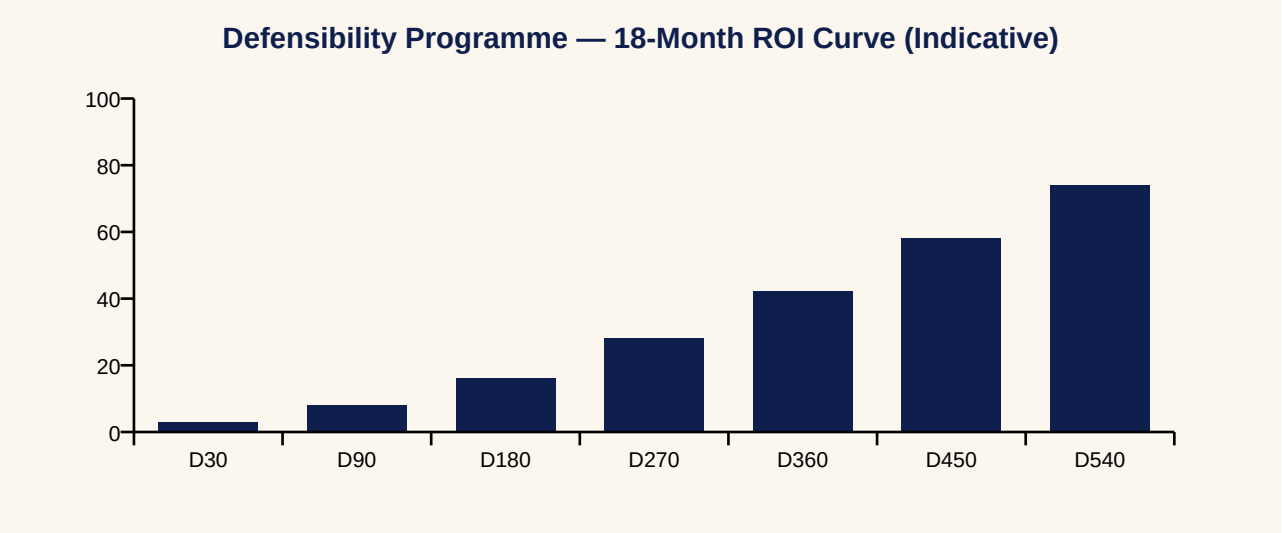


5.1 Three Board Questions

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 — Control Room — Substation Trip Event

Operator: Breaker 23B just opened. The HMI says no operator action.

Protection Engineer: Pull the relay event log. Is the trip signed by a protection scheme, an operator identity, or unsigned?

Operator: Signed by protection scheme. Differential element picked up. Legitimate.

Protection Engineer: Good. The signature distinguishes a legitimate protection trip from a hijacked SCADA command. The relay refuses unsigned writes by design.

Setting — Vendor — Firmware Update Conversation

OEM: Our latest firmware patches a CVE. Push tonight.

Protection Engineer: Through engineering change control, with a fresh key envelope, and not at 03:00. The relay validates the firmware signature against our HSM, not yours.

Setting — Regulator — Post-incident Hearing

Regulator: How can you prove the breaker was opened by a legitimate operator and not an attacker on the network?

CISO: The relay event log contains a DNP3-SA signature, the operator's signed identity, the freshness window, and the command payload. Reproducible at the relay, not at the SCADA.

Setting — Board

Director: Is this Zero Trust?

CISO: Zero Trust is a network model. Cryptographic actuation is a physics model. The relay is the policy enforcement point — not the firewall.

9. Case Study — Anonymised Engagement

Anonymised Case Study — Tier-1 European TSO

9.1 Context

A Tier-1 European TSO with mature IT Zero Trust and segmented substation networks, but unsigned DNP3 and IEC 61850 GOOSE/SV traffic across 600+ substations. Recent red-team demonstrated the ability to issue breaker commands from a compromised engineering workstation that the SCADA accepted as legitimate.

9.2 Intervention

Three-year cryptographic actuation programme: DNP3-SA enabled across legacy IEDs, IEC 62351-6 for GOOSE/SV on new builds, substation HSMs deployed, freshness windows tuned per protection class, joint protection-cyber key custody, relay event logs streamed to immutable evidence lake with signer attestation.

