Review of Applied Science and Technology

Volume: 1; Issue: 4
Pages: 146– 182

ADVANCED CYBERSECURITY ARCHITECTURES FOR RESILIENCE IN U.S. CRITICAL INFRASTRUCTURE CONTROL NETWORKS

Jabed Hasan Tarek[1]; Waladur Rahman[2]

[1]. Graduate Research Assistant, Department of Electrical & Electronic Engineering, Premier University, Chittagong, Bangladesh; Email: jabedhasan932@gmail.com

[2]. Researcher, American International University of Bangladesh; Email: w.rifat99@gmail.com

Doi: 10.63125/5rvjav10
Received: 15 September 2022; **Revised:** 24 October 2022; **Accepted:** 15 November 2022; **Published:** 26 December 2022

Abstract

This study examined predictive analytics for risk and compliance in IT-enabled project management systems by modeling how operational performance indicators and governance-control indicators jointly explained adverse project outcomes. A retrospective quantitative design was applied to 312 projects drawn from an initial pool of 353, with 41 projects excluded for incomplete baselines or missing workflow trails, producing an inclusion rate of 88.4%. The sample comprised 39.7% infrastructure projects (n = 124), 34.6% software/IT delivery projects (n = 108), and 25.6% mixed/operational projects (n = 80). Descriptive analysis indicated that 29.5% of projects met the schedule distress criterion (n = 92) and 20.5% met the cost distress criterion (n = 64), while 13.1% met the combined distress definition (n = 41). Compliance deviations were recorded in 17.9% of projects (n = 56), with repeated exceptions in 7.4% (n = 23). Key variables showed heavy-tailed distributions, including change requests with a mean of 9.8, median 7.0, and maximum 88, and documentation completeness with a mean of 91.6%, median 94.0%, and missingness of 11.5%; access-control anomaly indicators had the highest missingness at 18.6%. Correlation results showed alignment between instability and governance signals, including schedule variance with cost variance (r = .46) and change intensity (r = .41), and documentation completeness with exception recurrence (ρ = −.52) and approval latency with exception recurrence (ρ = .44). Stratified results showed stronger schedule variance–change coupling in software/IT projects (r = .48) than infrastructure projects (r = .31), and stronger late-phase governance–exception relationships for approval latency (ρ = .57) than early phase (ρ = .28). Reliability testing supported construct consistency with a = .88 for governance adherence, a = .91 for documentation completeness, and a = .84 for workflow conformance. Collinearity reduction lowered maximum VIF from 7.4 to 3.4 and maximum condition index from 28.3 to 17.6. Regression findings showed risk distress was positively associated with schedule variance (β = 0.41, p < .001) and change intensity (β = 0.29, p = .002), while compliance exceptions were strongly associated with documentation completeness (β = −0.47, p < .001) and approval adherence (β = −0.39, p < .001). Model performance improved with governance predictors, increasing AUC from 0.68 to 0.83 for risk distress and from 0.66 to 0.86 for compliance exceptions, with top-decile capture reaching 61% for risk distress and 69% for compliance exceptions.

Keywords

Predictive Analytics; Project Risk; Compliance Monitoring; IT-Enabled Governance; Project Management Systems.

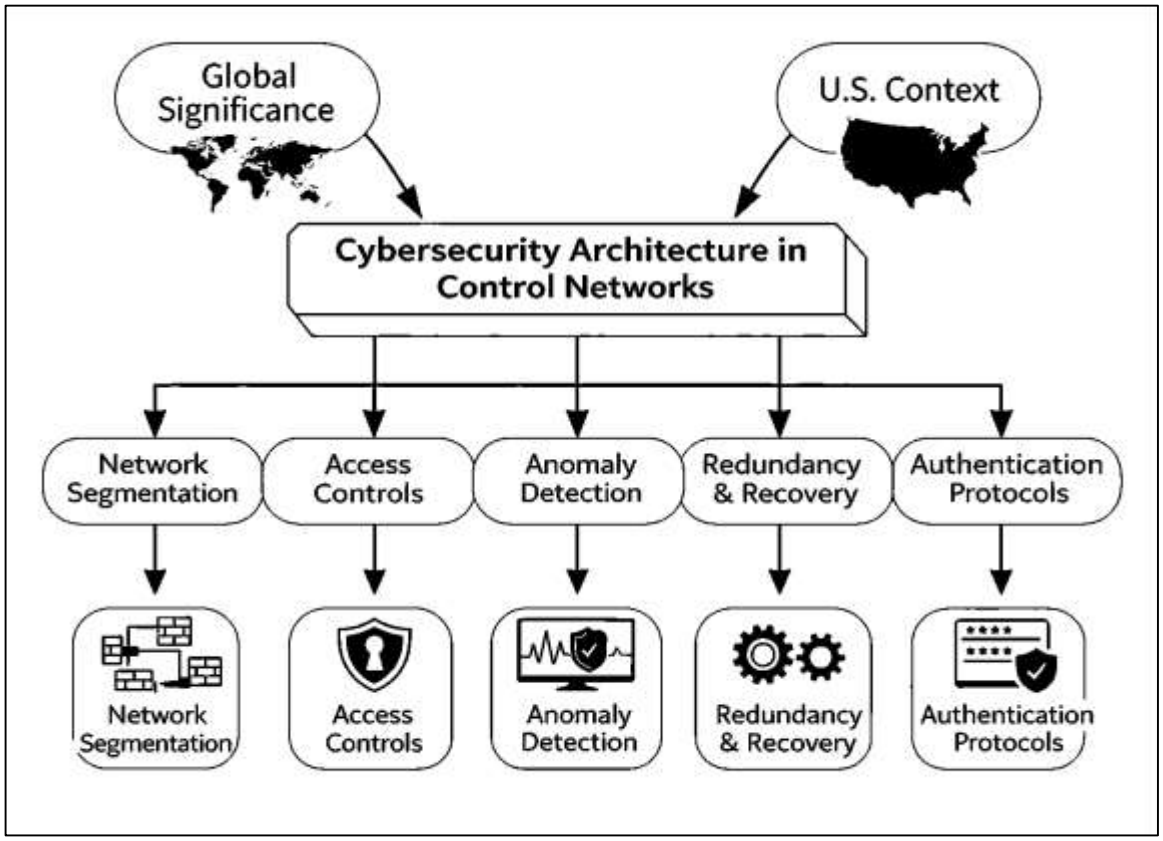
INTRODUCTION

Cybersecurity architecture refers to the structured design of policies, technologies, processes, and control mechanisms that collectively protect information systems and operational assets from unauthorized access, disruption, or manipulation. Within the domain of critical infrastructure control networks, cybersecurity architectures encompass layered defensive models integrating hardware, software, communication protocols, and governance frameworks that collectively maintain system integrity and operational continuity (Brennan et al., 2019). Control networks, commonly operationalized through Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS), form the technological backbone of energy grids, water treatment facilities, transportation systems, and industrial manufacturing environments. These systems differ fundamentally from traditional information technology networks due to their real-time operational constraints, deterministic communication requirements, and direct interaction with physical processes. As a result, cybersecurity architectures in control networks must balance computational security mechanisms with system availability, latency tolerance, and safety requirements. Quantitative cybersecurity research conceptualizes these architectures as measurable constructs composed of identifiable variables such as attack surface exposure, network segmentation depth, anomaly detection accuracy, response latency, and system recovery time (Siddiqui et al., 2019). Internationally, the formalization of cybersecurity architecture has evolved alongside standards developed by organizations such as the International Organization for Standardization, the International Electrotechnical Commission, and the National Institute of Standards and Technology, which provide structured taxonomies for assessing cyber risk in industrial environments. In this context, resilience is defined as the quantifiable capacity of a control network to sustain essential functions under adverse cyber conditions while maintaining measurable performance thresholds. The integration of architectural security principles within control networks reflects a shift from isolated technical safeguards toward systemic, data-driven security models that emphasize structural robustness (Bodeau et al., 2014). Quantitative inquiry into cybersecurity architectures therefore focuses on evaluating how architectural configurations influence measurable security outcomes, operational reliability metrics, and systemic fault tolerance across critical infrastructure environments.

