

SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

WP06 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0

Building Resilient Architectures

SABSA Applied to Critical Infrastructure Protection — NIS2, IEC 62443, and NIST CSF 2.0 for Operational Continuity



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP | MBA | BEng

27 Years' Cyber Security Experience | Big 4 Consulting — Deloitte · PwC · EY · KPMG

21 Years Financial Services & Banking | AI Cyber Security Programme Lead

Professor of Practice — Cybersecurity, AI & Quantum Computing | Schiphol University

Honorary Senior Lecturer, Imperials | Researcher, University College London (UCL)

Lead Auditor, ISF Auditors & Control | ISACA Platinum (London) | (ISC)² Gold (London) | PRMIA Cyber Lead

www.kie.ie | info@kieranupadrasta.com | April 2026

Specialisations: SABSA · NIS2 · ISO 27001:2022 · GDPR · IEC 62443 · NIST CSF 2.0 · DORA · ISO 42001 · Zero Trust · OT Security · M&A
Cyber Due Diligence · Board Reporting

Table of Contents

1. Executive Summary
2. Critical Infrastructure Threat Landscape
3. IEC 62443 Architecture — Zone, Conduit, and Security Level Design
4. NIST CSF 2.0 — Six Functions for Critical Infrastructure
5. IT/OT Convergence Architecture
6. Resilience Architecture — BCM and Disaster Recovery
7. Supply Chain Security Architecture
8. Operational Security Architecture — SOC for Critical Infrastructure
9. NIS2 Essential Entity Architecture Programme
10. Sector Deep Dives: Energy, Water, Transport
11. MITRE ATT&CK for ICS Mapped to SL4 Safety Zones
12. AI-Native Threat Detection for Critical Infrastructure
13. Conclusions and Strategic Recommendations

Executive Summary

11 NIS2 Critical Sectors	SL4 Highest IEC 62443 Security Level	6 NIST CSF 2.0 Functions	72h Max NIS2 Incident Notification
------------------------------------	--	------------------------------------	--

Critical infrastructure resilience is the defining security challenge of the decade. Energy grids, water treatment systems, transportation networks, financial market infrastructure, and healthcare systems face adversaries — nation-state actors, ransomware syndicates, hacktivist collectives — whose capabilities have outpaced the security posture of most critical infrastructure operators. NIS2, IEC 62443, and NIST CSF 2.0 collectively define the regulatory and technical response. SABSA provides the architecture that makes this response coherent, sustained, and operationally effective.

This white paper delivers the architecture doctrine for critical infrastructure resilience. It is written for Security Architects, CISO and Operations Directors in energy, utilities, transport, water, and healthcare sectors — those who must satisfy NIS2 Essential Entity obligations, achieve IEC 62443 security levels, and implement NIST CSF 2.0 across converged IT/OT environments where operational failure carries consequences measured in human safety, not just financial loss.

Critical Infrastructure Architecture Imperatives

NIS2 Article 21: Essential entities must implement "state-of-the-art" security measures — architecture evidence required

IEC 62443: Security Levels SL1–SL4 must be targeted and achieved — zone/conduit architecture is mandatory

NIST CSF 2.0: All six Functions (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER) must be addressed

IT/OT Convergence: The IT/OT interface is the highest-risk architectural boundary in critical infrastructure

Operational Safety: Security architecture must not degrade operational safety — fail-safe design is paramount

Critical Infrastructure Threat Landscape

Critical infrastructure faces a fundamentally different threat landscape than enterprise IT. Adversaries targeting critical infrastructure combine technical sophistication with a willingness to cause physical harm — demonstrated by attacks on the Ukrainian power grid (2015/2016), the Colonial Pipeline ransomware attack (2021), and the Saudi Aramco TRITON/TRISIS safety system attack (2017). These attacks share a common characteristic: they exploited the interface between IT and OT systems, using the IT network as the initial access vector and the OT network as the target.

