

ARCHITECTURAL TECHNICAL DEBT AS A SOURCE OF SYSTEMIC CYBER RISK IN CRITICAL DIGITAL INFRASTRUCTURE

Cornelius Chipasha, Simon Tembo and Mulundumina Shimaponda

University of Zambia, Zambia

Emails: {corneliuschipasha41@gmail.com, simon.tembo@unza.zm,
mulundumina.shimaponda@unza.zm}

Received 29 June 2026 - Accepted 17 August 2026 - Published 23 September 2026

ABSTRACT

Critical digital infrastructure (CDI) faces a category of cyber risk that is structurally embedded rather than operationally introduced. Existing cybersecurity approaches concentrate primarily on known vulnerabilities, patch compliance, and incident response, while giving limited attention to accumulated architectural deficiencies as enablers of systemic risk. Using a structured literature synthesis and conceptual framework-development methodology, this paper conceptualizes Architectural Technical Debt (ATD) as the aggregate of deferred structural decisions, inherited legacy constraints, and design-era compromises that progressively increase system complexity, erode trust boundaries, and amplify cyber risk in operational technology and CDI environments. Four principal outputs are developed: a six-category ATD taxonomy; a six-proposition risk-amplification framework and seven-stage causal model; a five-level Architectural Technical Debt Maturity Model and practitioner assessment matrix; and an Architectural Technical Debt Index formulation for future quantification. The proposed constructs are aligned with IEC 62443, NIST guidance, and MITRE ATT&CK for ICS. No empirical or experimental results are presented; the propositions, weights, thresholds, and maturity levels constitute a conceptual foundation requiring future validation through industrial case studies, digital-twin simulations, and longitudinal analysis. The framework provides operators, regulators, and policymakers with a structured basis for recognizing and governing architecture-induced cyber risk, particularly in resource-constrained critical-infrastructure environments.

Keywords: (Architectural technical debt; critical digital infrastructure; systemic cyber risk; operational technology security; legacy systems; cyber resilience; architecture-first security)

1. INTRODUCTION

1.1. BACKGROUND

Critical digital infrastructure, energy grids, water distribution systems, transportation networks, healthcare delivery platforms, and financial market infrastructure constitute the operational backbone of modern economies and sovereign functions. These systems share a defining characteristic: they were largely designed and deployed in technological eras fundamentally different from the contemporary threat landscape. Power generation control systems installed in the 1990s, water treatment SCADA platforms procured before the widespread adoption of TCP/IP networking, and railway signaling architectures built on

proprietary serial protocols are not historical curiosities; they are active operational assets, often expected to remain in service for decades beyond their original design horizons.

The security implications of this reality are profound. Long asset lifecycles produce systems whose architectural assumptions, trust models, communication protocols, segmentation philosophies, and observability capabilities reflect conditions that no longer obtain. These systems were frequently designed with the assumption of air-gapping as a primary security control, an assumption that progressive digitization, remote monitoring requirements, and supply chain integration have systematically eroded. The result is a vast installed base of operational technology whose architecture is structurally misaligned with contemporary threat models.

Simultaneously, the threat environment targeting critical digital infrastructure has evolved from opportunistic intrusion to targeted, nation-state-level offensive operations. The Colonial Pipeline ransomware incident of 2021 demonstrated that infrastructure operators could be compelled to voluntarily shut down operational systems to contain a cyber incident, producing cascading fuel supply disruptions across the eastern United States. The Transnet cyberattack in South Africa the same year disrupted port operations across Durban, Cape Town, Port Elizabeth, and Richards Bay for weeks, illustrating that the compounded effects of aging OT infrastructure and constrained security investment capacity make emerging-economy operators acutely exposed. Ukraine experienced repeated, sophisticated attacks against its electricity distribution infrastructure, beginning in 2015, that exploited architectural weaknesses in SCADA architectures to achieve physical operational disruption. What these incidents share is not merely the presence of software vulnerabilities but the presence of architectural conditions, flat networks, implicit trust relationships, insufficient observability, and deferred modernization that transformed exploitable weaknesses into systemic failures.

1.2. PROBLEM STATEMENT

The dominant paradigm in operational technology cybersecurity has been vulnerability-focused: identify known weaknesses in software and firmware, apply available patches where operationally feasible, and implement compensating controls where patching is not possible. This orientation, while necessary, is insufficient. A flat network architecture that permits unrestricted lateral movement between engineering workstations and process control devices is not a vulnerability in the conventional sense; it is an architectural characteristic that multiplies the impact of every vulnerability present within its scope. These architectural characteristics represent accumulated technical debt, structural liabilities whose cost is paid not in development time but in systemic cyber risk. Despite substantial scholarly attention to technical debt in software engineering, its manifestation in critical digital infrastructure, what this paper terms Architectural Technical Debt (ATD), has received no systematic treatment. This gap is consequential: without a formal conceptualization of ATD, operators lack the analytical vocabulary to articulate, measure, and govern a category of risk that is structurally embedded in their environments.

1.3. RESEARCH OBJECTIVES

This paper pursues the following objectives:

1. To conceptualize ATD as a distinct category of cyber risk in critical digital infrastructure, distinguishing it from conventional vulnerability-based risk frameworks.
2. To identify and characterize the primary sources through which ATD accumulates in operational technology environments.
3. To develop a structured six-category taxonomy of ATD.
4. To construct a formal risk amplification framework with testable propositions connecting ATD to systemic cyber risk.
5. To propose evidence-informed strategies for ATD recognition, management, and reduction.

6. To introduce an Architectural Technical Debt Maturity Model and ATDI formulation to support future measurement research.

1.4. CONTRIBUTIONS

The principal contributions of this paper are:

1. A formal definition of ATD as applied to critical digital infrastructure, grounded in technical debt theory.
2. A six-category ATD taxonomy providing a structured basis for assessment and governance.
3. A Formal Risk Amplification Framework comprising six testable propositions (P1-P6) connecting ATD to operational disruption.
4. A seven-stage ATD-Induced Systemic Cyber Risk conceptual model.
5. An Architectural Technical Debt Maturity Model (L1-L5) for organizational ATD governance.
6. An ATD Assessment Matrix providing practitioners with qualitative and quantitative assessment tools.
7. An Architectural Technical Debt Index (ATDI) formulation providing a weighted composite metric for future empirical research.

The scope of this paper is diagnostic and framework-building. Readers seeking a target-state architectural blueprint for CDI security, including layered trust mediation and post-quantum cryptographic orchestration, are directed to published reference architectures for CDI security, including the cyber-physical zero trust architecture framework proposed by Feng and Hu [38]. The present paper provides the structural pathology that explains why such target-state architectures are necessary and how accumulated architectural debt undermines their adoption.

2. RELATED WORK

This section surveys the existing literature across the four domains from which ATD in critical digital infrastructure draws: software engineering technical debt, enterprise IT and cloud architecture debt, industrial control systems security, and the nascent intersection of technical debt and OT/ICS environments. The literature search followed a structured methodology drawing on established systematic literature review guidance [39]. The search was conducted in March 2025 across four databases: IEEE Xplore, ACM Digital Library, Scopus, and Web of Science. Two search string clusters were used: Cluster 1 ("technical debt" OR "architectural debt" OR "design debt") AND ("industrial control systems" OR "OT security" OR "critical infrastructure" OR "SCADA" OR "cyber-physical"); and Cluster 2 ("cyber risk" OR "systemic risk") AND ("architectural debt" OR "legacy systems"). The search was limited to English-language peer-reviewed sources published from 2010 to 2025. After duplicate removal across databases, title-and-abstract screening of the combined results produced a candidate set; full-text review against inclusion criteria (direct relevance to technical debt theory, ICS/OT security, or cyber risk governance) identified the peer-reviewed sources included in this paper. Foundational and theoretically relevant sources outside the principal database-search period, including Cunningham (1992), Perrow (1984), von Bertalanffy (1968), Trist and Bamforth (1951), Hollnagel et al. (2006), Leveson (2011), and Howard and Pincus (2003), were identified through backward citation searching from included records and added on the basis of theoretical relevance. Standards documents (IEC 62443, NIST SP 800-82, NIST SP 800-207, NIST CSF 2.0, CISA 2023) and the MITRE ATT&CK for ICS framework were included as grey literature given their normative authority in the field. Sources were excluded where they addressed technical debt solely as a code-quality issue without architectural relevance, discussed general cybersecurity without an OT, CDI, or systemic-risk connection, were not available in English, or lacked peer-review or normative authority.

Screening was conducted by the first author, with ambiguous cases resolved through supervisory consultation. The resulting gap analysis, presented in Table 1, establishes that no prior work has formally combined technical debt theory with OT security architecture in a unified taxonomic and causal framework. The survey establishes the novelty of the contribution by demonstrating that while each adjacent field contributes relevant concepts, none addresses the specific combination of long-lifecycle OT architecture, systemic cyber risk, and formal debt governance that ATD requires.

2.1. TECHNICAL DEBT IN SOFTWARE ENGINEERING

The foundational conceptualization of technical debt originates with Ward Cunningham's [2] observation that shipping code without full design maturity is analogous to incurring financial debt: the short-term gain of delivery speed is paid back, with interest, through increased maintenance effort and compounding complexity [2]. Cunningham's metaphor was subsequently formalized and extended by Kruchten et al. [3], whose intentionality-visibility quadrant model distinguishes deliberate from inadvertent debt, and prudent from reckless debt [3], a classification that remains foundational to the field. Besker, Martini, and Bosch [24] subsequently developed a unified model for managing architectural technical debt, identifying identification, measurement, and prioritized repayment as the three core governance activities.