Critical infrastructure control networks hold global significance due to their central role in sustaining economic stability, public safety, and national security across interconnected societies. International supply chains, cross-border energy grids, global transportation corridors, and transnational communication systems increasingly depend on interoperable control networks governed by heterogeneous cybersecurity standards. Cyber incidents targeting control systems have demonstrated measurable transnational impacts, including economic losses, service disruptions, and cascading system failures affecting multiple jurisdictions simultaneously (Zhou et al., 2020). From a quantitative perspective, the international significance of cybersecurity resilience is reflected in comparative risk indices, infrastructure dependency models, and cross-national incident frequency analyses that document the systemic vulnerabilities of control networks. Global cybersecurity frameworks emphasize the harmonization of architectural security principles to address asymmetries in technical maturity, regulatory enforcement, and threat exposure. Empirical studies have documented statistically significant correlations between infrastructure digitalization levels and the probability of cyber-induced operational disruptions, highlighting the necessity of robust architectural controls. In control networks, resilience metrics such as mean time to failure, mean time to recovery, and fault propagation probability are increasingly used to benchmark system performance across national contexts. The international discourse on cybersecurity architecture also reflects geopolitical considerations, as state-sponsored cyber activities introduce persistent threats to infrastructure sovereignty (Siu et al., 2019). Quantitative assessments conducted by international agencies demonstrate that control network vulnerabilities exhibit non-linear escalation patterns when architectural segmentation and authentication controls are insufficiently enforced. These findings underscore the importance of standardized architectural resilience models capable of supporting cross-border infrastructure interoperability. The global interdependence of critical infrastructure systems positions cybersecurity architecture as a measurable determinant of systemic stability rather than a localized technical concern. Consequently, quantitative research in this domain contributes to an

evidence-based understanding of how architectural design choices influence resilience outcomes across diverse regulatory and operational environments (Prokhorenko & Babar, 2020).

Figure 1: Cybersecurity Architecture for Control Networks

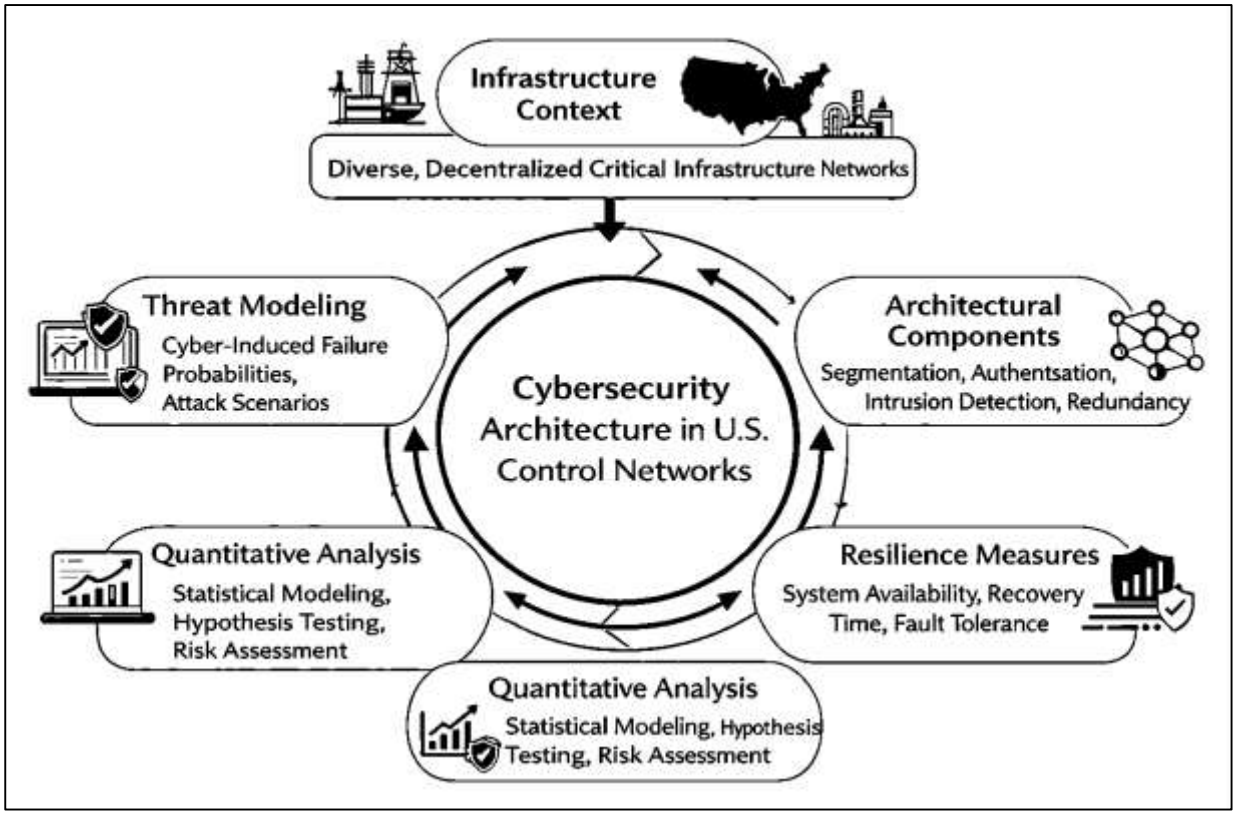


The United States represents a highly relevant empirical context for quantitative examination of cybersecurity architectures due to the scale, diversity, and decentralization of its critical infrastructure control networks. U.S. infrastructure systems encompass investor-owned utilities, federally regulated entities, state-managed facilities, and privately operated industrial networks, resulting in heterogeneous architectural implementations. Control networks within the U.S. energy, water, transportation, and manufacturing sectors are characterized by legacy system integration, protocol diversity, and variable cybersecurity maturity levels (Choras et al., 2015). Quantitative studies have identified statistically observable disparities in security posture across infrastructure sectors, driven by differences in investment levels, regulatory oversight, and technological modernization rates. U.S. policy frameworks emphasize risk-based cybersecurity management, promoting architectural assessments grounded in measurable performance indicators rather than prescriptive compliance alone. Control networks operating within this environment generate extensive operational telemetry, enabling quantitative modeling of intrusion detection accuracy, network traffic anomalies, and system response behaviors. Empirical analyses frequently employ multivariate regression, network simulation, and probabilistic risk modeling to evaluate how architectural configurations influence resilience outcomes. The U.S. context also provides longitudinal data on cyber incident reporting, enabling time-series analysis of attack frequency and system recovery metrics. Control network architectures in the U.S. are further influenced by sector-specific reliability standards, which introduce quantifiable thresholds for system availability and operational continuity (Linkov & Kott, 2019). These characteristics make U.S. critical infrastructure control networks particularly suitable for quantitative evaluation of architectural resilience constructs, allowing researchers to isolate the statistical relationships between security design variables and measurable system performance indicators.

Cybersecurity architectures for control networks are composed of discrete components that can be

operationalized as quantitative variables for empirical analysis. These components include network segmentation strategies, access control mechanisms, authentication protocols, intrusion detection systems, and redundancy configurations (Varadharajan & Tupakula, 2016). Each architectural element contributes to the overall resilience profile of the control network by influencing attack containment probability, detection latency, and recovery efficiency. Quantitative cybersecurity research models these components using metrics such as segmentation depth, privilege escalation frequency, false positive detection rates, and system downtime duration. Architectural layering enables statistical evaluation of defense-in-depth effectiveness by examining how multiple controls interact under simulated or observed attack conditions. Control networks generate high-resolution operational data that support the application of statistical learning techniques to identify correlations between architectural design choices and security outcomes (Galinec & Steingartner, 2017). Empirical studies have employed stochastic modeling to assess fault tolerance thresholds within segmented network architectures.

Figure 2: Quantitative Cybersecurity Architecture Framework



The integration of redundancy mechanisms introduces measurable trade-offs between system complexity and resilience capacity, which can be evaluated using performance optimization models. Architectural consistency across distributed control nodes further influences synchronization reliability and failure propagation patterns. Quantitative assessment of these architectural components supports hypothesis-driven analysis of resilience determinants within control networks, allowing for empirical validation of security design principles through observable system behavior (Scala et al., 2019).

Cyber threats targeting control networks exhibit measurable characteristics that can be systematically analyzed within quantitative research frameworks. Threat vectors such as malware propagation, unauthorized command injection, and denial-of-service attacks generate observable patterns in network traffic, system logs, and operational performance metrics. Quantitative risk characterization involves modeling threat likelihood, impact magnitude, and exploit feasibility using probabilistic methods. Control network vulnerabilities can be quantified through exposure indices that incorporate protocol weaknesses, authentication gaps, and system interconnectivity levels (Klingensmith & Madni,

2017). Empirical threat modeling studies have demonstrated statistically significant relationships between architectural complexity and vulnerability surface area. Quantitative cybersecurity research applies Bayesian inference, Monte Carlo simulation, and survival analysis to estimate the probability distributions of cyber-induced system failures. Control networks operating under constrained real-time conditions exhibit unique threat dynamics, where minor disruptions can escalate into large-scale operational consequences. Statistical analyses of historical incident datasets reveal patterns of attack recurrence and system recovery variability (Mohiul, 2020; Phillips et al., 2018). These findings support the development of measurable threat models that align cybersecurity architecture design with empirically observed risk profiles.

