

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

CSAIC Industrial & OT Cyber Doctrine Series · Paper 17 of 20

# The Hydraulic Hammer

*When Cyber Attacks End in Physics — Pressure, Pumps, and Pipeline Integrity*

*“The cyber event ends in physics.”*



## 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: Water | Pipelines | Chemicals | Energy | Insurers | Regulators | Fire and Safety Authorities

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

**[www.kie.ie](http://www.kie.ie) · [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · University of Schiphol (UOS)**

Keywords: Water | Pipelines | Chemicals | IEC 61511 | IEC 62443 | NIS2 | Cyber-Physical Insurance

## 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

Pump and valve manipulation creates destructive pressure transients — the hydraulic hammer — in water, pipeline, and process systems. The damage is physical, expensive, and slow to repair. The doctrine must end the cyber event before it reaches physics.

*“The cyber event ends in physics.”*

### 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 Containment Beats Detection

Detection without containment is a record-keeping exercise. Containment is the defence.

*“Detect, then contain. Or do not detect.”*

### 2.2 Engineering Limits Are the Last Defence

Engineered pressure relief, flow limits, and interlocks are the final defence. Maintain them as cyber controls.

*“Engineering survives the cyber event, or it is not engineering.”*

### 2.3 Telemetry of Transients Is Captured

High-frequency telemetry captures transients. Without it, forensics is guesswork.

*“Capture the transient, or invent it later.”*

### 2.4 Vendor Tuning Is Risk Tuning

Vendor-tuned limits are risk decisions. Govern them.

*“Every tuning is a credit decision.”*

### 2.5 Insurance Reaches Physical Damage

Cyber-driven physical damage is increasingly insurable. Build the evidence.

*“Cyber-physical loss is a claim, with evidence.”*

### 2.6 Joint Drills Include Maintenance

Maintenance teams drill alongside cyber teams. The repair plan is part of the response.

*“Repair plans drill with response plans.”*

### 3. Paper-Specific Adversary Economics

*Tailored to this paper's threat model.*

#### 3.1 Adversary Classes

- State actors targeting physical infrastructure via control-system manipulation.
- Criminal actors targeting water and pipeline systems for ransom.
- Insider abuse during maintenance windows.
- Vendor compromise of tuning parameters.

#### 3.2 Adversary Economics

Cheap to manipulate setpoints; expensive to repair physical damage. Doctrine ends the cyber event before it reaches physics through engineered limits + transient capture + maintenance-joined drills.

#### 3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Transient Asymmetry	Damaging transients are sub-second.	High-frequency telemetry capture
Repair Asymmetry	Repair is weeks; attack is seconds.	Engineered limits as last defence
Tuning Asymmetry	Vendor tuning evades risk review.	Vendor tuning governance

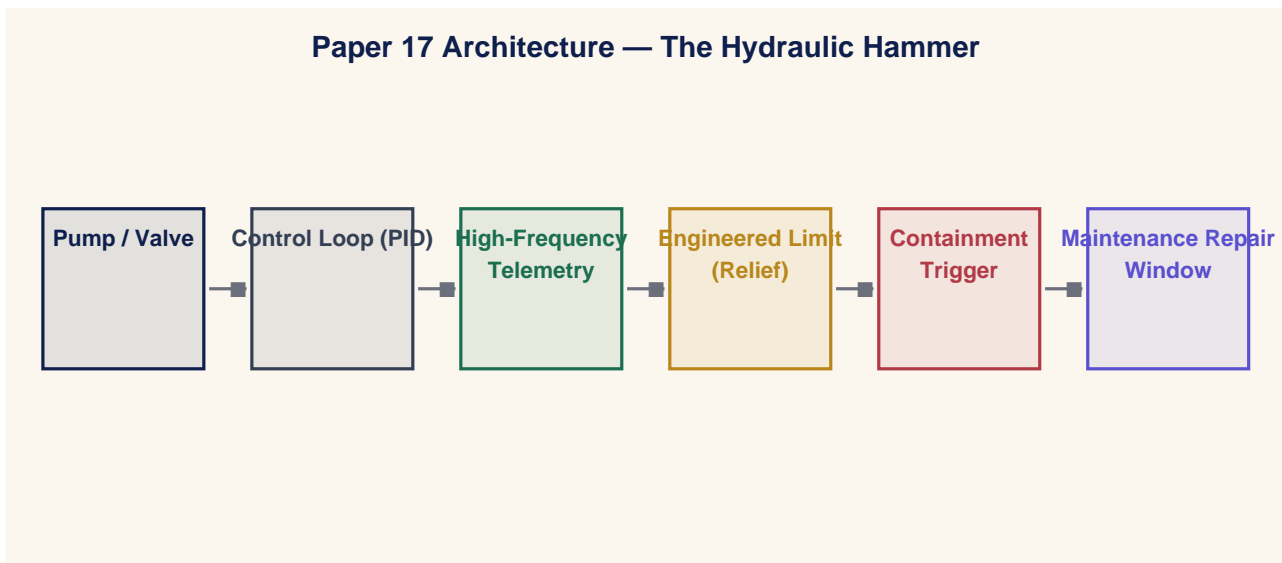
## 4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