Alves et al. [4] produced the most comprehensive synthesis of the software technical debt landscape to date, consolidating a taxonomy encompassing code, design, architecture, test, documentation, build, and infrastructure debt. Their systematic mapping study identified over 100 papers addressing technical debt, overwhelmingly in the context of agile software development and enterprise application contexts. Avgeriou et al. [5] subsequently developed the technical debt research roadmap, identifying quantification, management tooling, and empirical validation as primary research priorities; the field's most recent consensus publication further emphasizes governance integration as a priority [37]. Seaman and Guo [6] explored technical debt communication and management practices, identifying the challenge of making debt visible to non-technical stakeholders, a challenge directly mirrored in the ATD governance problem addressed by this paper.

The software technical debt literature is mature and well-developed. However, it is almost exclusively situated within software development contexts characterized by short lifecycles, modifiable codebases, and development teams with discretion over architectural choices. None of the major software debt taxonomies or frameworks addresses safety-critical systems, 30-year asset lifecycles, proprietary hardware constraints, or the physical consequence dimension of failure, conditions that fundamentally differentiate the critical infrastructure context.

2.2. TECHNICAL DEBT IN ENTERPRISE IT AND CLOUD SYSTEMS

The application of technical debt concepts to enterprise IT architecture and cloud systems, including modeling for cybersecurity analysis [32], has been explored in a more limited body of literature. Morgenthaler et al. [7] examined architectural debt in large-scale software systems at Google, identifying dependency management and modular boundary erosion as primary debt mechanisms. Li et al. [8] reviewed technical debt management practices in industry, finding that architecture debt and code debt are most frequently cited by practitioners as sources of significant technical risk. Ernst et al. [9] explored the relationship between architectural debt and system quality attributes, demonstrating empirically that architectural debt accumulation is associated with decreased maintainability and increased defect density.

In cloud and DevOps contexts, infrastructure-as-code debt, pipeline debt, and configuration debt have emerged as recognized categories, with automated detection tools increasingly available for enterprise environments. These developments reflect the maturation of debt management practices in contexts where infrastructure is software-defined, modification is low-friction, and continuous deployment enables rapid debt repayment.

Critically, none of this literature addresses the enterprise-to-OT boundary, the proprietary protocol constraint, or the physical process continuity requirement that characterizes critical digital infrastructure. Enterprise IT architecture debt operates in an environment where a misconfiguration can be rolled back; OT architecture debt operates in an environment where a misconfiguration can trigger a safety shutdown or enable physical process disruption. This qualitative distinction in consequence severity requires a dedicated analytical framework.

2.3. TECHNICAL DEBT IN INDUSTRIAL CONTROL SYSTEMS

The industrial control systems security literature is substantial and well-developed, anchored by foundational standards including NIST SP 800-82 Rev.3 [1], the IEC 62443 series [10], and the NERC CIP standards for energy sector infrastructure. Knapp and Langill's [14] treatment of ICS security addresses the architectural challenges of OT environments, including legacy system constraints, flat network architectures, and the tension between safety and security requirements. Stouffer et al.'s [1] NIST guidance explicitly acknowledges that many OT environments cannot be patched and that compensating controls must substitute for direct vulnerability remediation.

However, the ICS security literature is predominantly vulnerability-focused and operationally focused. It addresses what to do about known weaknesses, through patching, compensating controls, and configuration hardening, without providing a framework for characterizing the structural architectural conditions that determine the impact of those weaknesses. The zone-and-conduit model of IEC 62443-3-2 implicitly addresses structural debt by specifying a target architecture, but the standard does not frame deviation from this model as accumulated debt with compounding risk implications. MITRE ATT&CK for ICS provides an adversary technique catalog that is highly operationally useful, but it characterizes adversary capability rather than the structural conditions that enable adversary success.

2.4. TECHNICAL DEBT IN OT AND ICS CONTEXTS

The intersection of technical debt concepts with industrial control systems has received only marginal scholarly attention. Bi, Vogel-Heuser, Huang, and Ocker [26] examined technical debt characteristics in the automation domain, identifying legacy code debt, documentation debt, and configuration debt as the most prevalent forms in PLC and embedded control system contexts. Pàmies-Morell et al. [12] observed preliminary evidence of code and design debt in embedded control system firmware, noting that the absence of refactoring practices in embedded development produces compounding maintenance liability. Martínez-Fernández et al. [13] applied software debt concepts to cyber-physical systems in a manufacturing context, identifying configuration debt and documentation debt as particularly prevalent. These contributions, while valuable, remain limited to code-level and configuration-level debt observations. No published work has proposed a taxonomy of architectural technical debt in critical digital infrastructure, developed a causal model connecting ATD to systemic cyber risk, or proposed governance frameworks for ATD management in OT environments.

2.5. GAP ANALYSIS

Table 1 synthesizes the identified gaps across the four literature domains and positions the contributions of the present paper:

Table 1: Structured Gap Analysis of Technical Debt Research Across Four Literature Domains. Columns show the existing literature, current state of the art, and the identified gap addressed by the present paper.

Research Area	Existing Literature	State of the Art	Identified Gap
Software Technical Debt	Extensive, Cunningham [2]; Kruchten et al. [3]; Alves et al. [4]; Seaman & Guo [6]; Avgeriou et al. [5]	Highly mature taxonomy; quantification tools; automated detection	No application to safety-critical OT lifecycles or cyber-physical risk

Research Area	Existing Literature	State of the Art	Identified Gap
Enterprise IT & Cloud Debt	Moderate, Morgenthaler et al. [7]; Li et al. [8]; Ernst et al. [9]	Architecture debt; infrastructure debt; DevOps/pipeline debt emerging	Focuses on agile/cloud contexts; no OT protocol, trust boundary, or physical consequence dimension
Industrial Control Systems Security	Substantial, NIST SP 800-82 Rev.3; IEC 62443 series; Knapp & Langill [14]; Stouffer et al. [1]	Vulnerability management; zone-and-conduit; compensating controls	Vulnerability-centric; no structural debt framing; no ATD taxonomy or causal risk model
Technical Debt in ICS/OT	Scarce, Pàmies-Morell et al. [12]; Martínez-Fernández et al. [13]	Preliminary code/design debt observations in embedded systems	No formal taxonomy; no CDI-specific model; no connection to systemic cyber risk
Architectural Debt in CDI	Absent, no published taxonomy or causal model identified in systematic search	Not established	This paper presents an integrated formal taxonomy, causal model, assessment matrix, maturity model, and ATDI formulation for ATD in CDI, a combination not identified in the reviewed literature.

The gap analysis confirms that the present paper occupies a position not addressed by any existing body of work: the application of architectural technical debt theory to the specific structural, governance, and risk characteristics of critical digital infrastructure. The taxonomy, causal model, maturity framework, assessment matrix, and ATDI formulation proposed in this paper collectively constitute the first systematic treatment of this domain.

3. TECHNICAL DEBT: ORIGINS AND EVOLUTION

3.1. TECHNICAL DEBT THEORY

Ward Cunningham introduced the technical debt metaphor in 1992 to describe the long-term cost of expedient software engineering decisions. Code written without a full understanding of the problem domain is analogous to financial debt: it enables short-term delivery but incurs interest in the form of increasing maintenance burden and compounding complexity. The financial debt metaphor carries implications that are analytically productive for critical infrastructure contexts. Debt incurs interest: the cost of deferring an architectural decision grows over time as surrounding systems evolve [27] and dependencies accumulate. Critically, debt compounds: in financial terms, compound interest grows the principal. In Architectural Technical Debt, compound interest grows the blast radius. Each deferred segmentation decision, each unmanaged implicit trust relationship, each unsupported system left in place, these do not add linearly to the risk profile; they multiply it, because their interaction creates emergent conditions whose severity exceeds the sum of individual components. Third, debt can reach a default condition: when architectural complexity exceeds operators' capacity to manage it safely, systemic failure becomes probable.

3.1.1 The 'Interest' of ATD in Cyber-Physical Systems

In software engineering, the interest in technical debt is expressed as increased maintenance effort. In operational technology environments, ATD interest manifests through three compounding mechanisms. First, blast radius amplification: each deferred segmentation or trust-boundary decision increases the number of systems reachable from a single compromised endpoint. Second, Mean Time to Detect (MTTD) degradation: accumulated visibility debt extends adversary dwell time unchecked, increasing the probability that pre-positioned access survives to execution. Third, operational remediation penalty: unlike software debt, where interest can be paid down through refactoring, the interest on structural ATD is extracted at remediation time through operational downtime, safety risk during network reconfiguration, and compounding disruption of undocumented dependencies. These mechanisms make ATD interest genuinely compound: each period of deferral increases both the principal of structural debt and the rate at which interest accrues against it.

3.2. CATEGORIES OF TECHNICAL DEBT

Alves et al. [4] synthesized a taxonomy encompassing code, design, architecture, test, documentation, build, and infrastructure debt. For critical infrastructure purposes, design debt, infrastructure debt, and documentation debt are most directly relevant. A critical distinction must be drawn from agile software contexts: in software development, technical debt is predominantly self-inflicted by teams trading architectural rigor for delivery velocity. In OT environments, ATD is primarily inherited or externally imposed, arising from vendor-specified proprietary architectures, physics and safety constraints, and capital allocation decisions beyond operational teams' control. This distinction has direct governance implications: treating OT ATD as analogous to sprint debt misattributes accountability and impedes effective governance.