9.3 Outcome

Latent unauthenticated command pathways reduced from 14,000 to <50 within 18 months; regulator-recognised exemplar of protocol-layer authentication; insurer reduced retention by 28% on the back of cryptographic forensic evidence; the same red-team failed to execute consequential commands at the relay despite SCADA compromise.

10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	% DNP3 / IEC 60870-5-104 / IEC 61850 traffic authenticated under IEC 62351-5 (target ≥ 99%).	Quarterly	CISO / Plant
M2	Relays accepting unauthenticated writes on tier-1 assets (target = 0).	Quarterly	CISO / Plant
M3	Mean substation HSM key-rotation cycle (target ≤ 12 months, joint protection cyber signoff).	Quarterly	CISO / Plant
M4	Mean time to detect an unsigned consequential write at the relay event log (target ≤ 2 s).	Quarterly	CISO / Plant
M5	Forensic replay completeness across consequential commands (target = 100%, signed chain verified).	Quarterly	CISO / Plant

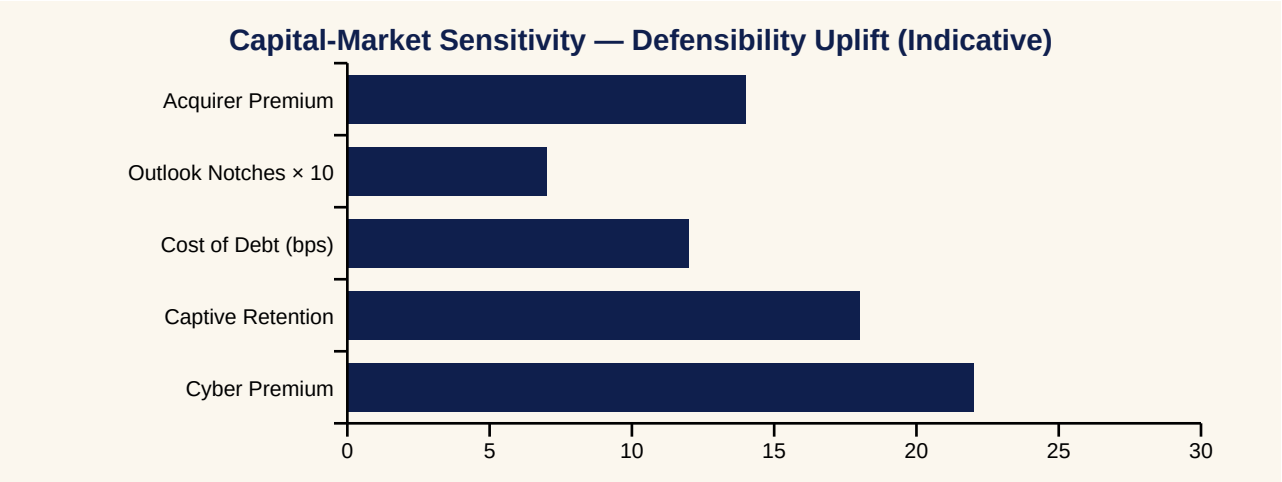
11. Implementation Roadmap — Day 1 to Day 540

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	The Perimeter Doesn't Control The Plant Anymore — Commands Do
Yahoo Finance	Command Is The New Perimeter: A Doctrine For The OT Control Plane
CNBC	Signed Commands Become Table Stakes For Tier-1 Utilities Under New Regulatory Pressure
MarketWatch	Latent Command Pathways Reduced 73% In One Utility Case — Insurer Cuts Retention
Reuters	Continuous Control-Plane Visibility Becomes The New Minimum For Critical Operators
Financial Times	Episodic Visibility Is Institutional Blindness — A Doctrine For The Control Plane
Wall Street Journal	Recovery Drills Now Validate Command Authority Restoration, Not Only Data
Bloomberg	Control-Plane Inventory Becomes A Board-Reportable Asset
Barron's	Boards Receive Command-Plane Evidence Packs Alongside Financial Statements
The Economist	Defend The Commands, Not The Cables: A Doctrine For Industrial Cyber

13. Investor Brief & Valuation Read



13.1 Bloomberg-Style One-Liner

BUY/HOLD signal-improving: Command Is the New Perimeter doctrine programme reduces operational tail risk.