Threat Actor Taxonomy — Critical Infrastructure

Threat Actor	Capability	Primary Targets
Nation-State APT	Sophisticated; long-dwell; ICS/SCADA knowledge	Power grid; water treatment; defence industrial base

Ransomware Groups	Opportunistic; double-extortion; IT-first lateral movement	Manufacturing; healthcare; logistics; energy distribution
Hacktivists	Moderate capability; politically motivated; DDoS + defacement	Water; government; financial services
Insider Threats	Privileged access; knowledge of OT systems; difficult to detect	Any sector with privileged OT access
Supply Chain	Compromised vendor; software updates; remote access	ICS vendors; SCADA software providers; remote monitoring

MITRE ATT&CK ICS — Critical Infrastructure Kill Chain

MITRE ATT&CK for ICS (Industrial Control Systems) defines the adversary kill chain specific to OT environments. Unlike enterprise ATT&CK, ICS-specific tactics include Engineering Workstation Compromise, Denial of Control, Manipulation of Control, and Damage to Physical Infrastructure. SABSA L5 Operational architecture must integrate ICS ATT&CK detection coverage alongside Enterprise ATT&CK — treating both matrices as mandatory coverage requirements, not optional enhancements.

ICS Kill Chain — SABSA Detection Architecture	
Reconnaissance	OSINT on facility; shodan for exposed OT; supply chain mapping. SABSA L1: Threat intelligence architecture.
Initial Access	Spearphishing; compromised vendor; Internet-exposed HMI. SABSA L3: Internet boundary architecture; VPN/remote access controls.
Lateral Movement (IT)	Credential theft; east-west propagation through IT network. SABSA L3: Micro-segmentation; PAM; east-west inspection.
IT/OT Interface Pivot	Historian server; engineering workstation; remote desktop to OT. SABSA L3: DMZ architecture; data diodes; OT jump server.
OT Execution	ICS protocol commands; logic modification; safety system manipulation. SABSA L4: OT-specific detection; ICS IDS; PLCGuard.
Impact	Process disruption; equipment damage; safety system compromise. SABSA L2: Resilience architecture; fail-safe design; emergency shutdown.

IEC 62443 Architecture — Zone, Conduit, and Security Level Design

IEC 62443 provides the definitive security architecture standard for industrial automation and control systems. Its core architectural concept — the Zone/Conduit model — divides the OT environment into security zones (groups of assets with similar security requirements) and conduits (communication channels between zones). Each zone has a Target Security Level (SL-T) that drives the security requirements for all assets within it. SABSA L3 Physical Architecture formalises and governs this model.

Zone and Conduit Architecture Design

Zone Type	Security Level	SABSA Architecture Response	Key Controls
-----------	----------------	-----------------------------	--------------

Enterprise Zone	SL1	Standard IT security architecture	Perimeter firewall; endpoint protection; IAM
DMZ/Conduit Zone	SL2	IT/OT interface architecture; data diodes	Deep packet inspection; ICS protocol awareness; historian
Operations Zone	SL2	OT operations architecture; jump server	MFA for OT access; OT IDS; patch management for HMI
Control Zone	SL3	Critical control architecture; strict segmentation	Air-gap consideration; no direct internet; hardware authentication
Safety Zone	SL4	Safety system architecture; hardware separation	Physical isolation; formal verification; no software-only controls

Security Level Assessment — Achieved vs. Target

A common failure in IEC 62443 implementations is the gap between Target Security Level (SL-T, the level the organisation wants to achieve) and Achieved Security Level (SL-A, the level currently implemented). This gap is the residual risk that must be managed, mitigated, or accepted at the SABSA L1 risk management layer. SABSA provides the instrument to track SL-T vs. SL-A gaps systematically, prioritise remediation investment, and demonstrate progressive improvement to NIS2 supervisory authorities.