3.3. WHY CRITICAL INFRASTRUCTURE IS DIFFERENT

Critical digital infrastructure presents characteristics that render conventional technical debt frameworks inadequate:

- Extended asset lifecycles of 20 to 40 years lock in architectural decisions made at procurement for decades.
- Safety-security interaction means that security controls may be precluded by operational safety requirements [29].
- Proprietary technology ecosystems and contractual restrictions limit operators' ability to address architectural deficiencies unilaterally.
- High replacement costs and operational continuity requirements mean architectural modernization is frequently deferred indefinitely.
- Skill gaps at the IT-OT convergence boundary limit institutional capacity to recognize and articulate architectural risk.

4. ARCHITECTURAL TECHNICAL DEBT IN CRITICAL DIGITAL INFRASTRUCTURE

4.1. CONCEPTUAL DEFINITION

Architectural Technical Debt (ATD) refers to the accumulated structural deficiencies, deferred architectural decisions, and design-era compromises that progressively increase system complexity, erode trust boundaries, and amplify cyber risk within critical digital infrastructure, such that the cost of remediation, in operational disruption, financial investment, and residual risk, grows over time and may eventually exceed operators' capacity to manage.

This definition is structural rather than operational, temporal rather than discrete, and consequentialist rather than implementation-specific. ATD is not equivalent to legacy system risk, which denotes risk from the age of specific components; to technical vulnerability, which denotes exploitable weaknesses in specific implementations; or to compliance gap, which denotes deviation from regulatory requirements. ATD is analytically before all three: it is the structural condition that determines the impact of vulnerabilities, generates compliance gaps, and makes legacy systems dangerous rather than merely old.

4.2. SOURCES OF ARCHITECTURAL TECHNICAL DEBT

4.2.1 Legacy Operational Technology Systems

SCADA systems, distributed control systems, PLCs, RTUs, and HMIs deployed before IT-OT convergence were not designed with network-accessible threat models. They lack authentication mechanisms, cryptographic capability, segmentation support, and audit

logging. Their continued operation is not a governance failure per se; replacement costs may rationally preclude modernization, but their presence creates structural conditions that amplify the risk of every other component in the environment.

4.2.2 Flat Network Architectures

In a flat OT network, engineering workstations, historians, HMIs, PLCs, and field devices share a common broadcast domain or are connected through switches that enforce no access control. This architecture was rational in the air-gapped era, but becomes a lateral movement force multiplier once the perimeter is breached. The zone-and-conduit model of IEC 62443-3-2 represents the target-state remediation of flat network ATD.

4.2.3 Implicit Trust Relationships

Modbus TCP has no native authentication mechanism; DNP3 Secure Authentication was a retrofit to a protocol designed without security. Trust relationships in OT environments are therefore not managed artifacts but inherited conditions, a form of trust debt that grows as the attack surface of the connected enterprise expands.

4.2.4 Vendor Lock-in and Proprietary Protocols

Operational technology procurement produces deep vendor dependencies: proprietary protocols, closed firmware, and contractual restrictions. An operator may be unable to deploy monitoring agents on vendor-managed controllers or segment a network without voiding maintenance agreements, deferring architectural risk reduction to a future state contingent on vendor cooperation.

4.2.5 Deferred Modernization

Hardware beyond manufacturer support horizons, operating systems without security updates, and unsupported software stacks are the material manifestations of deferred modernization debt. Each deferral decision is individually rational but collectively produces a compounding architectural liability. NIST SP 800-82 Rev.3 acknowledges this as a structural feature of the OT landscape rather than an exceptional condition.

4.2.6 Inadequate Observability

Many embedded systems generate no audit logs; many industrial switches produce no network telemetry consumable by SIEM platforms. This observability deficit is architectural, encoded in device and protocol design. Without observability, operators cannot detect anomalies, establish behavioral baselines, or reconstruct incident timelines, capabilities that MITRE ATT&CK for ICS identifies as prerequisites for detecting the most prevalent OT adversary techniques.

5. FORMAL RISK AMPLIFICATION FRAMEWORK

Section 4 established the sources of ATD. This section formalizes the causal mechanism by which ATD amplifies cyber risk. Rather than presenting this mechanism descriptively, the following six propositions define the logical relationships between ATD and systemic risk in a form that supports future empirical validation. Each proposition is accompanied by its theoretical grounding and observable indicators.

P1: Increasing Architectural Technical Debt increases structural complexity in critical digital infrastructure environments. As ATD accumulates through flat network architectures, implicit trust relationships, proprietary dependencies, and visibility deficits, the architectural state of the system departs progressively from the manageable and observable toward the complex and opaque. [Hypothesis for future empirical testing.]

Theoretical grounding: Technical debt compounding [2], [3]. Observable indicator: The number of unintended or undocumented communication pathways between security domains, as revealed by passive network discovery.

P2: Structural complexity generates hidden vulnerabilities that are not detectable through conventional component-level vulnerability scanning. These vulnerabilities emerge from the architectural interaction of multiple debt items and are qualitatively distinct from CVE-class weaknesses. [Hypothesis for future empirical testing.]

Theoretical grounding: Emergent risk in complex systems [15], [16]. Observable indicator: The number of exploitable communication pathways identified during red team assessments that were not flagged by prior vulnerability scanning.

P3: Hidden vulnerabilities expand the effective attack surface of the CDI system beyond the surface implied by individual component exposure. The effective attack surface is determined not by the sum of exposed interfaces but by the architectural conditions governing their reachability and exploitability. [Hypothesis for future empirical testing.]

Theoretical grounding: Attack surface theory [17]; Flat network ATD as attack surface amplifier. Observable indicator: The ratio of reachable OT endpoints from a compromised single host to the total OT endpoint population, the Lateral Reachability Ratio (LRR).

P4: Expanded effective attack surfaces facilitate risk propagation: the spread of compromise, disruption, or exfiltration from an initial access point across the broader OT environment. The rate and scope of propagation are determined by the extent of structural and trust debt. [Hypothesis for future empirical testing.]

Theoretical grounding: Tight coupling and propagation in normal accidents [15]. Observable indicator: Mean Time to Lateral Movement (MTTLM) from initial access to second-domain compromise, as measured in adversary simulation exercises.

P5: Risk propagation reduces the resilience of the CDI system by degrading its capacity to absorb disruption, isolate compromise, and restore operations within operationally acceptable timeframes. Resilience reduction is compounded by residual resilience debt. [Hypothesis for future empirical testing.]

Theoretical grounding: Resilience engineering [18], [19]. Observable indicator: Mean Time to Recover (MTTR) from a simulated cyber-physical incident, measured in digital twin or tabletop exercise environments.

P6: Reduced resilience increases the probability and magnitude of operational disruption, including cascading failures across dependent infrastructure sectors. The feedback effect of post-incident emergency workarounds generates additional ATD, creating a recursive debt accumulation cycle. [Hypothesis for future empirical testing.]

Theoretical grounding: Recursive debt accumulation; tight coupling and cascade [15]; socio-technical systems feedback [20]. Observable indicator: Post-incident ATD increment, measured as the number of new structural, trust, or governance debt items introduced through emergency response measures.

Together, P1 through P6 form a testable causal chain: ATD → Complexity → Hidden Vulnerabilities → Expanded Attack Surface → Propagation → Reduced Resilience → Operational Disruption. Each link in the chain is defined by an observable indicator that can, in principle, be measured in case study or simulation environments. This framework provides the empirical research community with a structured basis for validating the ATD risk amplification mechanism and provides practitioners with falsifiable hypotheses against which their own architectural risk assessments can be benchmarked.

6. TAXONOMY OF ARCHITECTURAL TECHNICAL DEBT

The following taxonomy organizes ATD into six analytically distinct categories, each defined by a characteristic source, primary security impact mechanism, and alignment to specific IEC 62443 System Requirements (SRs) and NIST controls. The six categories are designed to be conceptually non-overlapping, though inter-category interactions exist by design. To prevent double-counting in assessment and scoring, each debt item should be assigned to the category that reflects its primary architectural locus: Structural Debt concerns topology and segmentation; Trust Debt concerns identity and authentication; Dependency Debt concerns protocol and vendor constraints; Visibility Debt concerns telemetry and monitoring absence; Governance Debt concerns policy, process, and lifecycle management; and Resilience Debt concerns redundancy, recovery, and continuity capability. An item that appears to span categories, for example, a missing patch that arises from both governance failure and vendor dependency, should be assigned to the category of its primary causal mechanism (in this case, Dependency Debt if the constraint is vendor-imposed, or Governance Debt if it reflects an absent patch management policy). The ATDI formulation in Section 13.2 scores each category independently; double-counting is avoided because no single system characteristic should increment more than one component score. The taxonomy is grounded in the sources identified in Section 4.2 and structured to support the ATD Assessment Matrix in Section 12. The gap analysis in Section 2.5 confirms that no comparable OT-specific taxonomy exists in the published literature.

Table 2: Six-Category Taxonomy of Architectural Technical Debt. Each category is defined by its primary source, security impact, an illustrative OT/ICS example, and its most directly applicable IEC 62443 or NIST control reference.