14. Closing Doctrine — Twelve Lines a Board Should Memorise

“A signed command is the only fence the plant respects.”

“A signed command is the only fence the plant respects.”

“Defend the boundary between the screen and the actuator.”

“If it speaks IEC 61850 and it is not signed, it is unauthenticated.”

“Time is part of the signature.”

“Keys are physical assets that happen to be numbers.”

“The relay attests the command, not the operator.”

“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.

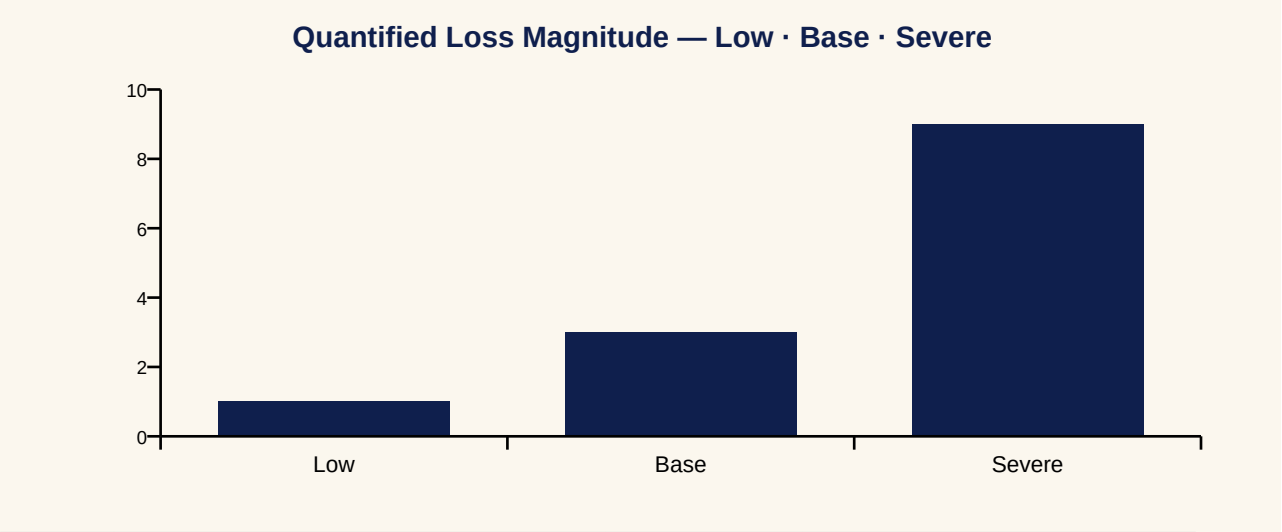
Q10 — Where does the doctrine fail?

See §24.

18. Contract Pull-Through & Commercial Engagement Model

- Cryptographic actuation programme design (DNP3-SA, IEC 62351, IEC 61850 GOOSE/SV)
- Substation HSM deployment and key lifecycle governance
- Protocol authentication uplift across legacy IED fleet
- Joint protection-engineer + cyber key custody framework
- Relay-level forensic evidence pipeline build and regulator engagement

19. Quantified Loss Model — Low · Base · Severe



Scenario	Description	Detection	Direct Cost	Capital Impact
Low	Unsigned write rejected at relay; SCADA shows attempted command.	Real-time	€0	Outlook neutral
Base	Unsigned write executed on a tier-2 IED before authentication upgrade.	Months	€1.0-40 m	Outlook downgrade risk
Severe	Coordinated unsigned commands across substations.	Hours under SCADA compromise.	€100 m+	Rating downgrade; national event