SL Assessment Programme

Initial assessment: Third-party IEC 62443 assessment team evaluates SL-A against SL-T for all zones

Gap register: Each SL gap documented as architecture remediation item — priority based on safety impact

Remediation architecture: SABSA L3/L4 remediation design for each gap — not just control selection

Annual reassessment: SL-A verified annually — progressive improvement demonstrated to NCA under NIS2

NIST CSF 2.0 — Six Functions for Critical Infrastructure

NIST Cybersecurity Framework 2.0, released February 2024, introduces a sixth Function — GOVERN — which addresses cybersecurity governance, risk management strategy, and supply chain risk. For critical infrastructure operators, the GOVERN Function is the architectural foundation that makes the other five Functions coherent: without governance, IDENTIFY produces an asset register with no ownership; PROTECT produces controls with no accountability; DETECT produces alerts with no authority to act; RESPOND produces playbooks with no mandate; RECOVER produces plans that are never exercised.

NIST CSF 2.0 — Six Functions, SABSA Layer Mapping

GOVERN (GV)

Cybersecurity governance, risk management strategy, supply chain risk, oversight. SABSA L0–L1: BAP, risk model, ARB, Board governance.

IDENTIFY (ID)	Asset management, business environment, risk assessment, improvement planning. SABSA L0–L2: Asset architecture, criticality classification.
PROTECT (PR)	Identity management, access control, awareness, data security, platform security. SABSA L2–L4: Logical through component security architecture.
DETECT (DE)	Continuous monitoring, adverse event analysis. SABSA L5 Operational: SIEM, OT IDS, anomaly detection architecture.
RESPOND (RS)	Incident management, analysis, mitigation, reporting. SABSA L5: IR playbooks, NIS2 reporting architecture, crisis comms.
RECOVER (RC)	Recovery planning, improvement, communications. SABSA L2+L5: BCM architecture, DR runbooks, lessons learned integration.

CSF 2.0 Subcategory Architecture Mapping

CSF 2.0 Category	SABSA Architecture Response	NIS2 Art.21 Alignment
GV.RM: Risk Management	L1: BAP risk model; monetised risk register; Board-approved appetite	Art.21(a): Risk analysis and information system security
GV.SC: Supply Chain Risk	L1: TPRM trust model; supplier minimum security architecture	Art.21(d): Supply chain security
ID.AM: Asset Management	L0–L2: Asset register; criticality classification; CMDB integration	Art.21(a): Information asset inventory
PR.AA: Access Control	L2–L3: IAM architecture; PAM; MFA; least privilege	Art.21(i): Human resources security and access control
PR.DS: Data Security	L3–L4: Encryption; DLP; data classification; key management	Art.21(h): Cryptography; Art.21(i) data protection
DE.CM: Continuous Monitoring	L5: SIEM + OT IDS; unified SOC; anomaly detection	Art.21(b): Incident handling detection capability
RS.MA: Incident Management	L5: IR playbooks; NIS2 Art.23 notification workflow	Art.21(b) + Art.23: Incident handling and reporting
RC.RP: Recovery Planning	L2+L5: BCM architecture; DR runbooks; tested recovery	Art.21(c): Business continuity

IT/OT Convergence Architecture

The convergence of IT and OT networks is the defining architectural challenge for critical infrastructure operators. Historically, OT networks operated in isolation — air-gapped from enterprise IT and the internet. Today, operational efficiency demands, remote monitoring requirements, and supply chain connectivity have collapsed this isolation in most environments. The SABSA architecture model provides the framework for managed, secure IT/OT convergence — maintaining the operational integrity of OT systems while enabling the business benefits of connectivity.

IT/OT Convergence Architecture Principles

1. **Governance Unification:** Single SABSA L0 governance framework applies across IT and OT — unified risk appetite, policy hierarchy, and Board accountability. No separate "OT security team" that reports outside the CISO structure.

2. **Architecture Separation:** SABSA L2–L4 maintains strict domain separation between IT and OT architectures. The logical security domains, physical network zones, and component specifications are distinct — governed by the same framework but designed independently.
3. **Interface Control:** The IT/OT interface (DMZ/Conduit Zone) is the most architecturally critical element. Every protocol, every data flow, and every access path through the interface must be explicitly designed, justified, and monitored.
4. **OT-First Safety:** Security architecture must not compromise operational safety. Fail-safe design — where security controls fail to a safe operational state rather than a secure but non-operational state — is mandatory for safety-critical OT systems.
5. **Operational Continuity Priority:** OT architecture availability requirements typically exceed enterprise IT (99.999% uptime for power grid control systems vs. 99.9% for enterprise applications). Security controls must be designed to this availability standard.