Resilience in cybersecurity architecture is conceptualized as a multidimensional construct encompassing resistance, absorption, adaptation, and recovery capacities. Quantitative resilience modeling translates these dimensions into measurable indicators such as system availability ratios, recovery time distributions, and functional degradation thresholds. Control networks provide a suitable environment for resilience measurement due to their continuous operation and deterministic performance requirements. Empirical resilience studies utilize system dynamics modeling to capture the interactions between architectural controls and operational stability (Jinnat & Kamrul, 2021; Qi et al., 2016). Statistical resilience indices aggregate multiple performance metrics into composite scores that enable comparative analysis across infrastructure sectors. Control network resilience is further influenced by architectural redundancy, failover mechanisms, and automated response capabilities, each of which can be evaluated using performance benchmarking techniques. Quantitative resilience assessment enables the identification of structural vulnerabilities that may not be evident through qualitative analysis alone. By operationalizing resilience as a measurable system property, quantitative research establishes an empirical foundation for evaluating cybersecurity architecture effectiveness within critical infrastructure control networks (Rabiul & Samia, 2021; Panda & Bower, 2020).

Quantitative cybersecurity research emphasizes hypothesis testing, variable measurement, and statistical inference to examine the relationships between architectural design and resilience outcomes. Control networks generate structured datasets suitable for inferential analysis, including time-stamped event logs, sensor telemetry, and performance records (Blom et al., 2016; Mohiul & Rahman, 2021). Quantitative methodologies applied in this domain include regression analysis, structural equation modeling, and network graph analytics. These methods enable researchers to isolate the effects of architectural variables while controlling for confounding operational factors. The use of quantitative models supports reproducibility and generalizability of findings across infrastructure contexts. Empirical cybersecurity architecture studies contribute to theory development by validating conceptual models through observable system behavior. Quantitative analysis also facilitates benchmarking across organizations and sectors by standardizing resilience metrics (Rahman & Abdul, 2021; Sridhar et al., 2017). This research orientation positions cybersecurity architecture as a measurable determinant of infrastructure stability, grounded in data-driven evaluation rather than descriptive assessment (Haider & Shahrin, 2021).

This quantitative study is guided by a set of measurable objectives focused on examining how advanced cybersecurity architectures shape resilience outcomes in U.S. critical infrastructure control networks. The first objective is to operationalize "advanced cybersecurity architecture" as a quantifiable construct by translating architectural elements—such as segmentation depth, identity and access control strictness, monitoring coverage, protocol hardening, and redundancy design—into measurable indicators that can be consistently captured across control-network environments. The second objective is to develop and validate a resilience measurement framework suitable for industrial control networks by defining dependent variables that reflect resilience performance in observable terms, including system availability, anomaly detection latency, containment effectiveness, service degradation magnitude, mean time to recovery, and operational stability under adverse events. The third objective is to statistically test the relationships between architectural indicators and resilience metrics using inferential models that estimate effect sizes, significance, and explanatory power while controlling for confounding operational factors such as asset age, protocol diversity, network size, operational criticality, and baseline cybersecurity maturity. A fourth objective is to compare resilience performance across architectural profiles by classifying control-network implementations into

structured groups (for example, high segmentation–high monitoring versus low segmentation–limited visibility) and evaluating whether the distributions of resilience outcomes differ significantly across groups using appropriate hypothesis tests. The fifth objective is to identify the most influential architectural predictors of resilience through multivariate modeling and robustness checks, enabling the ranking of architectural variables by their contribution to resilience variance and by their stability across alternative model specifications. A sixth objective is to evaluate measurement reliability and model validity by applying internal consistency checks, sensitivity analyses, and diagnostic assessments that ensure the empirical results reflect genuine architectural-resilience relationships rather than measurement noise or model misspecification. Collectively, these objectives structure the study around measurable variables, testable relationships, and replicable statistical procedures, ensuring that the analysis remains anchored in quantifiable evidence derived from control-network security architecture and operational performance data.

LITERATURE REVIEW

The literature review in this quantitative study consolidates and organizes empirical scholarship on advanced cybersecurity architectures and resilience measurement in U.S. critical infrastructure control networks. The purpose of this section is to establish a structured evidence base for how architectural controls in ICS/SCADA environments are operationalized as measurable variables, how resilience is quantified through performance indicators, and how statistical methods have been applied to test relationships between architecture design and resilience outcomes. Because control networks differ from conventional IT systems through real-time constraints, safety-critical operations, and protocol heterogeneity, the reviewed literature is organized around quantitatively testable constructs such as segmentation depth, visibility coverage, authentication strength, anomaly detection accuracy, response latency, and recovery time distributions. The section also synthesizes how researchers have modeled cyber risk and resilience using inferential and predictive techniques, including regression-based testing, probabilistic risk modeling, time-to-event analysis, and network-graph metrics. In addition, the literature review maps out measurement approaches used to convert technical security practices into numerical indicators, enabling benchmarking across infrastructure sectors and facilitating reproducible statistical evaluation. Overall, this review provides a quantitative grounding for the study variables, measurement logic, and analytical models, ensuring the research design is aligned with validated empirical patterns and established operational metrics in critical infrastructure cybersecurity research.

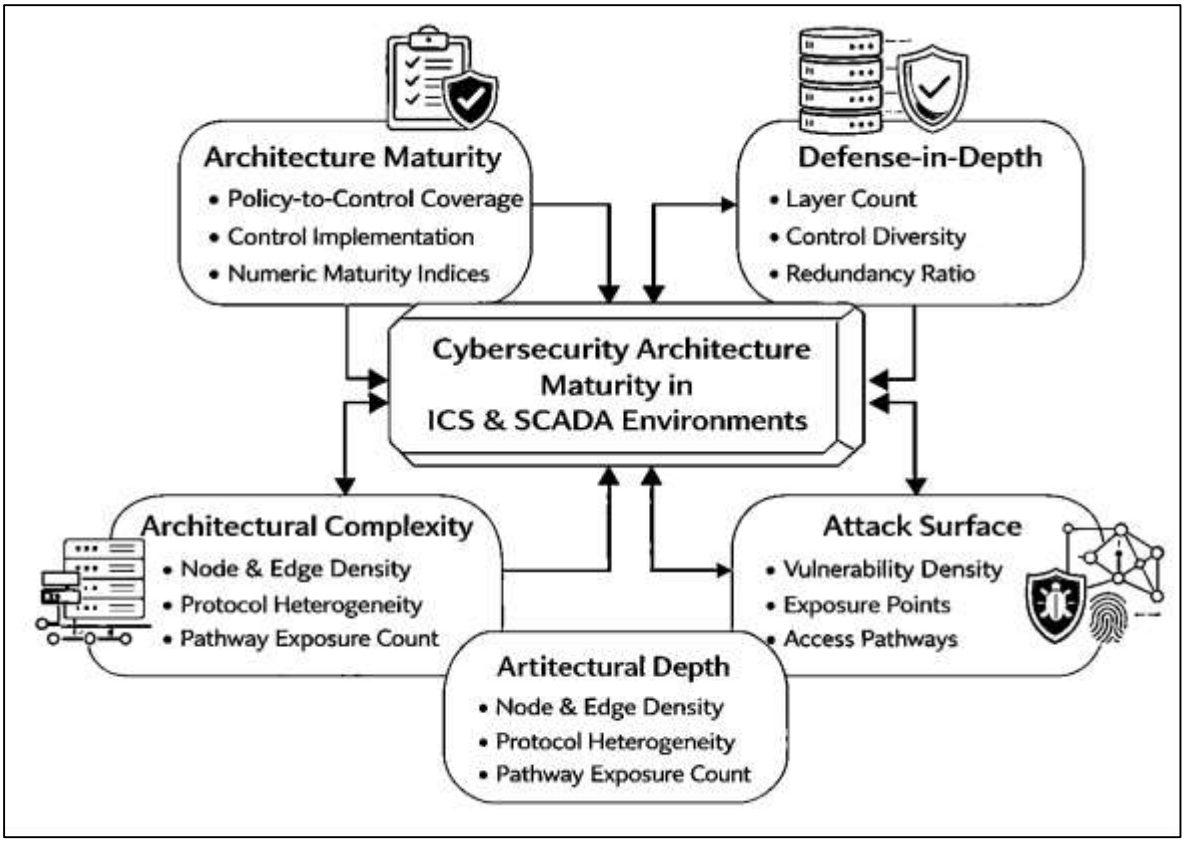
ICS/SCADA Cybersecurity Architecture Constructs