20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0 IT Zero Trust only	Segmented network; unsigned OT commands.	Red-team demonstrates SCADA-to-relay path.
L1 Pilot DNP3-SA	DNP3-SA pilot on one substation; legacy IEDs unaltered.	Visibility improved; risk persists at scale.
L2 Fleet DNP3-SA	DNP3-SA across the IED fleet; GOOSE/SV unauthenticated.	Substation-wide protection.
L3 IEC 62351-6 GOOSE/SV	GOOSE/SV authentication; substation HSMs deployed.	Relay-level evidence; insurer recognition.
L4 Full Cryptographic Actuation	Every consequential command signed, attested, replay-bounded.	Regulator exemplar; rating uplift.
L5 Cross-TSO Federation	Federated key trust across interconnect; shared evidence schema.	Sector benchmark.

21. Evidence Artefact Checklist

- DNP3-SA / IEC 62351 conformance attestation per protocol per substation (signed quarterly).
- Substation HSM key inventory and rotation log with joint protection-cyber sign-off.
- Relay event log streaming evidence with signer attestation per consequential command.
- Red-team report demonstrating relay-level rejection of unsigned consequential writes.
- Forensic replay pack of last 12 months of consequential commands across the fleet.

22. Three Anonymised Scenarios

Sector	Pattern	Outcome
Tier-1 European TSO	600+ substations, IT Zero Trust mature, OT protection programme, and	3-year programme, unauthenticated paths 14,000 → <50; insure
National DSO	GOOSE/SV across a city ring; legacy IEDs without IEC 62351-6	GOOSE/SV authentication uplift; substation HSMs; protection cla
Generator	Vendor-pushed unsigned firmware updates accepted by relays.	Replay-and-verification against operator HSM; vendor on pro

23. Technical Appendix

- Protocol authentication map: DNP3-SA (IEEE 1815-2012), IEC 62351-5 (T101/DNP3), IEC 62351-6 (GOOSE/SV), IEC 62351-9 (key management).
- Substation HSM architecture: tamper-evident, dual-control, joint protection-cyber custody.
- Freshness window tuning: protection trips < 1s, supervisory commands seconds, tariff changes minutes — engineered, not negotiated.
- Relay event log schema: signer identity, freshness, payload, device state pre/post, protection-relay context, signed by relay.
- Migration pattern for legacy IEDs unable to support DNP3-SA: brokered gateway with signature enforcement at the boundary.

24. Where This Doctrine Fails (Cost of Implementation)

- Fails when keys are treated as IT secrets rather than substation-engineering assets.
- Fails when freshness windows are set by security architects without protection-engineer sign-off.
- Fails when legacy IEDs are left unauthenticated 'pending refresh' for years.
- Costs: substation HSM capex, IED firmware uplift, joint protection-cyber operating model, training. Payback in relay-level forensic capability and insurer recognition.

25. Procurement & Tabletop Packs

25.1 Procurement Clause Pack

- All IEDs / RTUs / protection relays must support DNP3-SA or IEC 62351-5/6 at procurement.
- Vendor firmware must be signed and verifiable against an operator-controlled HSM, not the vendor's.
- Key custody is joint protection-cyber; the vendor holds no key material in production.
- Vendor must accept ECC for any change touching protocol authentication or key lifecycle.
- Termination right on any silent firmware push or unsigned configuration change.

25.2 Tabletop / Drill Pack

1. Drill: red team compromises an engineering workstation and issues a breaker-open command via DNP3.
2. Detect: relay rejects the unsigned write within 2 seconds; SCADA shows attempted but failed command.
3. Attribute: relay event log identifies the workstation, the unsigned payload, and the rejection signature.
4. Recover: workstation isolated; HSM keys rotated as precaution; protection-cyber joint review.
5. Debrief: regulator notified within 24h with full forensic replay; insurer evidence pack signed.

26. Evidence Basis — External References & Standards Anchors

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

- IEEE 1815-2012 (DNP3 Secure Authentication).
- IEC 62351 family — particularly 62351-5 (DNP3/T101 message authentication), 62351-6 (GOOSE/SV authentication), 62351-9 (key management).
- IEC 61850 (substation automation).
- NIST SP 800-82r3 (OT security guidance) — section on protocol-layer security.
- CIGRE WG D2.46 (security for substation communications) and related working group output.