Architecture Domain	IT (Enterprise)	OT (Industrial)
Primary Driver	Information security and compliance	Operational safety and availability
SABSA Primary Layer	L2–L4 (enterprise security domains)	L3 Physical (IEC 62443 zone/conduit)
Patching Cadence	Monthly/on-demand	Annual outage window — major constraint
Authentication	MFA; SSO; cloud identity	Local authentication; hardware tokens; operational constraints
Encryption	TLS 1.3 everywhere	Selected protocols only — latency constraints on safety-critical data
Monitoring	SIEM — enterprise ATT&CK	OT IDS (Clarity/Dracos) — ICS ATT&CK matrix
Incident Response	Standard IR playbook — hours	OT IR — minutes for safety-critical; controlled isolation

Resilience Architecture — BCM and Disaster Recovery

NIS2 Article 21(c) mandates business continuity management and ICT continuity for essential entities. For critical infrastructure operators, this obligation is existential — a power grid that cannot restore within 24 hours, or a water treatment system that cannot recover from a cyber incident within hours, poses immediate public safety risks. SABSA resilience architecture designs recovery capability into the system from the outset, not as an afterthought.

Resilience Architecture Design Targets

Infrastructure Type	RTO Target	RPO Target	Resilience Architecture Pattern
Safety-Critical OT (SL4)	<15 minutes	<1 minute	Active-active; hardware redundancy; no software-only failover
Critical Control (SL3)	<1 hour	<5 minutes	Active-active; warm standby; automated failover

Operations Technology (SL2)	<4 hours	<30 minutes	Warm standby; manual failover; daily snapshot
Enterprise IT (SL1/NIS2)	<24 hours	<4 hours	Cold standby; DR site; tested quarterly
Data/Analytics	<48 hours	<24 hours	Backup and restore; cloud-based DR; monthly test

Cyber Crisis Architecture — Incident to Recovery

Critical Infrastructure Incident Response Architecture

Phase 1 — Detect: OT IDS alert + SIEM correlation → automated severity classification → SOC analyst notification (target: <5 minutes)

Phase 2 — Contain: Automated isolation of affected zone(s) → operational safety assessment → emergency shutdown if safety risk (target: <15 minutes)

Phase 3 — Notify: NIS2 Art.23 early warning (24h) → operational emergency services notification → Board CISO briefing (target: <2 hours)

Phase 4 — Recover: Recovery runbook execution → OT system restoration → operational testing → controlled return to service

Phase 5 — Report: NIS2 Art.23 72h notification → ENISA cross-border coordination → Post-Incident Review → architecture update

Supply Chain Security Architecture

Critical infrastructure supply chain security — addressing NIS2 Article 21(d) and the NIST CSF 2.0 GV.SC category — requires an architecture model that extends beyond the enterprise perimeter to encompass the security posture of every significant supplier, vendor, and technology provider. The 2020 SolarWinds attack demonstrated that the most sophisticated adversaries now routinely use supply chain compromise as their preferred initial access vector.

Supply Chain Architecture Trust Model

Supply Chain Layer	SABSA Architecture Requirement
Tier 1: Critical OT Vendors	Full IEC 62443 SL assessment; architecture review; TLPT-equivalent testing; contractual minimum security architecture
Tier 2: OT Support Vendors	Simplified IEC 62443 assessment; secure remote access architecture; annual questionnaire + on-site verification
Tier 3: IT Service Providers	ISO 27001/NIS2-compliant assessment; standard contractual provisions; 18-month review cycle
Tier 4: Software Providers	SBOM (Software Bill of Materials) requirement; vulnerability disclosure programme; patch SLA contractual requirement
Tier 5: Hardware Manufacturers	Hardware security assurance; supply chain integrity documentation; country-of-origin risk assessment

Operational Security Architecture — SOC for Critical Infrastructure

Critical infrastructure SOC architecture differs fundamentally from enterprise IT SOC design. The monitoring tool stack must include OT-specific capabilities (Claroty, Dragos, Nozomi Networks) alongside enterprise SIEM. The analyst team must have OT/ICS knowledge alongside cybersecurity skills. Incident response playbooks must integrate with operational safety procedures. And the SOC must operate under SLAs calibrated to operational reality — a five-minute response time for a safety-critical OT alert, not the four-hour P1 SLA appropriate for an enterprise application outage.