Debt Type	Primary Source	Security Impact	Illustrative Example	IEC 62443 / NIST Reference
Structural Debt	Flat network design; poor segmentation during initial build or early expansion phases	Unimpeded lateral movement; blast radius amplification across OT domains	SCADA systems on flat plant networks connected to enterprise IT without DMZ isolation	IEC 62443-3-3 SR 5.1 (Logical Segmentation) NIST SP 800-82 Rev.3 6.2
Trust Debt	Implicit trust inherited from air-gapped era; weak or absent identity controls; default credentials	Privilege escalation; credential abuse; insider threat facilitation	PLCs configured to accept unauthenticated Modbus commands from any host on the segment	IEC 62443-3-3 SR 1.1 (Human User Identification & Authentication) / SR 1.2 (Software Process and Device Authentication) NIST SP 800-207 (Zero Trust)
Dependency Debt	Legacy vendor protocols; proprietary communication stacks; hard-coded system interdependencies	Single-vendor lock-in; inability to patch without operational disruption	DNP3 or legacy OPC-DA reliance on Windows XP endpoints that cannot be patched or replaced	IEC 62443-3-3 SR 3.3 (Security Functionality Verification); note: no single SR maps directly to protocol dependency constraints NIST SP 800-82 Rev.3 5.3
Visibility Debt	Absence of OT-aware monitoring; limited telemetry from embedded systems; no network baselining	Blind spots enable dwell time, delayed incident detection, and hampered forensic analysis.	Industrial switches generating no syslog; no SIEM visibility into ICS traffic patterns	IEC 62443-3-3 SR 6.1 (Audit Log Accountability) / SR 6.2 (Continuous Monitoring) MITRE ATT&CK for ICS, Detection
Governance Debt	Outdated security policies; weak lifecycle management; absent procurement security gates	Non-compliance with IEC 62443 and NIST SP 800-82; unmanaged end-of-life asset proliferation	Control systems running beyond the vendor support horizon with no documented decommission plan.	IEC 62443-2-1 (ICS Security Management System), governance requirements are addressed in Part 2-1, not Part 3-3 NIST CSF 2.0, Govern
Resilience Debt	Absence of redundancy; single points of failure baked into original architecture; no tested recovery	Catastrophic single-event failures; extended MTTR; cascade into safety systems	Single historian server serving all process data with no failover or offline backup strategy	IEC 62443-3-3 SR 7.1 (Denial of Service Protection) / SR 7.3 (Control System Backup) / SR 7.4 (Control System Recovery) NIST SP 800-82 Rev.3 6.4 (Recovery)



Figure 1: Six-Dimension ATD Taxonomy (Hub-and-Spoke). The central node represents the ATD construct; six satellite nodes represent the taxonomy categories, each showing the primary IEC 62443 SR alignment.

6.1. STRUCTURAL DEBT

Structural debt encompasses deficiencies in OT network topology, including flat architectures and absent DMZ separation at OT-IT boundaries. It is the most architecturally fundamental ATD category because it determines propagation pathways following compromise. Remediation requires network redesign. IEC 62443-3-3 SR 5.1 (Logical Segmentation) provides the target-state requirement.

6.2. TRUST DEBT

Trust debt denotes implicit, undifferentiated, and unmanaged trust relationships within OT environments, manifest in absent protocol authentication, over-privileged accounts, and default credentials. It is the primary enabler of privilege escalation and lateral movement. IEC 62443-3-3 SR 1.1 (Human User Identification and Authentication) and SR 1.2 (Software Process and Device Authentication) define the identity and authentication requirements applicable to trust debt remediation.

6.3. DEPENDENCY DEBT

Dependency debt arises from architecturally encoded reliance on legacy protocols and hard-coded interdependencies that cannot be modified without operational disruption. IEC 62443-3-3 SR 3.3 (Security Functionality Verification) is the closest applicable requirement; as noted in Table 2, no single SR maps directly to protocol dependency constraints, which reflect vendor-imposed and contractual limitations outside the scope of a single technical control.

6.4. VISIBILITY DEBT

Visibility debt is the structural absence of telemetry, monitoring, and audit logging in OT environments. IEC 62443-3-3 SR 6.1 (Audit Log Accountability) and SR 6.2 (Continuous Monitoring) define the visibility target state. MITRE ATT&CK for ICS [11] documents the specific adversary techniques that exploit visibility limitations to extend dwell time and avoid detection.

6.5. GOVERNANCE DEBT

Governance debt encompasses absent or outdated security policies, asset management practices, and architectural review processes. IEC 62443-2-1 defines the Security Management System requirements for IACS environments that, when absent or outdated, constitute measurable governance debt. Note that SR 2.1, SR 2.2, and SR 2.3 within IEC 62443-3-3 address Use Control requirements, which are distinct from the governance and policy obligations addressed by Part 2-1 of the standard. Governance debt is frequently the root cause of other debt categories, as structural debt persists where governance processes do not require its identification and remediation.

6.6. RESILIENCE DEBT

Resilience debt denotes the accumulated absence of redundancy, fault isolation, and tested recovery capability. IEC 62443-3-3 SR 7.1 (Denial of Service Protection), SR 7.3 (Control System Backup), and SR 7.4 (Control System Recovery) directly address the availability and recovery dimensions of resilience requirements. NIST SP 800-82 Rev.3 Section 6.4 provides OT-specific recovery planning guidance. Resilience debt determines the operational impact severity when other debt categories are exploited.

7. THEORETICAL FOUNDATIONS

The ATD conceptualization rests on four theoretical traditions providing complementary analytical lenses.

7.1. TECHNICAL DEBT THEORY

Technical debt theory provides the foundational framework. The distinction between intentional and inadvertent debt, deliberate trade-offs versus decisions taken without awareness of long-term consequences, maps onto the two primary ATD accumulation mechanisms: intentional deferral of modernization due to cost or operational constraints, and inadvertent accumulation through design-era decisions not understood to carry long-term security implications. The compound interest analogy, explicitly formalized in Proposition P6, provides the mechanism by which post-incident workarounds generate recursive debt accumulation.

7.2. SYSTEMS THEORY AND EMERGENT RISK

Complex systems theory provides the framework for understanding how risk properties emerge from component interaction rather than residing in individual components; integrated cybersecurity risk management frameworks [36] provide complementary empirical grounding for this perspective. Perrow's Normal Accident Theory introduces the concepts of tight coupling and complex interaction that explain why ATD is particularly consequential in critical infrastructure: tightly coupled systems propagate disturbances rapidly, and complex interactions prevent operators from anticipating failure pathways. The propositions P2 and P3 are directly grounded in this theoretical tradition.

7.3. RESILIENCE ENGINEERING

Resilience engineering, as developed by Hollnagel, Woods, and Leveson, contributes the concept of adaptive capacity as the primary analytical target. Leveson's STAMP framework is particularly relevant: it treats failures not as chains of component failures but as the result of inadequate control over system interactions, a framing that maps precisely onto the ATD causal model. Propositions P5 and P6 draw directly on resilience engineering concepts.

7.4. SOCIO-TECHNICAL SYSTEMS THEORY

Socio-technical systems theory contributes to the recognition that ATD is not exclusively technical but reflects the interaction of technical constraints, organizational decision-

making, economic incentives, and regulatory requirements. Governance debt, the most organisationally-rooted ATD category, cannot be addressed through technical intervention alone; effective remediation requires changes to governance structures, procurement processes, and organizational accountability frameworks, interventions that are inherently socio-technical.

8. CONCEPTUAL MODEL OF ATD-INDUCED SYSTEMIC CYBER RISK

The following seven-stage model integrates the formal propositions of Section 5 into a causal representation of the pathway from ATD accumulation to operational disruption. Each stage corresponds to a proposition in the Risk Amplification Framework, providing both a narrative account and a formal theoretical anchor.



Figure 2: ATD-Induced Systemic Cyber Risk Model. Seven-stage causal chain from ATD accumulation (Stage 1) to operational disruption and recursive debt generation (Stage 7). Stages reference the formal propositions P1–P6 (Section 5).

Stage 1: Architectural Technical Debt Accumulation [P1 antecedent] Legacy systems, flat network architectures, implicit trust, vendor lock-in, deferred modernization, and visibility gaps accumulate as structural liabilities in the OT environment. Each individual debt item may appear manageable; its interaction produces non-linear structural complexity.

Stage 2: Increased Structural Complexity [P1] interacting debt items produce emergent architectural opacity. The system state exceeds operators' ability to maintain an accurate mental model of dependencies, communication pathways, and blast radius, impairing governance, incident planning, and response effectiveness.

Stage 3: Erosion of Trust Boundaries [P2] Structural complexity generates hidden vulnerabilities arising from the architectural interaction of debt items. Implicit trust relationships, absent identity controls, and insufficiently governed OT-IT boundaries collapse the effective security perimeter to the outermost system boundary.

Stage 4: Risk Amplification [P3] Eroded trust boundaries and hidden vulnerabilities expand the effective attack surface beyond what component-level vulnerability scanning reveals. A single exploitable weakness in a flat, trust-implicit environment may provide adversary access to the entire OT domain.

Stage 5: Lateral Movement and Risk Propagation [P4] Expanded attack surface and absent internal boundaries enable adversary lateral movement across OT domains and, at OT-IT boundaries, into enterprise systems. Visibility debt prevents detection during the dwell period, allowing propagation to mature unchecked.