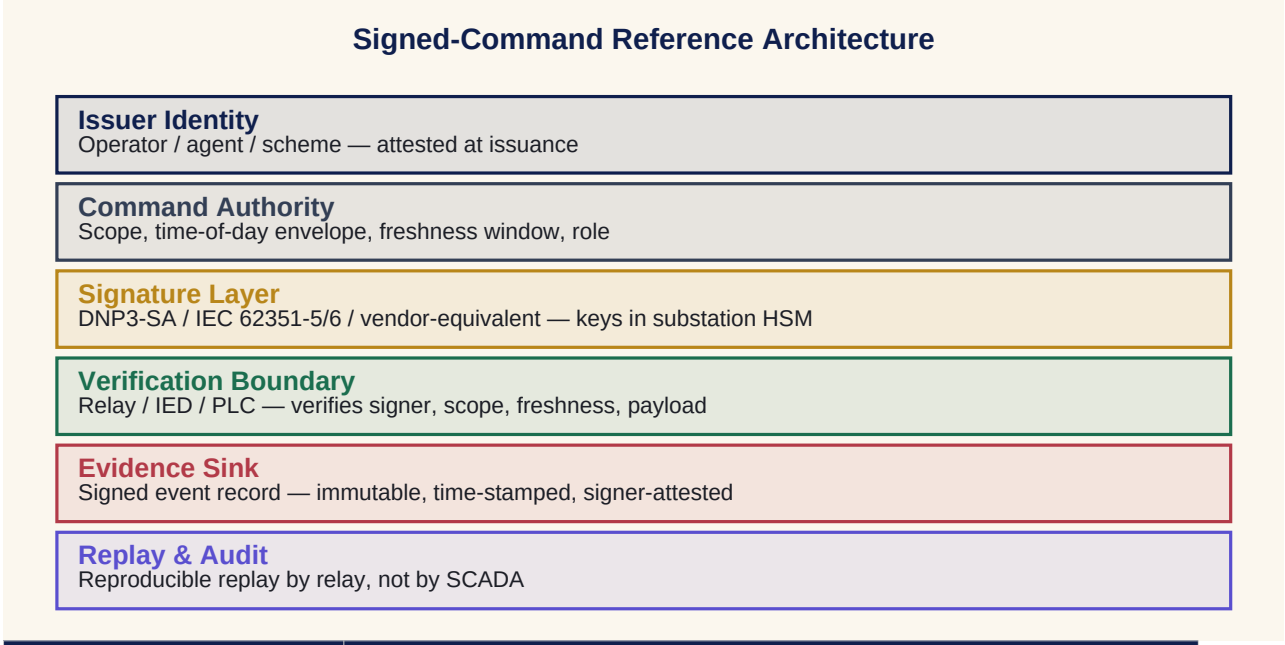
27. Counterargument & Rebuttal

Tier 1A doctrine is testable against its strongest critique.

The strongest critique is that cryptographic actuation duplicates the work of IT Zero Trust and adds operational complexity for marginal benefit. The rebuttal is empirical: every red-team that has reached the SCADA layer has executed consequential commands, irrespective of upstream Zero Trust posture, because the field device has no way to distinguish a legitimate operator from a compromised workstation. Cryptographic actuation closes the only door that controls physics. The operational cost is real and is the price of a defensible boundary.

28. Signed-Command Reference Architecture

The reference architecture below shows the cryptographic chain from issuer to actuator. Every consequential command traverses these six layers; the verification boundary at the relay/IED/PLC is the policy enforcement point.



Layer	Function
Issuer Identity	Operator / agent / scheme — attested at issuance
Command Authority	Scope, time-of-day envelope, freshness window, role
Signature Layer	DNP3-SA / IEC 62351-5/6 / vendor-equivalent — keys in substation HSM
Verification Boundary	Relay / IED / PLC — verifies signer, scope, freshness, payload
Evidence Sink	Signed event record — immutable, time-stamped, signer-attested
Replay & Audit	Reproducible replay by relay, not by SCADA

29. Command Inventory Method

A discoverable, classifiable, validatable, canonicalisable, governable approach to command-pathway inventory. The output is a living artefact, refreshed quarterly.