<5min OT Critical Alert Response	24/7 SOC Availability Requirement	70%+ ICS ATT&CK Coverage Target	2 Analyst Roles: IT + OT
---	---	---	------------------------------------

Unified SOC Architecture — IT/OT Integration

SOC Capability	IT Domain Tool	OT Domain Tool
Asset Discovery	CrowdStrike Falcon; Microsoft Defender	Claroty; Dragos; Nozomi
Threat Detection	Splunk/Sentinel SIEM; EDR	OT IDS with ICS protocol awareness
Vulnerability Management	Tenable; Qualys	Claroty; Dragos vuln module
Incident Response	Standard IR platform; playbooks	OT-specific IR; engineering team integration
Threat Intelligence	MITRE ATT&CK Enterprise; commercial TI	MITRE ATT&CK ICS; sector-specific ISACs

NIS2 Essential Entity Architecture Programme

NIS2 essential entities face proactive supervisory oversight, higher fine thresholds, and mandatory notification obligations that require operational infrastructure — not just policy documents. The architecture programme for NIS2 essential entity compliance is an 18-24 month structured programme that delivers five architecture outcomes: risk architecture, technical measures, incident reporting capability, supply chain security, and Board governance.

Programme Phase	Duration	Architecture Deliverable	NIS2 Obligation Addressed
Phase 1: Governance	Months 1–3	L0: BAP; risk appetite; ARB charter; Board training programme	Art.20: Management body accountability
Phase 2: Risk Architecture	Months 2–6	L1: Risk model; threat model; NIS2 scope assessment; TPRM framework	Art.21(a): Risk analysis measures
Phase 3: Technical Architecture	Months 4–12	L2–L4: Logical domains; IT/OT interface; IEC 62443 zones; component specs	Art.21(b)–(j): Technical security measures

Phase 4: Operational Architecture	Months 10–18	L5: SOC; IR playbooks; NIS2 notification workflow; monitoring architecture	Art.21(b): Incident handling; Art.23: Reporting
Phase 5: Assurance	Months 15–24	Architecture audit; penetration testing; TLPT (if required); NCA engagement	Art.32: Supervisory examination readiness

Sector Deep Dives: Energy, Water, Transport

Critical infrastructure is not monolithic. Energy, water, and transport sectors face distinct threat vectors, operational constraints, and regulatory requirements. This section provides architecture blueprints specific to each sector — translating IEC 62443, NIS2, and NIST CSF into sector-specific security levels, controls, and resilience patterns.

Energy Sector: SCADA Protection at SL3-SL4

Architecture Element	Security Level	IEC 62443 Controls	Regulatory Driver
Generation Control System	SL4	Formal verification; hardware security; air-gap isolation	NERC CIP (US); NIS2 Art.21 (EU)
Transmission SCADA	SL3	Encrypted command channels; DNP3 secure; cryptographic device auth	NIS2 Essential Entity; IEC 62443 SL3 target
Distribution OT	SL2	Historian on DMZ; read-only ICS data bridge; ICS IDS	NIS2 Operator; regional regulation
Field Devices (RTUs)	SL2–SL3	SCADA protocol security; modbus-over-TLS; hardened firmware	Distributed deployment; vendor standardisation

Water Sector: Telemetry Integrity and Quality Assurance

Architecture Element	Security Requirement	SABSA Control Pattern	Operational Impact
Quality Monitoring	Sensor integrity; anomaly detection	Redundant sensors; cryptographic verification; fail-safe block	No contaminated water reaches customers
Remote SCADA	Encrypted telemetry; MFA for operator access	Dedicated VPN; hardware tokens; session recording	Real-time visibility; <2min response to anomaly
Chemical Dosing	Logic integrity; injection prevention	DCS isolation; hardware authentication; logical verification	Precise chlorine/chemical dosing; no overdose risk
Backup/Failover	48-hour manual operation capability	Twin treatment lines; backup chemicals; operator training	Continuous supply during OT system outage