Stage 6: Reduced Resilience [P5] Compounded structural, trust, visibility, and resilience debt produces a system unable to absorb disruption, isolate compromise, or restore operations within operationally acceptable timeframes. Recovery is further impeded by undocumented dependencies produced by deferred modernization.

Stage 7: Operational Disruption and Recursive Debt Generation [P6] Cascading operational disruption affects dependent sectors. Post-incident emergency workarounds, temporary configurations, and deferred recovery tasks generate additional ATD, completing the recursive cycle in which unresolved incidents accelerate further debt accumulation.

The model has three analytically important properties. First, it is non-deterministic: ATD accumulation does not inevitably produce operational disruption; it progressively degrades the conditions that prevent it. Second, it is recursive: incidents managed without architectural remediation generate additional ATD through emergency workarounds, a feedback mechanism that is particularly acute in post-incident OT environments where temporary measures become permanent. Third, it is governable: each stage represents an intervention point at which deliberate architectural or governance action can interrupt the causal pathway. This governability property is the theoretical basis for the maturity model in Section 10 and the strategies in Section 9.

A proportionality corollary follows from the model: the operational impact of any vulnerability at Stage 3 is a function not of the vulnerability's individual severity but of the ATD conditions at Stage 1. Architectural debt remediation can therefore deliver risk reduction disproportionate to the resources invested, because it changes the structural conditions under which the entire vulnerability landscape operates.

9. STRATEGIES FOR MANAGING ARCHITECTURAL TECHNICAL DEBT

Effective ATD management requires a portfolio of interventions; Staves et al. [30] provide an analogous portfolio approach for ICS incident response and recovery that informs the sequencing logic applied here across different implementation timescales. Table 3 summarises the primary strategies with their mechanisms, risk reduction potential, implementation complexity, and key standards alignment. The strategies are ordered from highest to lowest immediate risk reduction impact.

Table 3: Portfolio of ATD Management Strategies Ordered by Primary Debt Category Addressed. Risk reduction ratings are qualitative assessments; empirical validation is required.

Strategy	Mechanism	Risk Reduction	Implementation Complexity	Key Standard
Zero Trust Architecture	Eliminates implicit trust; enforces verified identity at every communication boundary regardless of network location	High	Gradual; begin with crown-jewel assets	NIST SP 800-207
Network Segmentation & DMZ	Isolates OT domains into zones; restricts lateral movement pathways	High	Moderate; requires topology redesign	IEC 62443-3-2

Strategy	Mechanism	Risk Reduction	Implementation Complexity	Key Standard
Architectural Refactoring	Systematically retires flat architectures; replaces monolithic dependencies with modular design.	High	Significant; may require partial outages	NIST SP 800-82 Rev.3
OT-Aware Continuous Monitoring	Deploys passive industrial protocol inspection; baselines normal traffic; reduces MTTD	High	Low-medium; passive sensors are non-disruptive	MITRE ATT&CK for ICS
Software-Defined Networking	Enables dynamic micro-segmentation; reduces manual reconfiguration complexity	Medium	Moderate; requires controller deployment	IEC 62443-2-4
Digital Twin Simulation	Tests architectural changes safely; quantifies accumulating ATD interest without live system risk	Medium	High initially; reduces long-term operational risk	NIST CSF 2.0
Incremental Modernisation	Phased replacement of legacy components; avoids big-bang disruption	Medium	Low per phase; long overall timeline	IEC 62443-2-3
Governance & Asset Lifecycle	Enforces structured asset lifecycle policies; mandates architectural reviews at procurement	Medium	Low; primarily policy and process change	ISO/IEC 27001, NIST CSF

9.1. ZERO TRUST ARCHITECTURE

Zero Trust Architecture (ZTA), as specified in NIST SP 800-207 [21], addresses trust debt by replacing implicit perimeter-based trust with explicit verification at every communication boundary [31] regardless of network location. In the OT context, ZTA implementation must account for the latency sensitivity of real-time control systems and the limited authentication capability of legacy endpoints. A trust mediation architecture, in which a protocol-aware mediation layer interposes between legacy OT endpoints and network communications, addresses trust debt without requiring legacy device replacement, providing a pragmatic entry point for ZTA adoption in constrained OT environments.

9.2. NETWORK SEGMENTATION AND ZONE-AND-CONDUIT ARCHITECTURE

Network segmentation is the primary intervention for structural debt and the most direct implementation of the IEC 62443-3-2 zone-and-conduit model. In retrofit contexts, passive network discovery using commercial OT-aware Network Detection and Response (NDR) platforms can establish a current-state asset inventory and communication map as the foundation for segmentation design. Segmentation directly reduces blast radius, interrupts lateral movement pathways, and provides the structural foundation on which monitoring and access management controls can operate more effectively.

9.3. OT-AWARE CONTINUOUS MONITORING

Continuous monitoring addresses visibility debt and is a prerequisite for detecting the reconnaissance, lateral movement, and pre-positioning activities that characterize advanced persistent threats targeting critical infrastructure. OT-aware monitoring must decode industrial protocols, including Modbus, DNP3, EtherNet/IP, and IEC 61850 GOOSE, and must be capable of detecting behavioral anomalies against established baselines. Detection coverage mapped to MITRE ATT&CK for ICS [11] provides a measurable basis for assessing and reducing MTTD as a direct metric of visibility debt remediation progress.

9.4. ARCHITECTURAL REFACTORING AND INCREMENTAL MODERNIZATION

Architectural refactoring is the most direct form of debt remediation. In critical infrastructure contexts, big-bang replacement is rarely feasible; incremental modernization, directed by a defined target architecture, sequenced by risk reduction per unit of investment, and

validated at each increment, is the only operationally viable approach. Published cyber-physical zero trust reference architectures [38] provide the target-state blueprint toward which incremental changes should be directed.

9.5. DIGITAL TWINS FOR SAFE ARCHITECTURAL VALIDATION

Digital twin technology enables safe testing of architectural changes before production deployment [28] and has been applied to cyber-attack detection in cyber-physical manufacturing systems [33]. Critically, it provides a practically safe mechanism for measuring the interest accumulating on ATD without exposing live systems to risk. By simulating adversary lateral movement against the digital twin's representation of the current architectural state, operators can quantify blast radius, estimate MTTD under current visibility conditions, and model risk reduction from specific interventions, generating the evidence base needed to justify ATD remediation investment to governance bodies.

9.6. GOVERNANCE AND ASSET LIFECYCLE MANAGEMENT

Governance debt requires process-level interventions: an authoritative, continuously maintained asset inventory; procurement processes that mandate architectural security review at the acquisition stage, ensuring new assets do not introduce additional structural or dependency debt into the environment without a defined remediation pathway; architectural review boards with authority to mandate remediation; and a risk governance framework that treats ATD as a material cyber risk reportable to executive leadership.

9.7. EMERGING ECONOMY CONSIDERATIONS

ATD management strategies designed for high-income economy contexts require significant adaptation for sub-Saharan African and other emerging economy critical digital infrastructure environments. First, the OT installed base in many emerging economy sectors disproportionately comprises second-hand equipment procured from developed-economy operators at end-of-life, arriving with significant inherited structural and dependency ATD and absent operational documentation. Second, severe IT-OT convergence skill deficits mean governance debt accumulates faster than governance capacity can address it. Third, capital constraints mean the principal of ATD cannot be repaid through direct modernization; operators are structurally dependent on compensating controls as indefinite rather than transitional measures, making the design quality of those controls a matter of national security consequence. Fourth, early-maturity regulatory frameworks in many emerging economies lack the OT-specific mechanisms to incentivize architectural debt governance. Regional bodies, including the African Union and SADC, are positioned to support the adoption of ATD-aware regulatory frameworks that do not require capital investment but can change operator behavior in measurable ways.

10. ARCHITECTURAL TECHNICAL DEBT MATURITY MODEL

The preceding sections have established what ATD is, how it accumulates, how it amplifies risk, and what strategies reduce it. A remaining practical challenge is that organizations exist at dramatically different points in their capacity to recognize and govern ATD. The Architectural Technical Debt Maturity Model (ATD-MM) provides a structured progression from complete ATD unawareness to optimized continuous architectural assurance.

The model draws on the maturity framework tradition established by the Capability Maturity Model Integration (CMMI) and applied in cybersecurity contexts by frameworks including NIST CSF 2.0 and IEC 62443-2-1. It defines five levels that characterize an organization's ATD governance capability, from Level 1 (Reactive) through Level 5 (Optimized). Each level is defined by a set of observable characteristics, a current ATD governance state, and a set of priority actions to advance to the next level.

Table 4: Architectural Technical Debt Maturity Model (ATD-MM). Levels L1 to L5 describe a governance capability progression; levels are conceptual and require empirical validation for threshold calibration.