The concept of cybersecurity architecture maturity in ICS and SCADA environments has been extensively discussed in the literature as a means of translating abstract security postures into quantifiable and comparable constructs. Scholars commonly describe architecture maturity as the degree to which security policies, technical controls, governance mechanisms, and operational practices are systematically aligned and consistently implemented across control networks. Within industrial environments, maturity is not treated as a binary condition but rather as a graded continuum reflecting incremental levels of capability and control integration (Tan et al., 2020). The literature emphasizes numeric operationalization through maturity indices, weighted scoring models, and capability rating scales that assign measurable values to architectural attributes. These models typically aggregate indicators such as the proportion of documented policies mapped to active controls, the density of deployed security mechanisms across network zones, and the consistency of enforcement across operational assets. Quantitative studies highlight the importance of policy-to-control coverage ratios as indicators of alignment between governance intent and technical execution. Control implementation density is also widely discussed as a measurable proxy for architectural robustness, reflecting the distribution of authentication, monitoring, and segmentation mechanisms across system layers (Ferguson et al., 2014; Akbar & Sharmin, 2022; Zulqarnain & Subrato, 2021). Researchers consistently note that maturity scoring frameworks enable cross-organizational benchmarking and statistical comparison of control networks operating under different regulatory and operational conditions. The literature further underscores that numeric maturity representations facilitate empirical testing by allowing architecture maturity to function as an independent variable in statistical models examining resilience, detection effectiveness, and recovery performance. Through this quantitative framing, architecture maturity emerges as a measurable construct that bridges governance structures and

technical enforcement in ICS/SCADA cybersecurity research (Foysal & Subrato, 2022; Onwubiko, 2020; Rahman, 2022).

Defense-in-depth is a foundational architectural principle in control network cybersecurity literature and is consistently framed as a quantifiable design characteristic rather than a purely conceptual strategy. In ICS and SCADA contexts, defense-in-depth is operationalized through the presence and interaction of multiple security layers deployed across physical, network, system, and application domains. The literature describes layer count as a basic yet informative metric, representing the number of distinct security barriers an adversary must traverse to reach critical control assets. Beyond simple counts, researchers emphasize control diversity as a measurable dimension, reflecting the variety of security mechanisms employed, such as firewalls, intrusion detection systems, authentication controls, and protocol enforcement tools (Canaan et al., 2020; Zulqarnain, 2022).

Figure 3: ICS–SCADA Cybersecurity Architecture Framework



Control overlap coefficients are frequently discussed as indicators of whether multiple controls address the same threat vectors, enhancing containment capacity. Redundancy ratios further quantify architectural resilience by measuring the availability of backup controls or alternate operational pathways relative to asset criticality. Studies consistently report that architectures with higher redundancy-to-criticality ratios exhibit greater stability under stress conditions. The literature also notes that quantitative representations of defense-in-depth enable comparative analysis across infrastructure sectors by standardizing how layered security is assessed (Ashok et al., 2017). By translating architectural layering into numeric indicators, researchers are able to examine statistical associations between defense-in-depth configurations and outcomes such as attack containment, operational continuity, and fault tolerance. This body of work positions defense-in-depth as a measurable architectural property that directly supports empirical evaluation in control network cybersecurity studies.

Architectural complexity is widely recognized in the literature as a defining characteristic of ICS and SCADA systems and is increasingly examined through quantitative metrics. Complexity arises from the interconnection of heterogeneous devices, legacy components, proprietary protocols, and

distributed control logic. Researchers describe architectural complexity as a measurable construct that influences both system functionality and cybersecurity exposure (Conklin & Shoemaker, 2017). Common metrics discussed include node density, which captures the number of interconnected devices within a control network, and edge density, which reflects the volume of communication pathways among those devices. Protocol heterogeneity indices are also emphasized as numeric representations of the diversity of communication standards operating simultaneously within a network. The literature notes that higher heterogeneity often correlates with increased configuration burden and monitoring difficulty. Pathway exposure count is another frequently cited metric, representing the number of distinct communication routes through which unauthorized access could propagate (Tran et al., 2016). Quantitative studies consistently demonstrate that architectural complexity metrics provide valuable inputs for statistical models assessing vulnerability concentration and system fragility. Researchers argue that complexity metrics enable objective comparison of control networks that would otherwise appear qualitatively similar. By operationalizing complexity numerically, the literature supports empirical testing of how interconnectedness and diversity affect manageability, observability, and exposure in industrial cybersecurity architectures (Genge et al., 2017). The literature increasingly frames attack surface as a quantifiable outcome influenced by architectural maturity, defense-in-depth, and complexity characteristics. Attack surface is described as the cumulative set of points through which a system can be accessed, manipulated, or disrupted, and researchers consistently seek numeric representations to support empirical analysis. Studies frequently link higher node density, greater protocol diversity, and increased pathway exposure counts with expanded attack surfaces in control networks. Statistical analyses in the literature demonstrate measurable associations between architectural complexity metrics and vulnerability density, indicating that more interconnected architectures present a larger number of exploitable conditions. At the same time, research highlights that higher architecture maturity scores and stronger defense-in-depth indicators are associated with constrained attack propagation and reduced exploit reachability (Xu et al., 2018). The literature emphasizes the use of correlation analysis, regression modeling, and network analytics to examine how architectural variables contribute to observable attack surface characteristics. These studies collectively demonstrate that attack surface expansion is not random but structurally shaped by architectural design choices. By integrating maturity indices, layering metrics, and complexity indicators into statistical frameworks, the literature establishes a data-driven foundation for analyzing how cybersecurity architecture constructs influence exposure levels in ICS and SCADA environments. This synthesis reinforces the role of quantitative architectural assessment in understanding and comparing control network security postures (Vittor et al., 2017).

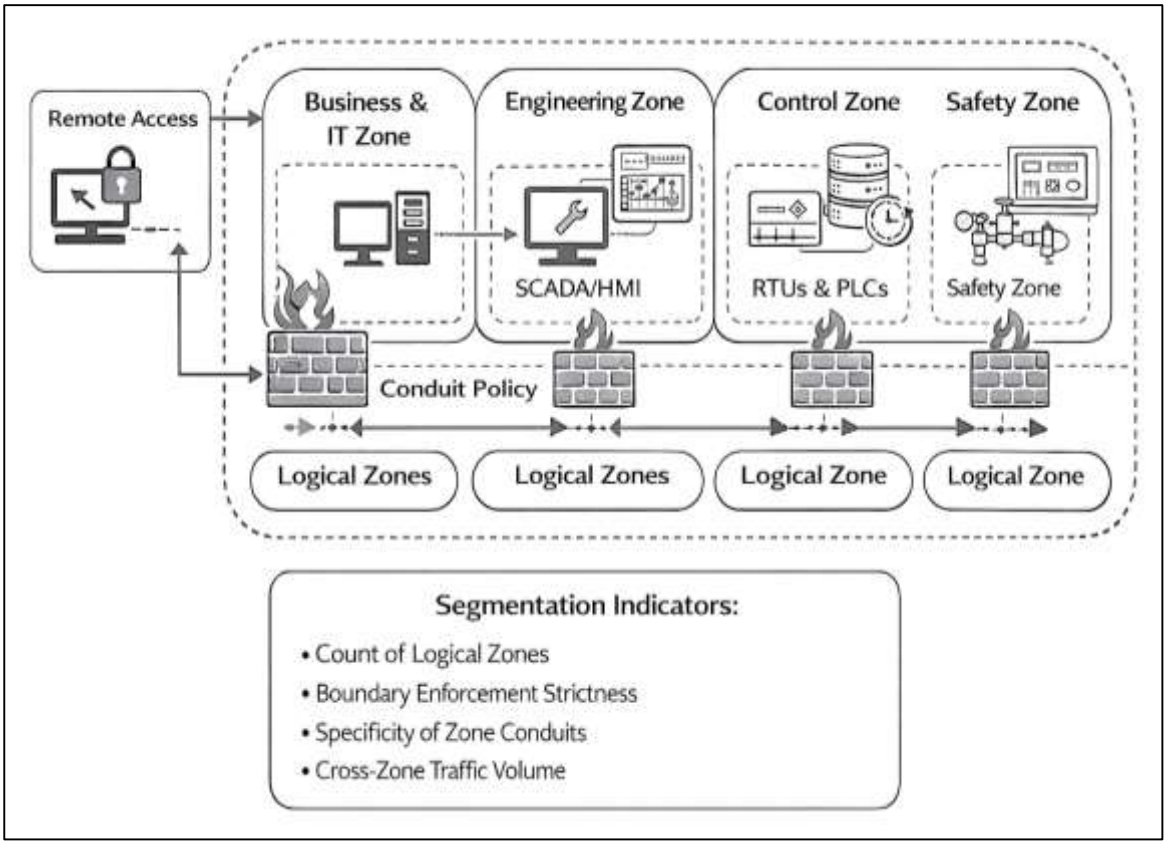
Micro-Segmentation Models in Control Networks