### 4.1 Four Operating Layers

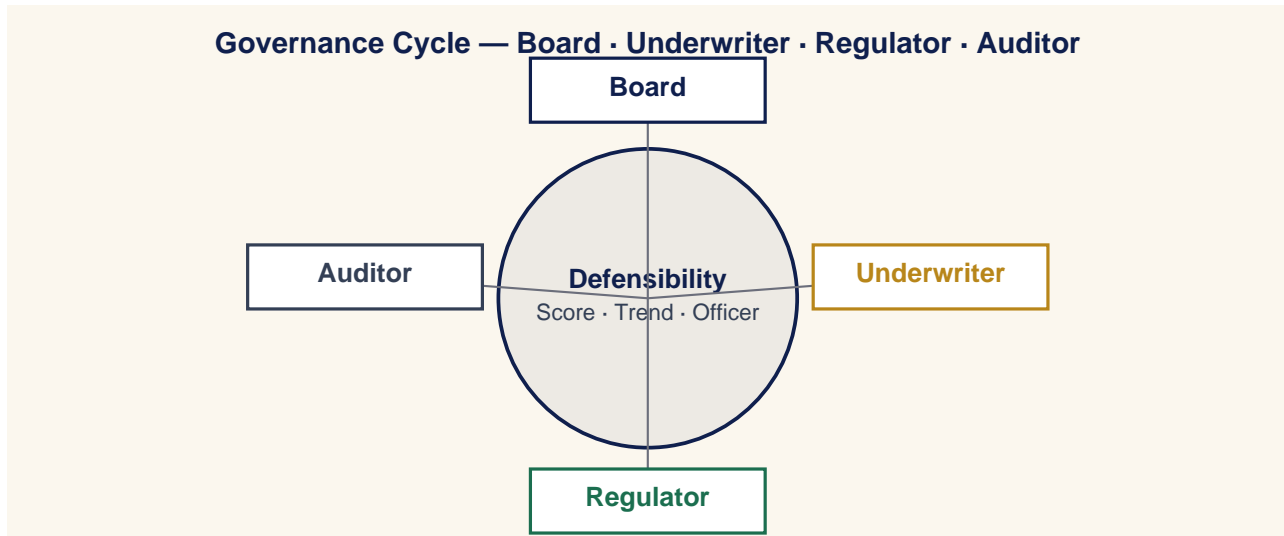
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