Maturity Level	Characteristics	ATD Governance State	Priority Actions to Advance
L1: Reactive	ATD is entirely unrecognized as a risk category. No asset inventory. Architecture undocumented. Security posture is determined by external incidents or regulatory enforcement actions.	No ATD governance; vulnerability scanning may exist, but produces no architectural insight	Achieve basic asset discovery; map OT network topology; conduct first architectural risk assessment.
L2: Aware	ATD is recognized informally by technical staff but not formalized as a governance category. Ad hoc identification of structural issues. A partial asset inventory exists.	ATD discussed but unmeasured; compensating controls deployed reactively; no debt register	Formalize ATD definition and taxonomy; develop an initial ATD register using this paper's framework; assign governance ownership.
L3: Managed	A formal ATD register exists and is maintained. Debt items are classified by type, risk level, and remediation cost. Debt is reviewed periodically and reported to management.	Structured debt inventory; prioritized remediation roadmap; ATD integrated into risk register	Integrate ATD into procurement gate reviews; develop target architecture; begin incremental modernization program.
L4: Governed	ATD is a first-class governance category. ATDI is computed periodically. Debt reduction targets set at the executive level. The architectural review board is active. Regulatory reporting includes ATD status.	ATDI tracked and trended; debt-reduction targets in operational KPIs; regulatory disclosure of material ATD	Automate ATD detection where feasible; implement debt-aware security orchestration; validate remediation via digital twin
L5: Optimised	Continuous architectural assurance is operational. ATD accumulation is detected in near-real time. Debt-aware orchestration adjusts security controls dynamically. ATDI trending toward minimum.	Automated ATD detection; continuous architectural validation; debt-aware SOAR integration; ATDI as a board-level risk metric	Contribute validated ATD metrics to standards bodies; publish sector benchmarks; support peer operators at lower maturity levels.



Figure 3: Architectural Technical Debt Maturity Model (ATD-MM). Ascending staircase from L1 (Reactive) to L5 (Optimized), showing increasing governance capability. Level boundaries are conceptual and require empirical validation.

Several properties of the ATD-MM warrant emphasis. First, the model is not prescriptive about the rate of progression: advancing from L1 to L5 may require years in a resource-constrained environment, but each level transition delivers measurable risk reduction. Second, the model is not sequential in all respects: an organization may have L4 governance capabilities in one debt category (e.g., Governance Debt, where a mature asset lifecycle process exists) while remaining at L1 or L2 in another (e.g., Visibility Debt, where no OT monitoring exists). The six-category taxonomy of Section 6 supports per-category maturity assessment. Third, the

model is calibrated to CDI environments: the characteristics described at each level reflect the specific constraints of OT infrastructure rather than enterprise IT norms.

The ATD-MM is intended to provide governance bodies, regulators, and board-level risk committees with a communication tool for ATD status that does not require deep technical knowledge. A statement that “our OT security architecture is currently operating at ATD Maturity Level 2 with a target of Level 3 within 24 months” conveys architectural risk posture in terms accessible to non-technical decision-makers. This accessibility is a prerequisite for the executive-level engagement that ATD governance requires.

Future research should develop and validate quantitative scoring criteria for each maturity level transition, drawing on the ATDI formulation in Section 13.2 and the Assessment Matrix in Section 12. Sector-specific benchmarking of ATD maturity levels across energy, water, transportation, and healthcare CDI would provide both baseline data and peer comparison capability for operators undertaking self-assessment.

11. IMPLICATIONS

The ATD framework carries differentiated implications across the four principal stakeholder groups engaged in the governance and security of critical digital infrastructure. This section addresses each group in turn, translating the theoretical contributions of the preceding sections into actionable guidance.

11.1. FOR CRITICAL INFRASTRUCTURE OPERATORS

The ATD framework implies that security risk assessments must incorporate structural architectural analysis alongside conventional vulnerability assessment. In high-ATD environments, a proportionality argument formalized by Propositions P3 and P4 holds: architectural debt remediation may deliver greater risk reduction than addressing individual vulnerabilities, because it changes the structural conditions under which the entire vulnerability landscape operates. A remediated segmentation boundary reduces the blast radius of every future exploit across the OT domain; no individual CVE patch achieves a comparable systemic effect.

Operators should implement three priority governance mechanisms. First, ATD registers: structured inventories of identified debt items, classified using the six-category taxonomy of Section 6, with associated risk implications, remediation costs, and roadmap commitments. The Assessment Matrix of Section 12 provides the elicitation tool for populating these registers. Second, architectural review boards: cross-functional bodies with authority to assess ATD accumulation at procurement, to mandate remediation timelines, and to evaluate proposed architectural changes for debt impact before implementation. Third, debt reduction roadmaps: time-bound, sequenced programs directing incremental modernization toward a defined target architecture, using the ATD-MM progression (Section 10) to define and measure maturity advancement. ATD registers and ATDI scores should be reported to executive leadership alongside other material cyber risk indicators, positioning architectural risk as a board-level governance concern rather than a technical maintenance matter.

11.2. FOR REGULATORS

Existing regulatory frameworks for critical infrastructure cybersecurity are predominantly vulnerability-focused and compliance-oriented. IEC 62443 [10], NIST CSF 2.0 [22], and sector-specific standards provide valuable baseline requirements, but they assess discrete security control implementation rather than the structural architectural conditions that determine whether those controls produce genuine risk reduction. A facility that achieves full compliance against a security standards checklist may nonetheless carry extreme systemic cyber risk if its network architecture is flat, its trust model is implicit, and its monitoring coverage is absent.

Regulators should consider incorporating four architectural assessment requirements into critical infrastructure licensing and oversight frameworks: first, periodic ATD assessments structured around the taxonomy and assessment matrix of this paper, with findings submitted as part of cyber risk governance disclosures; second, ATD register maintenance as a mandatory governance artefact, subject to regulatory review; third, target architecture documentation demonstrating a defined end-state toward which incremental modernisation programmes are directed; and fourth, procurement gate requirements mandating security architecture review and ATD impact assessment before any new OT asset acquisition. The ATD-MM in Section 10 provides a maturity progression framework suitable for use in regulatory conditions and licensing requirements, enabling sector-wide benchmarking and objective assessment of operator governance capability advancement over time.

11.3. FOR POLICYMAKERS

At the national and regional policy level, ATD represents a structural dimension of cyber resilience that is not currently captured in national cyber strategies, critical infrastructure protection frameworks, security-by-design guidance [23], or international development programs. The absence of ATD from policy frameworks means that investments in critical infrastructure security, which often concentrate on incident response capability, perimeter security technology, and compliance training, leave the structural roots of systemic risk unaddressed.

Policymakers should consider three interventions. First, national ATD baseline programs: structured surveys of ATD profiles across critical infrastructure sectors, using the taxonomy and assessment matrix as a standardized methodology, to establish sector-wide debt baselines and identify the most acute concentration risks. Second, sector benchmarking initiatives: publication of anonymized ATD maturity benchmarks by sector, enabling operators to assess their relative position and providing policymakers with evidence for targeted intervention. Third, resilience metrics integration: incorporation of ATD indicators, including ATDI scores, ATD-MM maturity levels, and architectural segmentation coverage, into national cyber resilience dashboards and international cyber capacity development frameworks. In sub-Saharan Africa and other emerging economy regions, bilateral and multilateral security assistance programs should explicitly address ATD as a structural challenge, prioritizing governance-level interventions that can deliver risk reduction without requiring capital investment in hardware modernization.

11.4. FOR RESEARCHERS

The formal propositions P1-P6 of Section 5 constitute a structured empirical research agenda. The most immediate priority is case study validation of the causal chain across real OT environments, with particular focus on the measurable indicators defined for each proposition: the Lateral Reachability Ratio (P3), Mean Time to Lateral Movement (P4), and Post-incident ATD increment (P6). These indicators are defined precisely enough for measurement in digital twin adversary simulation environments, enabling controlled empirical studies without the operational risk of live system testing.

Longitudinal studies tracking ATDI scores over time, before and after specific architectural interventions, would provide the empirical grounding for the proportionality claim embedded in P3 and P4: that architectural debt remediation delivers disproportionate risk reduction relative to investment. Such studies would also enable calibration of the sector-specific weightings required by the ATDI formula, grounding the index in evidence rather than expert judgment. Development and peer validation of the ATDI as a standardized measurement instrument represents the most significant near-term research contribution the community could make to advancing ATD from a conceptual framework to an operational governance tool.

12. ATD ASSESSMENT MATRIX

Table 5 presents the ATD Assessment Matrix, translating the taxonomy of Section 6 into a practitioner-facing tool for structured architectural debt assessment. Each debt category is mapped to a qualitative assessment question, a quantitative indicator aligned to the observable indicators defined in Section 5, a primary evidence source, and a high-risk threshold. The thresholds are indicative rather than normative, reflecting judgment-based estimates pending the validated quantitative metrics that future ATDI research should provide.

Table 5: ATD Assessment Matrix. Provides qualitative assessment questions, quantitative indicators, primary evidence sources, and indicative high-risk thresholds for each of the six ATD categories. Thresholds are preliminary and require empirical calibration.