Transport Sector: Signalling System Resilience (SIL4)

Architecture Element	Safety Integrity Level	SABSA Architecture	Recovery Target
Train Spacing Logic (CBTC)	SIL4	Cryptographic command integrity; fail-to-stop on auth failure	Emergency brake within 2 seconds of attack detection
Operational Control Centre	SIL3 (safety-critical signals)	Dispatcher smartcard auth; no external connectivity; all commands logged	Zero unauthorised timetable changes; forensic record
Track Geometry / Position	SIL3	Redundant sensors (GPS + ground radar); cryptographic verification	Position anomaly detected and blocked within 1 train cycle
Maintenance Access	SIL2 (asset/supply chain)	Firmware signing; dual approval before deployment; spare parts chain-of-custody	Zero unauthorised firmware; 100% spare parts authenticity

MITRE ATT&CK for ICS Mapped to SL4 Safety Zones

MITRE ATT&CK for Industrial Control Systems provides the adversary kill chain for OT environments. Unlike enterprise ATT&CK, ICS tactics include Engineering Workstation Compromise, Denial of Service (impacts safety, not just availability), and Damage to Physical Infrastructure. SABSA SL4 safety zone architecture must map each MITRE ICS tactic to detection and mitigation points, with particular focus on the IT/OT interface where adversaries cross into critical systems.

ICS Tactics to Purdue Model Mapping

MITRE ICS Tactic	Purdue Level Entry	SABSA Detection Zone
Engineering Workstation Compromise	Level 3 (SCADA)	DMZ historian monitoring; anomalous historian queries; engineering tool execution tracking
Lateral Movement in OT	Level 2 (Supervisory Control)	ICS IDS monitoring inter-zone traffic; protocol anomaly detection; command signature validation
Denial of Service (OT-Specific)	Level 1 (Process/Safety)	Process anomaly detection (sensor readings); state machine verification; safety system watchdog
Logic/Parameter Modification	Level 1	Safety system integrity checking; PLCGuard (PLC firmware integrity); redundant execution
Manipulation of Physical Processes	Level 0 (Field Devices)	Physical process monitoring; independent sensor verification; safety interlock monitoring

Kill Chain Interruption at Each Security Level

ICS Kill Chain Interruption Architecture

L5 (Enterprise IT)	Reconnaissance; initial access through enterprise network. Detection: EDR; SIEM; email security. Interruption: Credential protection; endpoint hardening.
L4 (IT/OT DMZ)	Lateral movement into OT; historian access; HMI compromise. Detection: Historical data anomaly; ICS protocol deviation. Interruption: Data diode; historian read-only; PLC firmware lock.
L3 (SCADA/Supervisory)	SCADA command injection; setpoint manipulation. Detection: Command signature anomaly; state machine deviation. Interruption: Command signing; hardware MFA.
L2 (Safety-Critical)	Logic modification; safety system bypass attempt. Detection: Safety system integrity check; firmware signature verification. Interruption: Hardware security module; formal verification.
L1 (Field Devices)	Physical device compromise; sensor manipulation. Detection: Redundant sensor verification; physical intrusion detection. Interruption: Physical isolation; air-gap activation.

AI-Native Threat Detection for Critical Infrastructure

Traditional rule-based OT IDS is brittle — it detects known attacks but fails on novel variants. AI-native threat detection for critical infrastructure uses autonomous agents for OT-specific anomaly detection, process-aware model deviation alerting, and automated isolation protocols. Machine learning models trained on baseline process telemetry (temperature, pressure, flow rate, equipment state) detect deviations that rule-based systems miss.