### 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.

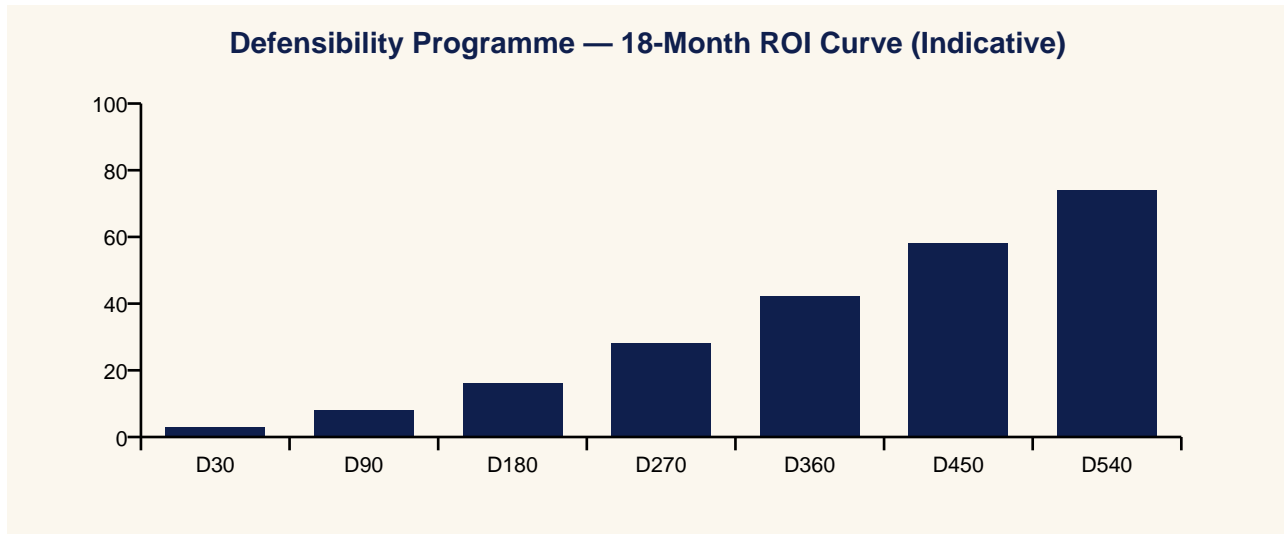


### 5.1 Three Board Questions

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:** Pressure spiked to 14 bar.

**CISO:** Containment activated at 12 bar. The asset survived.

### Setting — Insurer

**Insurer:** Was containment engineered or improvised?

**CISO:** Engineered. Drill records attached.

### Setting — Board

**Director:** Worst case?

**CISO:** A burst main and a 90-day repair.

### Setting — Regulator

**Regulator:** Is this cyber or safety?

**CISO:** Both. We govern them as one.

## 9. Case Study — Anonymised Engagement

### Anonymised Case Study — Water Utility

#### 9.1 Context

A water utility with broad pump and valve exposure and no high-frequency transient capture.

#### 9.2 Intervention

Containment programme: engineered limits, transient capture, vendor tuning governance, joint drills.

#### 9.3 Outcome

Two potential hammer events contained pre-physics; insurer extended physical-damage cover; regulator referenced model in supervisory guidance.

## 10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	Engineered containment coverage on tier-zero assets (target = 100%).	Quarterly	CISO / Plant
M2	High-frequency transient capture coverage (target $\geq$ 95%).	Quarterly	CISO / Plant
M3	Vendor tuning governance coverage (target = 100%).	Quarterly	CISO / Plant
M4	Joint drill cadence with maintenance (target $\geq$ quarterly).	Quarterly	CISO / Plant
M5	Cyber-physical insurance coverage (target $\geq$ defined cap).	Quarterly	CISO / Plant

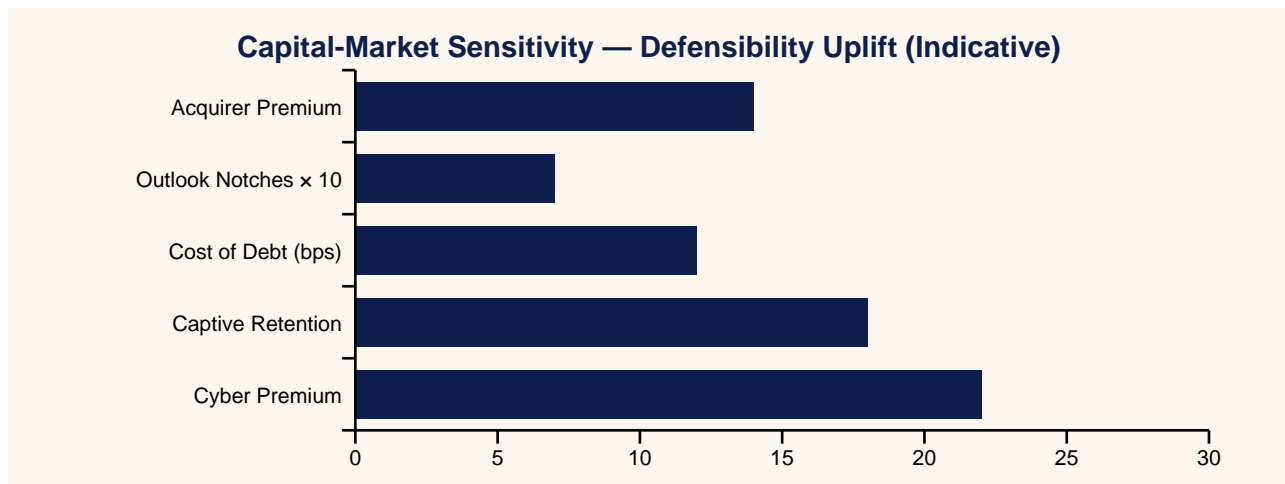
## 11. Implementation Roadmap — Day 1 to Day 540