Quantitative scholarship on ICS/SCADA security consistently treats network segmentation as an architectural construct that can be operationalized into measurable indicators suitable for statistical comparison across critical infrastructure settings. Segmentation depth is commonly represented through observable structural properties, including the number of logical zones, the specificity and restrictiveness of conduit policies connecting zones, and the realized isolation strength achieved through enforcement mechanisms (Januário et al., 2019). In industrial control networks, segmentation is frequently discussed through the lens of zone-and-conduit architectures where critical assets, safety systems, historian servers, engineering workstations, and business IT interfaces are placed into discrete security domains. Quantitative literature operationalizes this design by using measurable variables such as the count of security zones, the intensity of boundary enforcement across conduits, and the volume or proportion of cross-zone traffic as a proxy for segmentation effectiveness. VLAN counts and subnet boundaries appear frequently as measurable segmentation primitives, yet studies emphasize that VLAN presence alone does not represent isolation strength unless combined with enforced access control rules, authenticated pathways, and strict traffic allowlists (Buinevich & Vladyko, 2019). The concept of conduit policy strictness is often represented through rule granularity, the ratio of permitted-to-denied flows, protocol restrictions, and the degree to which conduits limit bidirectional communication. Cross-zone traffic volume is treated as a behavioral indicator, capturing how often segmentation boundaries are traversed during normal operations and how large the operational exposure becomes if boundary controls are misconfigured. This body of literature frames segmentation

depth as a measurable structural variable that supports empirical testing, allowing researchers to compare segmented architectures across facilities and to associate segmentation indicators with downstream outcomes such as containment, detection efficiency, and operational continuity under cyber stress (Rieger et al., 2020).

The literature positions segmentation and micro-segmentation as key architectural mechanisms for reducing lateral movement opportunities in control networks, with containment conceptualized as a measurable outcome rather than a descriptive claim. Lateral movement in ICS environments is commonly framed as the attacker's ability to pivot between hosts, traverse trust boundaries, and escalate toward high-impact control functions, often beginning at boundary-facing systems such as remote access gateways, engineering workstations, or IT–OT integration points. Quantitative studies examine containment rate as the proportion of intrusion attempts that remain restricted to an initial foothold zone, reflecting whether segmentation boundaries disrupt propagation (Babiceanu & Seker, 2019).

Figure 4: Quantitative Network Segmentation in ICS/SCADA



Mean attack path length is discussed as a measurable indicator derived from network topology and policy constraints, representing how many transitions an adversary must complete to reach critical nodes. Breach propagation probability appears as another measurable outcome, capturing the likelihood that compromise extends across zones under specified access rules, credential exposure conditions, or monitoring coverage. The literature also highlights that micro-segmentation introduces finer-grained policy boundaries at the workload, device, or application level, transforming lateral movement from a broad network traversal problem into a constrained sequence of permitted flows (Leszczyna, 2018). Studies using attack-graph reasoning and network analytics describe how segmentation reduces reachable exploit paths, increases the number of chokepoints, and concentrates security enforcement at predictable boundaries. These works also describe containment effects in terms of reduced reachable sets, reduced pivotability, and lower transition feasibility under allowlist-driven conduits. Across the literature, the common quantitative framing is that segmented architectures reshape the probability distribution of attacker progress by constraining movement pathways and

increasing the number of enforced boundary crossings required for escalation.

Quantitative research also connects segmentation design to operational performance outcomes by examining downtime magnitude and recovery duration as dependent variables affected by containment strength and incident scope (Khan et al., 2020). Industrial control environments provide measurable operational continuity indicators, enabling studies to examine whether segmented architectures correspond to shorter disruption windows, lower service degradation, and faster restoration. In this literature, downtime is commonly treated as total disruption duration, frequency of service interruption events, or cumulative operational loss time within a defined period. Recovery duration is often operationalized through time-to-restore metrics that capture the length between incident detection, containment completion, and restoration of safe operational states. Statistical approaches reported in this domain include group-based comparisons between segmented and flat architectures using variance-based testing, model-based estimation of downtime while controlling for organizational and technical covariates, and time-to-event approaches that treat restoration as an event outcome with measurable hazard or duration characteristics (Wang & Govindarasu, 2020). Regression frameworks are frequently discussed as tools for estimating how segmentation indicators—such as zone count, boundary strictness, and cross-zone flow rates—relate to downtime while accounting for factors like legacy asset density, patch latency, protocol diversity, and monitoring coverage. Some studies describe survival-style reasoning for restoration time by focusing on the distribution of recovery durations across incidents and comparing duration patterns across architecture profiles. In this body of work, segmentation is treated as an explanatory factor that influences incident spread, which in turn shapes operational disruption length and restoration complexity. This quantitative focus enables segmentation to be evaluated not only as a security control but also as a structural feature with measurable associations to continuity outcomes (Jin et al., 2017).

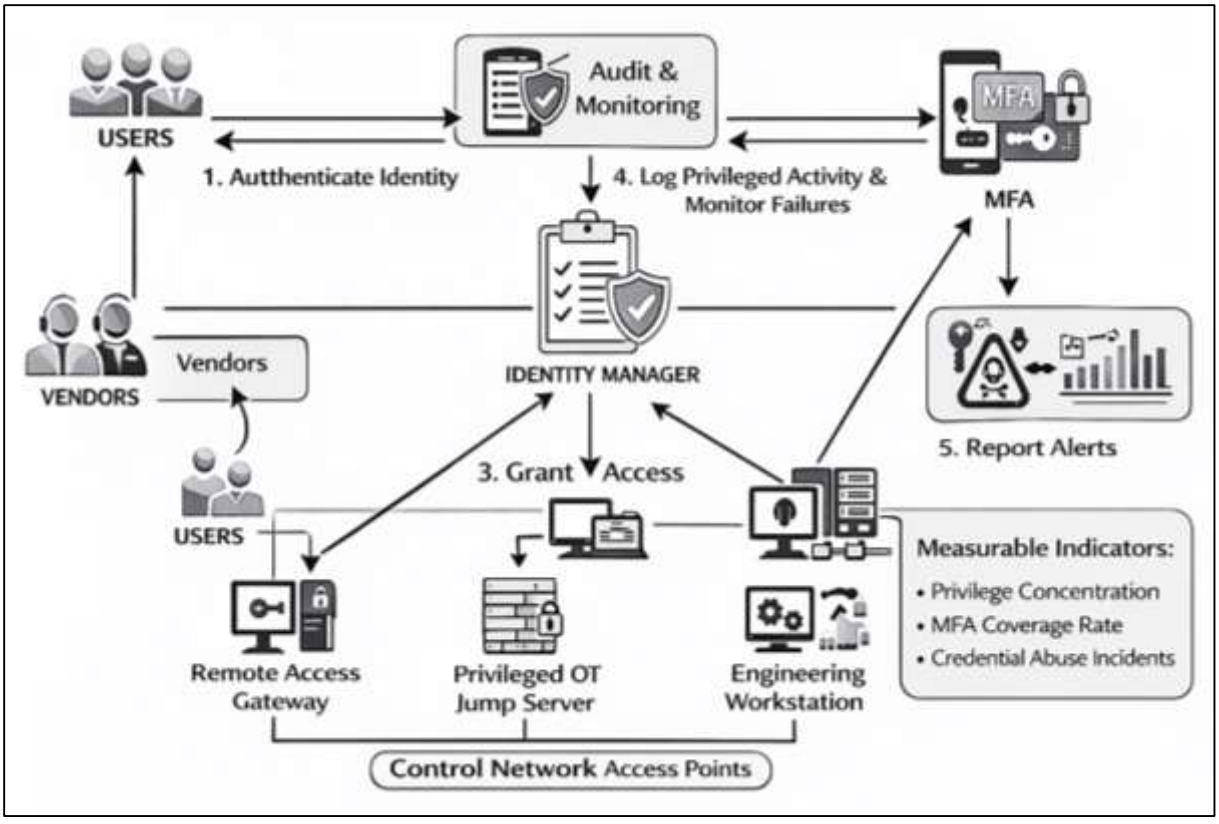
Authentication Metrics in ICS Environments