Autonomous OT Anomaly Detection Architecture

Detection Component	Data Source	Anomaly Type
Process Baseline ML Model	SCADA process parameters (temperature, pressure, flow)	Deviation >3 std dev from baseline; unexpected transitions
Equipment State Machine	Equipment operational state; mode transitions	Unexpected state change; logic sequence violation
Network Traffic Profiling	ICS protocol flows; packet size/timing; command frequency	Protocol anomaly; command rate spike; unexpected device talking
Anomalous Isolation Protocol	Consensus across 3+ detection models	Multiple anomaly signals from different models (>2 independent detectors)

ML Model Governance for Safety-Critical OT

AI Model Validation Requirements for SL4 Systems

Baseline establishment: 30-day operational baseline collection before ML model deployment; capture all normal operational modes (startup, ramp, shutdown, switching)
 Validation testing: 90-day supervised deployment (parallel to rule-based IDS); validate no false negatives in known attack scenarios

False positive tolerance: <0.1% for SL4 systems (1 false alarm per 1000 normal operations maximum)

Retraining schedule: Quarterly model refresh with new baseline data; version control of all model artifacts

Explainability requirement: All automated isolation triggers must include feature attribution explaining which parameters deviated

Conclusions and Strategic Recommendations

Critical infrastructure resilience under NIS2, IEC 62443, and NIST CSF 2.0 requires an architecture-led approach. The stakes — operational safety, public welfare, national security — demand more than compliance checkboxes. They demand architectures designed to operate under adversarial conditions, recover from attacks, and demonstrate progressive security improvement to supervisory authorities.

1. Commission an IEC 62443 Zone/Conduit architecture assessment: map all OT assets to security zones, determine Target Security Levels, assess Achieved Security Levels, and prioritise remediation by safety impact.
2. Implement the IT/OT interface architecture: every protocol, data flow, and access path through the IT/OT boundary must be explicitly designed, monitored, and justified — no undocumented paths.
3. Deploy OT-capable SOC: enterprise SIEM alone is insufficient for critical infrastructure monitoring — OT IDS with ICS protocol awareness is mandatory for detecting adversary activity in OT environments.
4. Build the NIS2 Art.23 incident reporting pipeline: automated severity classification, notification workflow, and evidence package assembly are operational capabilities, not manual processes.
5. Develop tested recovery runbooks for all critical OT systems: BCM architecture is only as good as the last test — quarterly OT recovery exercises are the standard.
6. Establish supply chain security architecture: Tier 1 critical OT vendors require full IEC 62443 SL assessment and contractual minimum security architecture schedules.

Critical Infrastructure Resilience Architecture Outcomes

- ✓ NIS2 Essential Entity compliance: architecture evidence across all Art.21 categories
- ✓ IEC 62443 SL targets achieved: zones defined, conduits controlled, security levels validated
- ✓ NIST CSF 2.0 six Functions implemented: GOVERN through RECOVER operationally active
- ✓ IT/OT interface controlled: every cross-domain path designed, monitored, and evidenced

About the Author

27 Years Cyber Security	21 Years Financial Services	4 Big 4 Firms	6 Global Certifications
-----------------------------------	---------------------------------------	-------------------------	-----------------------------------

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is one of Europe's foremost Enterprise Security Architects, with 27 years' cyber security experience spanning Big 4 consulting — Deloitte, PwC, EY, and KPMG — and 21 years in Financial Services and Banking. He is recognised globally as a practitioner-researcher whose work bridges theoretical security architecture doctrine and operational enterprise programme delivery at the highest levels of regulated industry. His white papers are cited by national regulators, procurement bodies, and architecture review boards as reference-grade doctrine for enterprise security programme design.

Mr. Upadrasta has over 27 years' experience of business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management. He has worked with the largest corporations globally to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI-DSS, SAS 70, DORA, NIS2, GDPR, and the EU AI Act. His security architecture practice consistently delivers contract-winning, board-ready security programmes that command immediate regulatory and procurement confidence across all tiers of regulated enterprise — from FTSE 100 to sovereign wealth, from critical infrastructure operators to global systemically important financial institutions.

As Professor of Practice at Schiphol University and Honorary Senior Lecturer at Imperials, he trains the next generation of enterprise architects and security programme leads. His research at University College London spans AI governance, post-quantum cryptographic migration, and zero-trust deployment frameworks for critical infrastructure sectors under NIS2 and DORA obligations.