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 Cyber Event Ends In Physics: Hydraulic Hammer Becomes The New Industrial Risk <span style="float: right;">Headline</span>
Yahoo Finance	Engineered Containment Becomes The Last Defence Against Cyber-Driven Pressure Transients
CNBC	Water Utilities Add High-Frequency Transient Capture As Forensics Requirement
MarketWatch	Insurers Extend Physical-Damage Cover For Operators With Engineered Hydraulic Containment
Reuters	Joint Drills With Maintenance Teams Become Standard For Cyber-Physical Resilience
Financial Times	Detect, Then Contain — Or Do Not Detect: A New Doctrine For Cyber-Physical Defence
Wall Street Journal	Vendor Tuning Of Engineered Limits Now Treated As A Risk Decision
Bloomberg	Pipeline And Chemical Operators Add Cyber-Physical Insurance Lines
Barron's	The Hydraulic Hammer Becomes The Cyber-Physical Risk Headline Underwriters Watch
The Economist	When Cyber Ends In Physics: Pressure, Pumps And Pipeline Integrity

## 13. Investor Brief & Valuation Read



### 13.1 Bloomberg-Style One-Liner

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

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

*“The cyber event ends in physics.”*

*“Detect, then contain. Or do not detect.”*

*“Engineering survives the cyber event, or it is not engineering.”*

*“Capture the transient, or invent it later.”*

*“Every tuning is a credit decision.”*

*“Cyber-physical loss is a claim, with evidence.”*

*“Repair plans drill with response plans.”*

*“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, <del>slight</del> <del>medium</del> command reference where appropriate.	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.

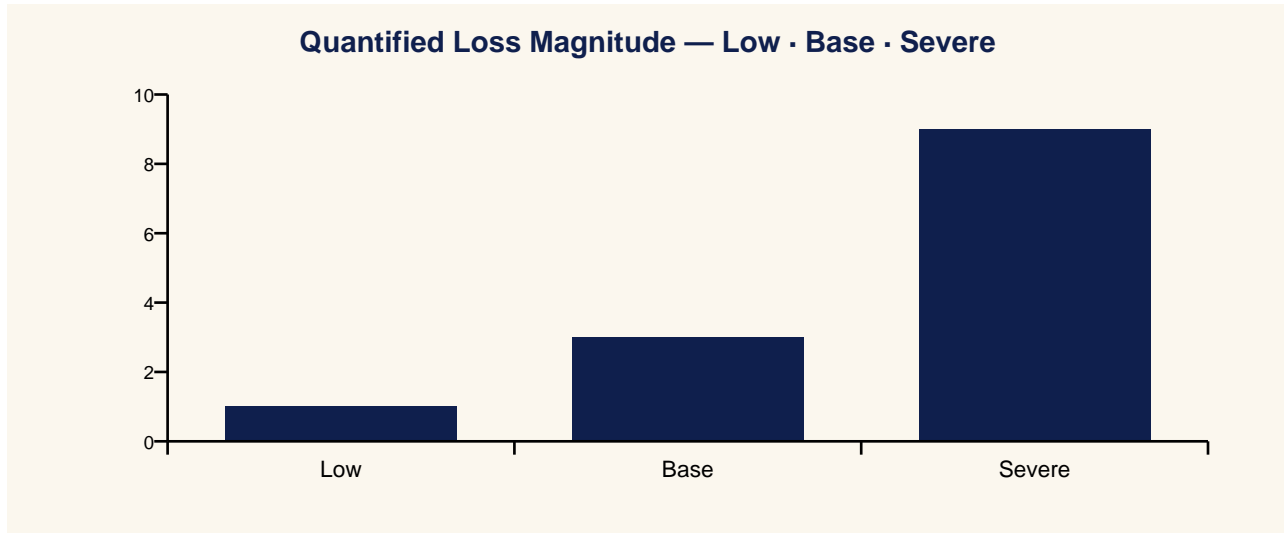
### **Q10 — Where does the doctrine fail?**

See §24.

## 18. Contract Pull-Through & Commercial Engagement Model

- Hydraulic containment programme
- Transient capture architecture
- Vendor tuning governance
- Joint drill with maintenance
- Insurer-aligned physical-damage evidence

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



Scenario	Description	Direct Damage	Repair Time	Customer Impact
Low	Pressure spike contained at 12 bar by engineered relief.	None	Drill repeat	Nil
Base	Burst lateral main; localised damage.	€3-10 m	2-4 wks	Tens of thousands
Severe	Major rupture; multi-week outage.	€50-200 m	8-12 wks	Hundreds of thousands

## 20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0	No engineered containment; vendor tuning un	High exposure.
L1	Engineered limits on critical assets only.	Reactive.
L2	High-frequency transient capture pilot.	Forensic capability.
L3	Engineered containment standard; vendor tuning	Governmental hands cover.
L4	Joint cyber-maintenance drills quarterly.	Sector recognition.
L5	Public attestation of cyber-physical posture.	Regulator exemplar.