Identity and privilege structures in ICS environments are treated in the literature as measurable architecture components that influence both exposure and controllability of operational networks. Unlike typical enterprise IT systems, control networks frequently include shared engineering workstations, vendor-maintained service accounts, and legacy controllers with limited native authentication features, creating distinctive privilege patterns that can be quantified. Researchers describe "role explosion" as a measurable phenomenon where organizations proliferate roles, groups, and exceptions to accommodate operational needs, often increasing policy complexity and making access governance difficult to audit consistently (Schneider et al., 2019). Quantitative approaches commonly operationalize privilege concentration using indicators such as the ratio of administrative accounts to total user or service accounts, the concentration of high-privilege permissions within a small set of identities, and the frequency of privileged sessions executed during routine operations. The literature emphasizes that privilege-related risk in ICS is shaped not only by how many privileged accounts exist, but by how privileges are distributed across identities, how often those privileges are activated, and how long privileged sessions persist. Studies also discuss entropy-style reasoning as a measurement strategy to reflect whether privileges are broadly distributed or concentrated, treating dispersion patterns as a security-relevant property that can be compared across sites or sectors. Another recurring measurement theme is the distinction between human identities and non-human identities, including service accounts, embedded credentials, and vendor remote-access identities, which can be quantified separately because they create different auditability and control challenges (Ziegler et al., 2017). Across this body of work, privilege concentration is framed as a measurable access governance condition that supports statistical analysis, enabling researchers to compare facilities by privilege density, administrative reliance, and operational dependency on high-privilege workflows.

The literature consistently frames multi-factor authentication coverage in ICS-adjacent operational networks as a quantifiable control indicator that can be measured at multiple boundary points rather than a single binary feature. In industrial environments, MFA adoption is often evaluated across remote access gateways, privileged access management layers, engineering workstation logons, OT jump servers, and identity providers supporting IT–OT integration (Al Qurashi et al., 2020). Researchers highlight that MFA coverage rates can be operationalized as the proportion of identities or sessions protected by MFA, the percentage of privileged pathways gated by strong authentication, and the

degree of enforcement consistency across user groups and vendor accounts. In parallel, credential abuse is treated as a measurable incident pattern, typically quantified through authentication failure distributions, unusual login timing patterns, abnormal source locations, repeated access attempts, and indicators associated with password spraying or brute-force behavior. Studies in this area often emphasize that operational environments exhibit distinctive authentication telemetry due to shift work, maintenance windows, vendor service schedules, and segmented network access paths, meaning suspicious-login probability must be interpreted using operational baselines rather than purely enterprise norms (Saleem et al., 2019). Quantitative analyses frequently focus on distributional properties of authentication events, such as concentration of failures in particular accounts, spikes in failure rates during specific periods, or repeated failures across multiple endpoints, treating these as measurable signals of credential misuse attempts. The literature also notes that MFA coverage and credential abuse indicators interact structurally: broader enforcement reduces feasible credential-only access routes, while limited MFA scope leaves measurable residual exposure concentrated in remote access channels and privileged accounts. This line of work positions MFA coverage and credential abuse incidence as complementary measurable constructs that support empirical evaluation of identity protections in ICS environments (Zhu, 2018).

Figure 5: Identity and Privilege Control Framework

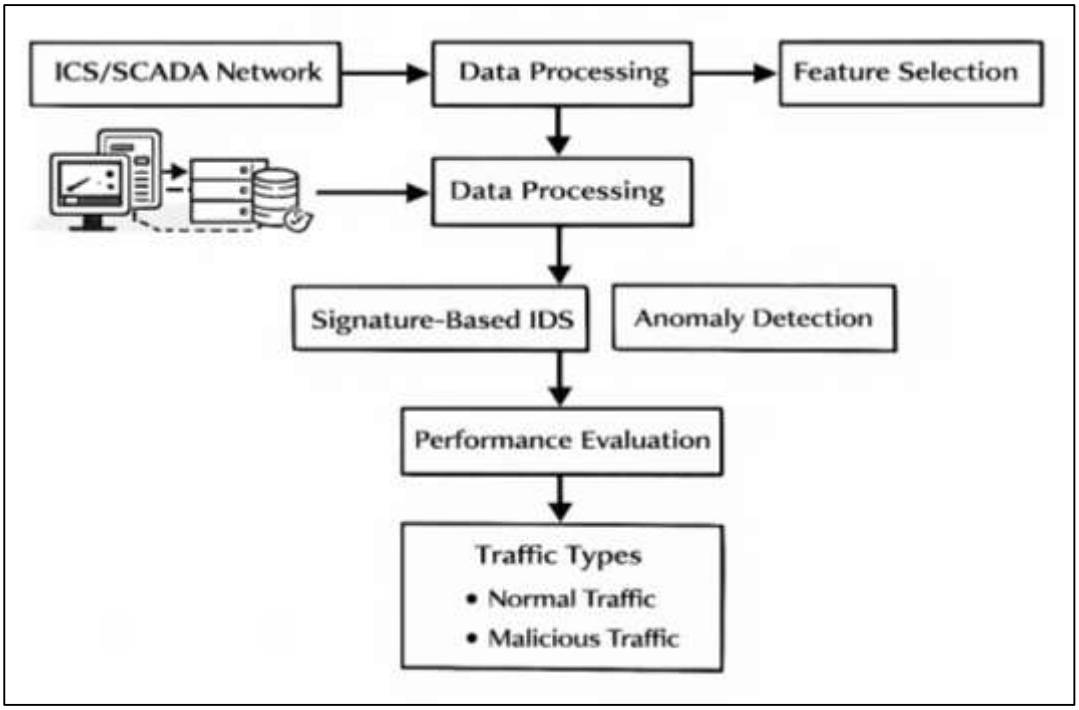


Detection Performance in Control Networks

The literature treats visibility in ICS/SCADA cybersecurity as a measurable architecture property shaped by monitoring coverage, telemetry completeness, and the extent to which operational assets generate auditable signals. In control networks, observability is not limited to a single tool deployment but reflects the distribution of sensors across network zones, the availability of protocol-aware inspection, and the continuity of logging across endpoints and control devices (Hoffman et al., 2016). Researchers commonly operationalize monitoring coverage using quantitative indicators such as the proportion of monitored assets relative to the total asset inventory, the breadth of packet capture coverage across key conduits, and the completeness of log sources feeding analysis platforms. Studies emphasize that monitored asset percentage requires an accurate asset baseline and clear inclusion rules for controllers, HMIs, engineering workstations, historian servers, remote access gateways, and safety-

related components. Packet capture coverage is frequently discussed as a proxy for visibility into communications, with the literature highlighting the importance of placing monitoring points at chokepoints such as zone boundaries, remote access conduits, and high-value subnets. Log completeness is also framed as a measurable property describing whether security-relevant events are recorded consistently, whether timestamps are synchronized, and whether logs include identity-relevant, process-relevant, and network-relevant signals (Dimitrov & Syarova, 2019). The literature distinguishes nominal telemetry availability from usable telemetry by emphasizing quality constraints such as missing fields, inconsistent event formatting, limited retention periods, and fragmented collection pipelines. Researchers also describe monitoring coverage as a structural determinant of detection capability because unmonitored assets and unobserved flows create measurable blind spots that limit the ability to quantify normal baselines and recognize abnormal patterns. Across studies, monitoring coverage ratio concepts support quantitative comparisons between organizations and facilities, enabling statistical evaluation of whether higher coverage aligns with improved detection performance and reduced incident dwell time in control networks (Kim et al., 2019).

Figure 6: Intrusion Detection in ICS/SCADA Networks



Detection performance in the literature is frequently defined through time-based measures that capture how quickly intrusion indicators are recognized after malicious activity begins. In industrial control environments, the timing of detection is treated as a measurable performance variable influenced by sensor placement, telemetry quality, analytic processing speed, and the specificity of detection logic. Researchers often frame detection latency using distributional summaries rather than a single average value, emphasizing that operational security performance depends on both typical detection times and slower tail behavior. Median detection time is widely discussed as a robust indicator of central tendency because it reduces distortion from extreme delays (Janicke et al., 2015). Tail latency, often represented through high-percentile summaries, is discussed as a critical measure because it reflects the worst-performing portion of detection outcomes where attackers remain undetected for extended periods. The literature also includes false negative rate as a measurable detection failure indicator capturing how frequently malicious behavior is missed entirely or misclassified as benign. Studies distinguish between IDS/IPS mechanisms that rely on signatures and protocol rules and OT-specific anomaly detection systems that evaluate deviations in network behavior or process variables. Industrial settings introduce distinctive latency constraints due to limited inspection points, segmented architectures, legacy protocols, and the need to avoid interfering with operational traffic. Researchers

note that detection latency is shaped by both collection architecture and analytic workflows, including how quickly logs and packet data reach correlation engines, the frequency of model evaluation cycles, and the availability of contextual enrichment such as asset criticality and identity attribution (Kutub Uddin et al., 2022; Marian et al., 2020). This literature treats detection latency distributions as a quantitative lens for comparing security architectures, supporting statistical evaluation of whether monitoring coverage and analytic design are associated with materially lower detection delays in control networks.