Academic & Research Appointments

Institution / Role	Details
Schiphol University	Professor of Practice — Cybersecurity, AI & Quantum Computing
Imperials	Honorary Senior Lecturer — Enterprise Security Architecture
University College London (UCL)	Researcher — Cyber Risk, AI Governance, Quantum Security
ISF Auditors and Control	Lead Auditor — ISO 27001 / NIS2 / DORA Assurance

Professional Memberships & Recognition

Organisation	Membership / Role
ISACA — London Chapter	Platinum Member

(ISC)² — London Chapter	Gold Member
PRMIA	Cyber Security Programme Lead
SABSA Institute	Accredited Practitioner & Author
ISF	Lead Auditor

Core Specialisations

- SABSA Enterprise Security Architecture — all six layers: Contextual through Operational
- DORA (EU 2022/2554) — ICT Risk Management, Incident Reporting, TLPT, Third-Party Risk
- NIS2 Directive (EU 2022/2555) — Essential & Important Entity Compliance Architecture
- ISO/IEC 27001:2022 — ISMS Design, Implementation, Certification & Internal Audit
- ISO/IEC 42001:2023 — AI Management Systems Governance for Regulated Enterprises
- GDPR — Data Protection by Design, DPIA, Article 32 Technical & Organisational Measures
- IEC 62443 — OT/ICS Security Architecture, Zone/Conduit Design, Security Levels SL0–SL4
- NIST CSF 2.0 — Enterprise Risk Management & Security Posture across six Functions
- Zero Trust Architecture (NIST SP 800-207) — Enterprise-Scale Deployment & Governance
- Post-Quantum Cryptography — NIST FIPS 203/204/205, Cryptographic Agility Frameworks
- M&A Cyber Due Diligence — Architecture Integration Cost Estimates, Security Assessment
- Board Reporting — Executive Cyber Risk Communication, Business Attribute Profiles

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

References & Standards

- [1] SABSA Institute. SABSA Framework White Papers and Practitioner Guides. <https://sabsa.org>, 2024.
- [2] European Parliament. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2). OJ L 333, December 2022.
- [3] ISO/IEC. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization, 2022.
- [4] IEC. IEC 62443 Series — Security for Industrial Automation and Control Systems. Parts 1-1 through 4-2. IEC, 2018–2023.
- [5] NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, February 2024.
- [6] European Parliament. Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, L 119, April 2016.
- [7] NIST. Zero Trust Architecture, Special Publication 800-207. National Institute of Standards and Technology, August 2020.
- [8] European Parliament. Regulation (EU) 2022/2554 — Digital Operational Resilience Act (DORA). OJ L 333, January 2023. Effective January 2025.
- [9] ISO/IEC. ISO/IEC 42001:2023 — Artificial Intelligence Management Systems. International Organization for Standardization, December 2023.
- [10] NIST. AI Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, January 2023.
- [11] European Commission. Regulation (EU) 2024/1689 — Artificial Intelligence Act. Official Journal, July 2024.
- [12] NIST. FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.
- [13] NIST. FIPS 204 — Module-Lattice-Based Digital Signature Standard. August 2024.
- [14] NIST. FIPS 205 — Stateless Hash-Based Digital Signature Standard. August 2024.
- [15] ENISA. NIS2 Directive: Mapping to Technical Measures and Good Practices. ENISA, 2023.
- [16] ENISA. Cybersecurity of AI and Standardisation. European Union Agency for Cybersecurity, March 2023.
- [17] MITRE Corporation. MITRE ATT&CK Enterprise Framework v15. <https://attack.mitre.org>, 2024.
- [18] Cloud Security Alliance. Zero Trust Advancement Center — Enterprise Deployment Guide. CSA, 2024.
- [19] NCSC UK. Guidelines for Secure AI System Development. National Cyber Security Centre, 2024.
- [20] Upadrasta, K. SABSA Architecture Doctrine for Regulated Enterprises. www.kie.ie, 2026.