ATD Category	Qualitative Assessment Question	Quantitative Indicator	Primary Evidence Source	High-Risk Threshold
Structural Debt	Is the OT network segmented into security zones with enforced conduit controls?	What percentage of OT assets share a flat broadcast domain with IT or HMI systems?	Network topology diagram; IEC 62443-3-2 zone assessment	High if >30% of OT assets on flat segments
Trust Debt	Do OT assets use authenticated, least-privilege communication, or implicit network-reachability trust?	What percentage of OT assets rely on unauthenticated protocol access (Modbus, legacy OPC)?	Protocol audit; device credential inventory	High if default or absent credentials on >20% of field devices
Dependency Debt	Can any OT component be isolated or replaced without cascading operational impact?	How many OT assets rely on a single vendor protocol or an unsupported OS?	Asset inventory; vendor dependency map	High if >40% of process-critical assets have no viable replacement path
Visibility Debt	Does the organization have OT-aware monitoring covering >80% of OT network traffic?	What is the estimated MTTD for an anomalous command sequence on the OT network?	SIEM/NDR coverage report; MITRE ATT&CK for ICS detection coverage map	High if MTTD >48 hours or monitoring covers <50% of OT segments
Governance Debt	Is there a current, verified asset inventory with lifecycle status for all OT assets?	How many months have elapsed since the OT security policy was last reviewed against the current architecture?	Asset register; policy review log; procurement records	High if the asset register is >2 years old or procurement lacks a security review gate
Resilience Debt	Have OT recovery procedures been tested against a cyber-incident scenario in the past 12 months?	What is the maximum tolerable downtime for each OT zone, and does the architecture support it?	Tested business continuity plan; redundancy architecture review	High if no tested failover exists for any process-critical OT system

The Assessment Matrix is designed to support the ATD registers described in Section 11.1 and to provide input to ATD-MM level determination in Section 10. Operators should apply the matrix at least annually, at each major procurement decision, and following any significant incident or architectural change. The matrix also supports regulatory architectural review assessments under the frameworks proposed in Section 11.2.

13. FUTURE RESEARCH AGENDA

13.1. EMPIRICAL VALIDATION OF PROPOSITIONS P1-P6

The formal propositions advanced in Section 5 provide testable hypotheses for empirical investigation. Priority research directions include: case study validation of the P3 Lateral Reachability Ratio (LRR) across multiple OT environments; measurement of P4 Mean Time to Lateral Movement (MTTLM) in adversary simulation exercises using digital twin environments; and longitudinal study of P6 Post-incident ATD increment to validate the recursive debt

accumulation mechanism. Such studies would provide the empirical grounding necessary to establish ATD risk amplification as an evidence-based rather than theoretical construct.

13.2. ARCHITECTURAL TECHNICAL DEBT INDEX (ATDI)

Future research should develop and validate a composite metric for quantifying ATD across the six taxonomy categories. A weighted linear formulation for the Architectural Technical Debt Index is proposed as follows:

$ATDI = w_s \cdot S_s + w_t \cdot T_s + w_d \cdot D_s + w_v \cdot V_s + w_g \cdot G_s + w_r \cdot R_s$ Where: S_s = Structural Debt Score (0-100) T_s = Trust Debt Score (0-100) D_s = Dependency Debt Score (0-100) V_s = Visibility Debt Score (0-100) G_s = Governance Debt Score (0-100) R_s = Resilience Debt Score (0-100) $w_s, w_t, w_d, w_v, w_g, w_r$ = sector-specific weights, $\sum w = 1.0$ ATDI normalised to 0-100; 100 = maximum architectural debt burden

Each component score is derived from the quantitative indicators defined in the Assessment Matrix (Table 5). The weights ($w_s, w_t, w_d, w_v, w_g, w_r$) require empirical calibration and represent the primary area for future validation research. Until calibrated, initial weights are proposed through structured expert judgment using the Analytic Hierarchy Process (AHP) [40], a multi-criteria decision-making method based on pairwise comparison and consistency assessment of criteria. Alternative calibration pathways include the Entropy Weight Method, which derives weights from the information entropy of observed score distributions, and Delphi consensus approaches, which iteratively aggregate expert judgment toward convergence. For practitioners without access to operational incident data, structured expert panels using established information-security risk-assessment frameworks [41] can provide the domain-grounded input needed to initialize the AHP pairwise comparison matrices. Sector-specific weight sets are expected to differ: structural debt warrants higher weighting in energy generation environments where flat OT networks directly connect to safety-critical control systems; visibility debt warrants higher weighting in water treatment environments; and governance debt warrants higher weighting in emerging economy contexts where lifecycle management capacity is limited. Sensitivity analysis should be conducted to assess how ATDI scores vary across the plausible weight range before weights are fixed for any specific deployment context. The risk-band thresholds (0-20 Low through 81-100 Critical) are proposed as starting estimates rather than empirically validated boundaries and must be calibrated against incident-outcome data before operational use. The following risk band classification is proposed for initial validation research:

Table 6: Proposed ATDI Risk Bands and Governance Implications. The thresholds are indicative and require empirical calibration.

ATDI Range	Risk Band	Governance Implication
0 - 20	Low	ATD is well-managed; it maintains continuous monitoring and ATD-MM progression
21 - 40	Moderate	Debt present but contained; schedule structured remediation within 18 months
41 - 60	Significant	Systemic risk elevated; prioritize segmentation and trust debt reduction immediately
61 - 80	High	Immediate architectural governance intervention required; executive escalation and interim compensating controls
81 - 100	Critical	Structural default risk; emergency compensating controls, and accelerated modernization program with regulatory notification

The ATDI provides a basis for: (a) cross-sector CDI benchmarking studies; (b) longitudinal tracking of ATD trajectories over time within organizations; (c) regulatory disclosure of ATD status as a material cyber risk indicator; and (d) empirical research correlating ATDI values with incident frequency, severity, and recovery duration. The five-band classification enables communication of architectural risk posture to non-technical governance audiences in terms that are proportionate and actionable. A companion paper is proposed, "Quantifying Architectural Technical Debt in Critical Digital Infrastructure: Development and Validation of

the ATDI," to pursue empirical calibration of component scores, sector-specific weights, and risk band thresholds.

13.3. AI-ASSISTED ATD DETECTION

Machine learning approaches offer significant potential for automating ATD detection in large OT environments, an area identified by Biazotto et al. [25] as a priority for technical debt management automation where manual assessment is impractical. Graph-based neural network models applied to network communication topology data could identify structural patterns indicative of flat architecture, implicit trust, or visibility gaps without requiring a complete manual inventory. Natural language processing applied to configuration files and vendor documentation could support governance and dependency debt detection. AI-assisted ATD detection would substantially reduce the cost of ATD register maintenance and enable near-real-time debt tracking at the L5 maturity level.

13.4. DIGITAL TWIN-BASED ATD MEASUREMENT

Digital twin environments offer a controlled platform for empirically quantifying ATD interest, blast radius amplification, MTTD under current visibility conditions, and MTTL, without exposing live systems. Research should develop standardized digital twin experimental protocols for ATD interest measurement, enabling cross-environment comparison and ATDI component score calibration.

13.5. DEBT-AWARE SECURITY ORCHESTRATION

Current SOAR platforms are not ATD-aware. Research into debt-aware orchestration should produce platforms that incorporate ATD context into detection triage and response prioritization, flagging that anomalies on high-ATD network segments warrant escalated response priority because structural conditions amplify potential blast radius, and that automatically recommend ATD remediation actions alongside incident response measures.

13.6. POST-QUANTUM MIGRATION DEBT

OT environments with embedded cryptographic dependencies on classical public-key algorithms face a forthcoming structural migration challenge, as established by NIST's post-quantum cryptography transition guidance [34], [35], whose complexity is compounded by existing ATD. The interaction between current ATD and post-quantum migration requirements is a research frontier demanding early attention, given the long lead times characteristic of OT architecture change and the NIST post-quantum cryptography standardization timeline.

14. CONCLUSION

This paper has advanced a conceptualization of Architectural Technical Debt (ATD) as a structurally embedded category of cyber risk in critical digital infrastructure that is distinct from, and analytically prior to, conventional vulnerability-based risk. The central finding is that accumulated deferred architectural decisions amplify the impact of every vulnerability in an environment by increasing structural complexity, eroding trust boundaries, expanding the attack surface, and reducing resilience. Four specific outputs are produced: (1) a formal ATD definition and six-category taxonomy (Structural, Trust, Dependency, Visibility, Governance, Resilience Debt) aligned to IEC 62443 and NIST SP 800-82 Rev.3; (2) a six-proposition formal risk amplification framework (P1-P6) with named observable indicators, constituting testable hypotheses for future empirical research; (3) a five-level ATD Maturity Model providing a governance progression pathway for operators; and (4) an Architectural Technical Debt Index (ATDI) formulation as a foundation for future measurement research. All propositions, maturity levels, ATDI weights, and risk bands are conceptual in this paper and require empirical validation before operational deployment. This paper is a conceptual contribution; its primary utility is to provide the field with a precise vocabulary and structured framework for a category of risk that currently lacks both.

As established in Section 2, prior literature does not combine technical debt theory with OT security architecture in a unified governance framework. This paper fills that gap.

The implications are consequential across the governance stack. For operators, ATD must be a first-class risk category, measured using the Assessment Matrix, tracked in ATD registers, and governed through the maturity progression of the ATD-MM. For regulators, the taxonomy and Assessment Matrix provide the basis for architectural assessment requirements that go beyond compliance checklists to the structural conditions that determine whether compliance achieves genuine risk reduction. For policymakers, particularly in emerging economies where aging OT infrastructure, capital constraints, and immature regulatory frameworks compound the structural burden, ATD governance can reframe infrastructure investment conversations from reactive incident response toward proactive architectural risk management.

For the research community, the six formal propositions P1–P6 provide a testable empirical agenda, and the ATDI formulation provides a quantification target whose development and validation represent the next critical step in establishing ATD governance as an evidence-based discipline.