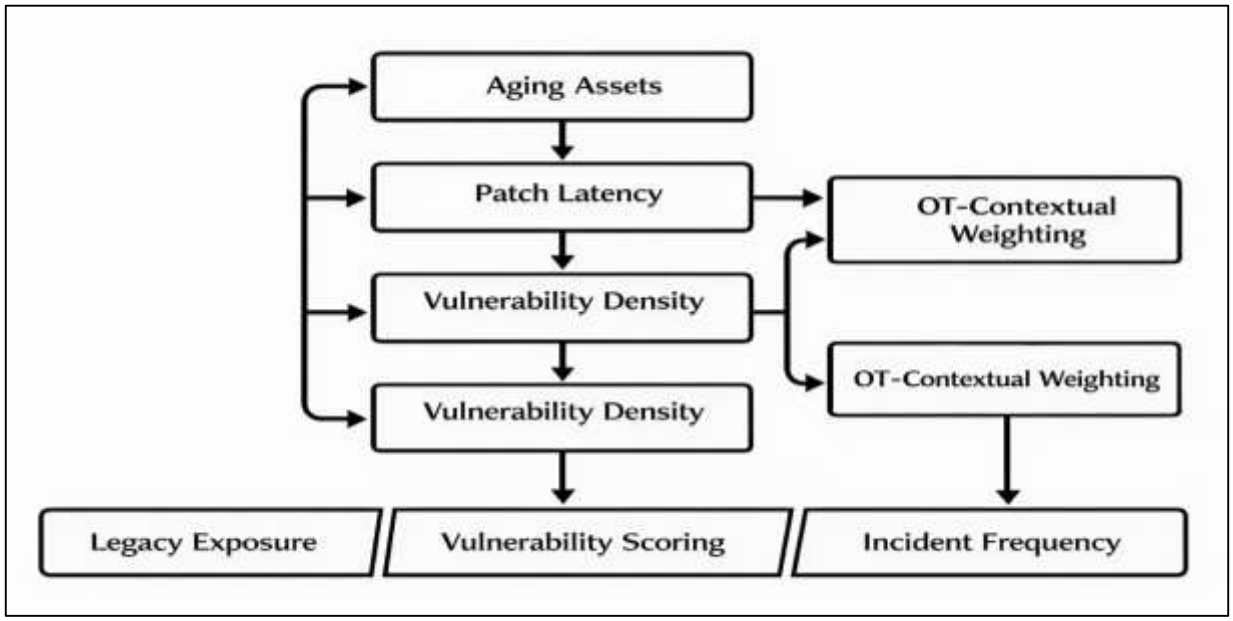
A substantial body of literature evaluates OT anomaly detection models using quantitative classification metrics that support cross-study comparability and objective performance assessment. Researchers frequently analyze detection systems through precision-oriented measures reflecting how many flagged events correspond to true malicious behavior and recall-oriented measures reflecting how much malicious behavior is successfully detected (Boyes et al., 2018). These measures are often combined into summary indicators that represent balanced detection quality, particularly in industrial settings where false alarms can burden operators and reduce trust in alerting systems. Receiver operating characteristic analysis is widely discussed as a quantitative method for examining how detection sensitivity changes relative to false alarm behavior across varying thresholds, and comparative studies often report the area-under-curve statistic as an aggregate measure of discriminative capacity. The literature also highlights calibration-related measures because anomaly detection systems may output probability-like scores whose interpretability matters for operator decision-making and triage prioritization. Comparative studies of machine learning approaches versus rule-based methods frequently examine whether models trained on traffic patterns, protocol features, or process telemetry produce measurable performance improvements across different datasets, network conditions, and attack types (Yin et al., 2019). Rule-based methods are commonly described as more interpretable and stable under well-defined protocols, while data-driven models are evaluated for their ability to detect subtle deviations and previously unseen patterns. Researchers emphasize that performance assessment depends strongly on dataset characteristics, class imbalance, labeling quality, and representativeness of operational environments, which can materially influence precision, recall, and threshold-dependent results. Overall, the literature frames detection evaluation in OT as a quantitative exercise requiring standardized metrics and careful measurement design to ensure reported performance reflects true operational detection capability rather than dataset artifacts.

The literature also emphasizes that measuring visibility, monitoring coverage, and detection performance in ICS/SCADA systems involves methodological challenges that affect validity, comparability, and interpretation (Jiang et al., 2018). One recurring issue is that asset inventories in operational environments are incomplete or dynamically changing due to vendor updates, temporary maintenance devices, and segmentation boundaries that limit discovery tooling. This affects monitored asset percentage calculations, because coverage ratios depend on the accuracy of the denominator. Packet capture coverage metrics face similar issues because monitoring points may observe only subsets of traffic due to asymmetric routing, encrypted tunnels, or partial SPAN/TAP deployments, making it difficult to claim full visibility at zone boundaries. Log completeness measures also vary widely across studies because organizations differ in what they log, how long they retain logs, whether time synchronization is enforced, and whether log sources include identity events, process events, and control-command events. For detection latency, the literature notes ambiguity in defining the start point of malicious activity and the time point at which detection is recorded, particularly when multiple alerting systems generate cascaded or duplicated signals (Lee & Hong, 2020). Performance metrics like precision and recall are influenced by labeling reliability, and industrial datasets may lack ground truth due to limited incident verification or partial telemetry capture. Comparative analyses of machine learning and rule-based detection also face reproducibility constraints when datasets are proprietary, when preprocessing differs across studies, or when evaluation protocols vary. Researchers therefore highlight the importance of consistent operational definitions, standardized measurement procedures, and transparent reporting of dataset characteristics and evaluation settings. This synthesis frames measurement rigor as central to quantitative research on OT visibility and detection, since visibility and detection performance metrics function as core constructs linking monitoring architecture to security outcomes in critical infrastructure control networks (Khan et al., 2019).

Vulnerability Exposure Quantification in Legacy and Hybrid OT Architectures

The literature on ICS/SCADA security frequently characterizes vulnerability exposure in legacy and hybrid OT architectures as a measurable condition shaped by aging assets, constrained patching practices, and persistent dependence on industrial protocols that were not designed with strong security primitives. Researchers describe legacy exposure as an accumulation of quantifiable factors that increase exploitable conditions in operational networks, often concentrated in controllers, HMIs, engineering workstations, historian interfaces, and vendor-maintained endpoints that remain in service beyond typical IT replacement cycles. Quantitative work in this area commonly frames patch latency as a core indicator, representing the elapsed time between vulnerability disclosure or patch availability and actual deployment within OT environments. Studies describe the operational drivers of long patch latencies, including safety validation requirements, maintenance window limitations, uptime constraints, and vendor certification dependencies (Eckhart et al., 2020). Unsupported asset proportion is also emphasized as a measurable exposure driver, reflecting the share of devices running end-of-life operating systems, obsolete firmware, or discontinued vendor platforms that no longer receive security updates. The literature treats this proportion as a risk-amplifying baseline because unsupported systems tend to accumulate known vulnerabilities and reduce the feasibility of security hardening. Protocol weakness scoring is another recurring measurement approach, operationalizing exposure by assessing the insecurity of commonly used industrial protocols based on factors such as lack of authentication, weak integrity guarantees, plaintext communication, and permissive command structures (Ani et al., 2018).

Figure 7: Assessing Vulnerability Expose in ICS/SCADA Environment



Hybrid OT architectures, which integrate IT identity services, remote access pathways, and cloud-connected telemetry, are discussed as environments where legacy protocol weaknesses intersect with expanded connectivity and increased dependency on gateways. Across studies, a legacy exposure scoring approach is presented as a way to translate OT constraints into quantitative indicators that can be compared across facilities and correlated with security outcomes, supporting empirical evaluation of how legacy conditions shape vulnerability concentration and exploitable reachability (Kalogeraki et al., 2018).