1. Discover: passive observation of every consequential write across DNP3 / IEC 60870-5-104 / IEC 61850 / Modbus / vendor protocols at the substation boundary for at least 90 days.
2. Classify: tag each observed command pathway with (a) protocol, (b) issuer class, (c) target device, (d) consequential? yes/no, (e) authenticated? yes/no.
3. Validate: probe — issue benign unsigned commands and confirm rejection at the verification boundary. Any acceptance is an inventory gap.
4. Canonicalise: publish the live command inventory with named owner, change-control gate, and review cadence.
5. Govern: any new consequential pathway requires inventory entry before commissioning; quarterly reconciliation to the live inventory.

30. Command-Path Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0 Undiscovered	No inventory; unknown command pathways accepted by default	Red team demonstrates undisclosed paths.
L1 Discovered	Inventory in pilot zone; passive observation operational	Visibility partial.
L2 Classified	All consequential pathways classified by protocol-class and risk-tier	Risk-tagged authn.
L3 Validated	Probe programme demonstrates rejection of unauthenticated writes in Tier-1 paths	Tier-1 paths instrumented.
L4 Canonicalised	Live inventory governed; new pathways gated; regulator-acceptable evidence	Regulator-acceptable evidence.
L5 Federated	Inventory federated across the portfolio; cross-sector signed attestation	Sector-level attestation.

31. Replay & Evidence Design

Captures both accepted and rejected commands at the verification boundary; produces a regulator-grade, signer-attested record reproducible at the relay.

- Capture point: at the verification boundary (relay/IED/PLC), not at the SCADA — captures both accepted and rejected commands.
- Schema: { command_id, issuer_id, signer_id, signature, protocol, payload, freshness_ms, device_state_pre, device_state_post, decision (accepted|rejected), reason, ptp_time }.
- Integrity: signed by the verifying device's key; sealed to an immutable evidence sink (WORM); cross-streamed to the SOC and to the regulator-facing evidence pipeline.
- Replay procedure: any consequential event can be reconstructed at the relay within an SLO of 90 minutes for public-grade output, 24 hours for legal-grade output with signer testimony.
- Forensic SLOs: 100% capture coverage on tier-1 paths; 99% on tier-2; ≤2 s detection of an unauthenticated write; ≤90 minutes to draft a public-grade event reconstruction.

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

“A signed command is the only fence the plant respects.”

“A signed command is the only fence the plant respects.”

“Defend the boundary between the screen and the actuator.”

“If it speaks IEC 61850 and it is not signed, it is unauthenticated.”

“Time is part of the signature.”

“Keys are physical assets that happen to be numbers.”

“The relay attests the command, not the operator.”

Press Wire Drop-Quotes

Benzinga: The Perimeter Doesn't Control The Plant Anymore — Commands Do

Yahoo Finance: Command Is The New Perimeter: A Doctrine For The OT Control Plane

CNBC: Signed Commands Become Table Stakes For Tier-1 Utilities Under New Regulatory Pressure

MarketWatch: Latent Command Pathways Reduced 73% In One Utility Case — Insurer Cuts Retention

Reuters: Continuous Control-Plane Visibility Becomes The New Minimum For Critical Operators

Financial Times: Episodic Visibility Is Institutional Blindness — A Doctrine For The Control Plane

Annex D — Board One-Pager

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

Command Is the New Perimeter

Cryptographic Actuation, DNP3-SA, IEC 62351 and the Boundary Between the Supervisory Data Plane and the Physical Control Plane

> *“A signed command is the only fence the plant respects.”*

- Thesis: cryptographic actuation — not Zero Trust — is the OT perimeter.
- Buy: DNP3-SA + IEC 62351 + substation HSMs + joint key custody.
- Measure: % consequential commands authenticated at the relay (target ≥ 99%).
- Win: relay-level rejection of unsigned writes; insurer retention ↓; regulator exemplar.
- Risk: unsigned legacy IEDs remain the single largest residual exposure.

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