## 21. Evidence Artefact Checklist

- Engineered containment coverage on tier-zero assets.
- High-frequency transient capture coverage and last test.
- Vendor tuning governance log.
- Joint drill log (maintenance + cyber).
- Insurer-aligned physical-damage evidence pack.

## 22. Three Anonymised Scenarios

Sector	Pattern	Outcome
Water utility	Broad pump/valve exposure; no transient capture	Containment programme; 2 events contained pre-physics; insurer notified.
Pipeline	Vendor-tuned limits raised silently.	Tuning ECC; vendor on probation; insurer notified.
Chemicals	Maintenance team unaware of cyber-containment triggers	Continually drill cadence.

## 23. Technical Appendix

- Hydraulic transient diagram: setpoint manipulation → control loop response → engineered limit → containment.
- Pump/valve manipulation sequence with PID tuning context.
- Pressure-relief control map (set, response, isolate, drain).
- Repair-cost scenario by asset class.

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

- Fails when engineered limits exist on paper but are not commissioned.
- Fails when maintenance team is not in the drill.
- Fails when forensics rely on second-resolution data.
- Costs: engineered limit refresh, transient capture, joint drill cadence. Payback in single avoided burst main.

## **25. Procurement & Tabletop Packs**

### **25.2 Tabletop / Drill Pack**

1. Drill: setpoint manipulation creates pressure transient.
2. Detect: high-frequency telemetry alarms within 200 ms.
3. Contain: engineered limit isolates affected segment.
4. Recover: maintenance window with joint cyber-maintenance team.
5. Debrief: insurer evidence pack signed within 24h.

## 26. Evidence Basis — External References & Standards Anchors

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

- IEC 61511 (process safety).
- API 754 (process safety performance indicators).
- IEC 62443-3-3 (system security).
- CISA Water Sector Cybersecurity Advisory.
- NIST SP 800-82r3 (OT security).

## 27. Counterargument & Rebuttal

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

Critics argue that hydraulic transients are an engineering problem and that cyber-physical framing inflates the case. The rebuttal is that the engineering control fails if the engineering parameters are mutable by cyber means — which they almost always are. The doctrine restores the parameter as the immutable last defence.

## 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)<sup>2</sup> London.
- Programme Lead, Cyber Security — PRMIA.

Contact: [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie) · [linkedin.com/in/kieranupadrasta](https://www.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

---

*“The cyber event ends in physics.”*

*“Detect, then contain. Or do not detect.”*

*“Engineering survives the cyber event, or it is not engineering.”*

*“Capture the transient, or invent it later.”*

*“Every tuning is a credit decision.”*

*“Cyber-physical loss is a claim, with evidence.”*

*“Repair plans drill with response plans.”*

---

### Press Wire Drop-Quotes

**Benzinga:** The Cyber Event Ends In Physics: Hydraulic Hammer Becomes The New Industrial Risk Headline

**Yahoo Finance:** Engineered Containment Becomes The Last Defence Against Cyber-Driven Pressure Transients

**CNBC:** Water Utilities Add High-Frequency Transient Capture As Forensics Requirement

**MarketWatch:** Insurers Extend Physical-Damage Cover For Operators With Engineered Hydraulic Containment

**Reuters:** Joint Drills With Maintenance Teams Become Standard For Cyber-Physical Resilience

**Financial Times:** Detect, Then Contain — Or Do Not Detect: A New Doctrine For Cyber-Physical Defence

## Annex D — Board One-Pager

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

---

### The Hydraulic Hammer

*When Cyber Attacks End in Physics — Pressure, Pumps, and Pipeline Integrity*

*“The cyber event ends in physics.”*

- Thesis: cyber events end in physics; containment is the defence.
  - Buy: engineered limits + transient capture + joint drills.
  - Measure: engineered containment on tier-zero = 100%; transient capture coverage  $\geq 95\%$ .
  - Win: insurer extends physical-damage cover; regulator-recognised.
  - Risk: vendor tuning silently widens engineered limits.
- 

*Engagement contact: [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie) · University of Schiphol (UOS).*