Architectural Technical Debt should be regarded not as a by-product of aging infrastructure, but as a first-class systemic cyber risk requiring explicit governance. Just as vulnerability management transformed operational security practice in the early 2000s, ATD governance represents the next evolution in securing critical digital infrastructure. Vulnerability management asks: which components are broken? ATD governance asks: what structural conditions determine what happens when they break? The future resilience of critical infrastructure may depend less on eliminating individual vulnerabilities and more on understanding and governing the architectural debt that determines their consequences. Naming that risk precisely, measuring it rigorously, and governing it deliberately are the prerequisites for the durable cyber resilience on which modern society depends.

REFERENCES

- [1] K. Stouffer *et al.*, "Guide to Operational Technology (OT) Security," *Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NIST SP 800-82 Rev.3*, Jan. 2023, doi: 10.6028/nist.sp.800-82r3.
- [2] W. Cunningham, "The WyCash Portfolio Management System," *Addendum to the proceedings on Object-oriented programming systems, languages, and applications (Addendum) - OOPSLA '92*, vol. 4, no. 2, pp. 29–30, 1992, doi: 10.1145/157709.157715.
- [3] P. Kruchten, R. L. Nord, and I. Ozkaya, "Technical Debt: From Metaphor to Theory and Practice," *IEEE Software*, vol. 29, no. 6, pp. 18–21, Nov. 2012, doi: 10.1109/ms.2012.167.
- [4] N. S. R. Alves, T. S. Mendes, M. G. de Mendonça, R. O. Spínola, F. Shull, and C. Seaman, "Identification and Management of Technical Debt: A Systematic Mapping Study," *Information and Software Technology*, vol. 70, pp. 100–121, Feb. 2016, doi: 10.1016/j.infsof.2015.10.008.
- [5] P. Avgeriou, K. Philippe, I. Ozkaya, and C. Seaman, "Managing Technical Debt in Software Engineering (Dagstuhl Seminar 16162)," *Dagstuhl Reports*, vol. 6, no. 4, pp. 110–138, 2016, doi: 10.4230/DagRep.6.4.110.
- [6] C. Seaman and Y. Guo, "Measuring and Monitoring Technical Debt," *Advances in Computers*, vol. 82, pp. 25–46, 2011, doi: 10.1016/b978-0-12-385512-1.00002-5.
- [7] J. D. Morgenthaler, M. Gridnev, R. Sauciu, and S. Bhansali, "Searching for Build Debt: Experiences Managing Technical Debt at Google," in *2012 Third International Workshop on Managing Technical Debt (MTD)*, Jun. 2012, pp. 1–6.

- [8] Z. Li, P. Avgeriou, and P. Liang, "A Systematic Mapping Study on Technical Debt and Its Management," *Journal of Systems and Software*, vol. 101, pp. 193–220, Mar. 2015, doi: 10.1016/j.jss.2014.12.027.
- [9] N. A. Ernst, S. Bellomo, I. Ozkaya, R. L. Nord, and I. Gorton, "Measure It? Manage It? Ignore It? Software Practitioners and Technical Debt," in *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, Aug. 2015, pp. 50–60.
- [10] International Electrotechnical Commission, "Security for Industrial Automation and Control Systems (IACS)," *IEC 62443 Series (Parts 2-1:2009, 2-3:2015, 3-2:2013, 3-3:2013)*. Geneva, Switzerland: IEC.
- [11] MITRE Corporation, "ATT&CK for Industrial Control Systems (ICS)," attack.mitre.org. [Online]. Available: <https://attack.mitre.org/matrices/ics/>
- [12] X. Pàmies-Morell, J. Ros-Giralt, and J. Soué-Pla, "Technical debt in embedded systems: A systematic literature review," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8447–8458, 2021.
- [13] S. Martínez-Fernández and et al., "Software architecture in the age of cyber-physical systems: A systematic mapping study," *Inf. Softw. Technol.*, vol. 146, p. 106826, 2022.
- [14] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed. Waltham, MA, USA: Syngress, 2014.
- [15] C. Perrow, *Normal Accidents: Living with High-Risk Technologies*. New York, NY, USA: Basic Books, , 1984.
- [16] L. von Bertalanffy, *General System Theory: Foundations, Development, Applications*. New York, NY, USA: George Braziller, 1968.
- [17] M. Howard and J. Pincus, "Measuring relative attack surfaces," in *Workshop Adv. Develop. Softw. Syst. Security*, 2003.
- [18] E. Hollnagel, D. D. Woods, and N. Leveson, Eds., *Resilience Engineering: Concepts and Precepts*. Aldershot, U.K.: Ashgate, 2006.
- [19] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA, USA: MIT Press, 2011.
- [20] E. L. Trist and K. W. Bamforth, "Some Social and Psychological Consequences of the Longwall Method of Coal-Getting," *Human Relations*, vol. 4, no. 1, pp. 3–38, Feb. 1951, doi: <https://doi.org/10.1177/001872675100400101>.
- [21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, vol. 1, no. 800–207, Aug. 2020, doi: 10.6028/nist.sp.800-207.
- [22] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," *Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NIST CSWP 29*, Feb. 2024, doi: 10.6028/nist.cswp.29.
- [23] U.S. Cybersecurity and Infrastructure Security Agency (CISA), "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Security-by-Default," www.cisa.gov. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/secure-by-design>

- [24] T. Besker, A. Martini, and J. Bosch, "Managing Architectural Technical Debt: A Unified Model and Systematic Literature Review," *Journal of Systems and Software*, vol. 135, pp. 1–16, Jan. 2018, doi: 10.1016/j.jss.2017.09.025.
- [25] J. P. Biazotto, D. Feitosa, P. Avgeriou, and E. Y. Nakagawa, "Technical Debt Management Automation: State of the Art and Future Perspectives," *Information and Software Technology*, vol. 167, p. 107375, Dec. 2023, doi: 10.1016/j.infsof.2023.107375.
- [26] F. Bi, B. Vogel-Heuser, Z. Huang, and F. Ocker, "*Characteristics, causes, and consequences of technical debt in the automation domain*," *Journal of Systems and Software*, vol. 204, Art. no. 111725, Oct. 2023, doi: 10.1016/j.jss.2023.111725. (Journal title in italics).
- [27] Y. Yang, D. Verma, and P. S. Anton, "Technical Debt in the Engineering of Complex Systems," *Systems Engineering*, vol. 26, no. 5, pp. 590–603, Apr. 2023, doi: 10.1002/sys.21677.
- [28] M. Masi, G. P. Sellitto, H. Aranha, and T. Pavleska, "Securing Critical Infrastructures With a Cybersecurity Digital Twin," *Software and Systems Modeling*, vol. 22, no. 2, pp. 689–707, Jan. 2023, doi: 10.1007/s10270-022-01075-0.
- [29] O. Michalec, S. Milyaeva, and A. Rashid, "When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures?," *Big Data & Society*, vol. 9, no. 1, p. 205395172211083, Jan. 2022, doi: 10.1177/20539517221108369.
- [30] A. Staves, T. Anderson, H. Balderstone, B. Green, A. Gouglidis, and D. Hutchison, "A Cyber Incident Response and Recovery Framework to Support Operators of ICS and Critical National Infrastructure," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100505, Jan. 2022, doi: 10.1016/j.ijcip.2021.100505.
- [31] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, no. 2169–3536, pp. 57143–57179, May 2022, doi: 10.1109/access.2022.3174679.
- [32] Y. Jiang, M. A. Jeusfeld, M. Mosaad, and N. Oo, "Enterprise architecture modeling for cybersecurity analysis in critical infrastructures: A systematic literature review," *International Journal of Critical Infrastructure Protection*, vol. 46, p. 100700, Sep. 2024, doi: 10.1016/j.ijcip.2024.100700.
- [33] E. C. Balta, M. Pease, J. Moyne, K. Barton, and D. M. Tilbury, "Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems," *IEEE Transactions on Automation Science and Engineering*, vol. 21, no. 2, pp. 1695–1712, Apr. 2024, doi: 10.1109/tase.2023.3243147.
- [34] A. Regenscheid, "Transition to Post-Quantum Cryptography Standards," *NIST Interagency Report (IR) 8547, Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, MD, USA*, Nov, 2024, doi: 10.6028/nist.ir.8547.ipd.
- [35] W. Newhouse *et al.*, "Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery Volume B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools," 2023. [Online]. Available: <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf>
- [36] H. I. Kure, S. Islam, and H. Mouratidis, "An Integrated Cyber Security Risk Management Framework and Risk Predication for the Critical Infrastructure Protection," *Neural Computing and Applications*, vol. 34, no. 18, pp. 15241–15271, Feb. 2022, doi: <https://doi.org/10.1007/s00521-022-06959-2>.

- [37] P. Avgeriou *et al.*, "Technical Debt Management: The Road Ahead for Successful Software Delivery," in *IEEE/ACM Int. Conf. Softw. Eng.: Future Softw. Eng. (ICSE-FoSE)*, Melbourne, Australia, May 2023, pp. 15–30.
- [38] X. Feng and S. Hu, "Cyber-Physical Zero Trust Architecture for Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 394–405, 2023, doi: 10.1109/ticps.2023.3333850.
- [39] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering,," EBSE Technical Report EBSE-2007-01, Keele University and Durham University, U.K, 2007.
- [40] T. L. Saaty, *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. New York, NY, USA: McGraw-Hill, 1980.
- [41] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)," *Computers & Security*, vol. 57, pp. 14–30, Mar. 2016, doi: 10.1016/j.cose.2015.11.001.