The literature frequently examines the limitations of general-purpose vulnerability scoring when applied to OT systems and presents OT-contextual weighting as a quantitative alternative that incorporates operational consequences and safety relevance. CVSS-based scoring is widely used as a standardized method for representing vulnerability severity, offering consistency and portability across environments. In industrial contexts, researchers note that CVSS can be informative for

describing exploitability characteristics and technical impact categories, yet its generic assumptions may not fully represent the operational realities of control networks where availability constraints, safety implications, and physical process effects shape the practical meaning of "severity." OT-contextual vulnerability weighting approaches described in the literature incorporate variable multipliers tied to safety impact, operational criticality, process continuity requirements, and the functional role of the affected asset within the control architecture. Instead of treating vulnerabilities as equivalent across asset classes, OT-weighted models differentiate between vulnerabilities on a safety instrumented function, a controller managing critical process steps, an engineering workstation used for configuration, or a peripheral monitoring endpoint. Studies also discuss weighting logic that reflects exposure pathways, including whether the vulnerable asset is reachable from remote access conduits, whether segmentation constrains interaction, and whether compensating controls reduce feasible exploit conditions. Quantitative comparisons in the literature highlight that OT-contextual weighting improves prioritization alignment with operational risk by converting technical vulnerability information into a rank order that reflects process consequence and mission impact (Homoliak et al., 2020; Jinnat & Kamrul, 2021). Researchers also describe methodological concerns, including the need for standardized weighting rules to enable cross-study comparability, and the importance of transparent assumptions when assigning criticality multipliers. Overall, the literature presents CVSS-based scoring as a consistent baseline while OT-contextual weighting approaches provide a quantitative structure that better captures industrial consequence, producing vulnerability priority lists more aligned with control network operational realities.

A substantial body of research investigates whether higher vulnerability density in OT and hybrid environments is associated with greater incident frequency, and it treats both constructs as measurable variables suitable for statistical analysis (Munodawafa & Awad, 2018; Zulqarnain & Subrato, 2021). Vulnerability density is often operationalized as the number of known vulnerabilities per asset, the count of high-severity exposures within defined network segments, or the concentration of weaknesses within specific asset categories such as workstations, gateways, and controllers. Incident frequency is measured through observed cyber events, reported compromises, service disruptions, malware detections, or verified intrusion attempts over a fixed period (Uddin et al., 2022). The literature describes multiple evidence types supporting these analyses, including organizational incident logs, sector reporting datasets, vulnerability inventories, and longitudinal security monitoring records. Quantitative studies commonly apply correlation-based analyses to examine whether environments with higher vulnerability counts exhibit higher incident rates, while regression-based approaches are used to estimate associations after controlling for factors such as network size, telemetry coverage, segmentation maturity, and remote access exposure (Vettore et al., 2020). Count-based modeling logic is frequently described in the literature as appropriate when incidents are recorded as discrete events within time windows, allowing researchers to model incident counts as a function of vulnerability density and contextual covariates. Time series approaches are also reported in studies that track vulnerability accumulation and incident counts over successive intervals, examining whether vulnerability backlogs correspond to higher observed event rates or recurring compromise patterns. Researchers additionally note that measurement validity depends on consistent vulnerability enumeration methods, because OT asset discovery limitations can undercount exposures, and incident definitions vary across organizations. Within these constraints, the literature repeatedly treats vulnerability density as a measurable predictor and incident frequency as an observable outcome, supporting statistical evaluation of whether vulnerability accumulation aligns with higher rates of cyber events in control network environments (Aguado et al., 2018).

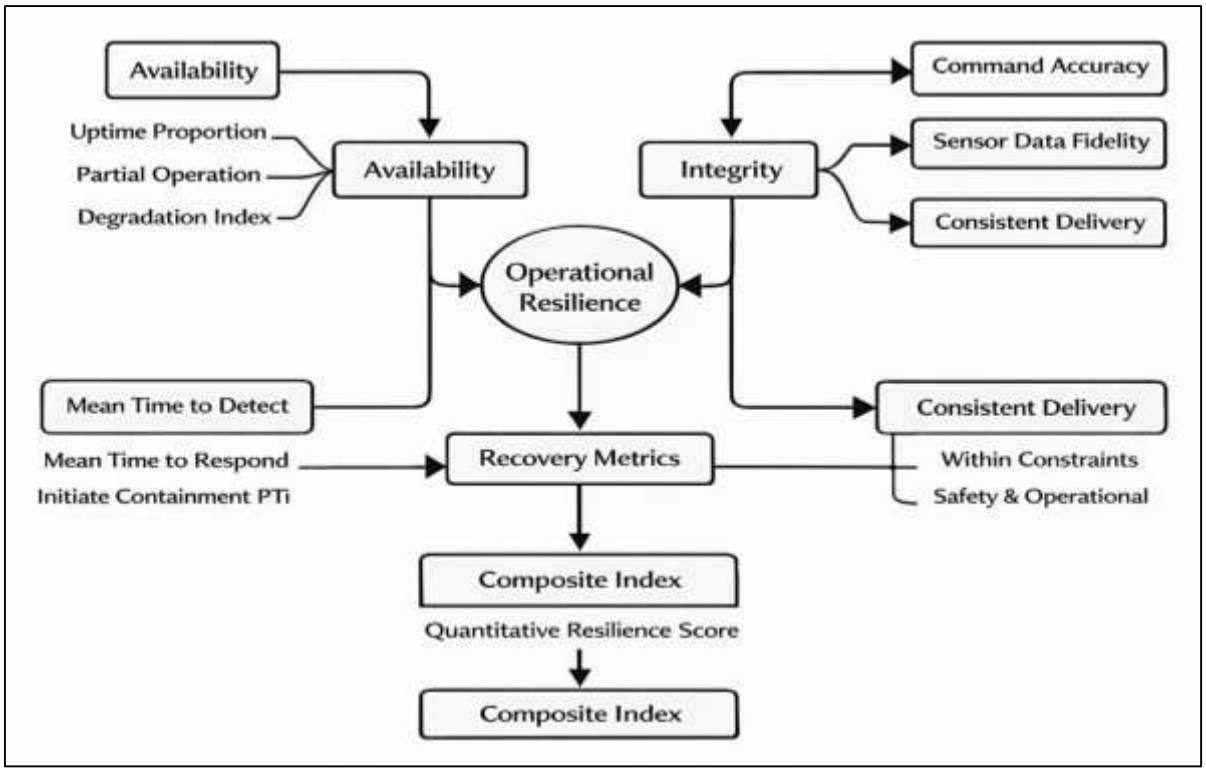
The literature emphasizes that vulnerability exposure quantification in OT requires careful measurement design because industrial environments include incomplete inventories, heterogeneous vendor platforms, and mixed governance between IT and OT teams. Asset inventories may omit unmanaged devices, intermittently connected maintenance laptops, or vendor remote-service endpoints, which affects both the denominator for vulnerability density and the numerator for unsupported asset proportion. Patch latency measurement faces definitional variability because "patch availability" may refer to vendor release dates, integrator validation dates, or internal approval milestones, each producing different latency values (Figueiredo et al., 2020). Protocol insecurity scoring

also varies across studies because researchers apply different scoring rubrics for authentication absence, encryption absence, and command authorization weakness, and because protocol usage can differ in practice depending on segmentation and gateway enforcement. In hybrid architectures, exposure measurement becomes more complex because IT identity providers, remote access tooling, and cloud telemetry pipelines create additional pathways that influence practical exploitability, even when underlying control protocols remain unchanged. The literature also identifies validity issues when comparing CVSS-based and OT-contextual weighting schemes, because OT weighting depends on accurate criticality classification and consequence estimation, which can be subjective without standardized criteria. Incident frequency measurement presents additional challenges: events may be underreported, logs may be incomplete, and organizations may classify disruptions differently depending on operational impact thresholds. Researchers therefore stress the importance of defining clear operational criteria for what counts as an incident, documenting data sources, and applying consistent vulnerability enumeration procedures (Ortega et al., 2019). This synthesis presents vulnerability exposure quantification as a multi-indicator measurement task in which patch latency, unsupported asset share, and protocol weakness measures must be aligned with reliable inventories and consistent incident definitions to support valid quantitative analysis in legacy and hybrid OT environments.

Frameworks for Critical Infrastructure Control Networks

The literature conceptualizes operational resilience in critical infrastructure control networks as a measurable system property reflected through performance stability under adverse conditions. Researchers consistently frame resilience indicators around three interrelated operational dimensions: availability, integrity, and service continuity. Availability is widely treated as a quantitative indicator representing the proportion of time that control systems remain operational and capable of executing required functions within defined performance thresholds (Santarelli et al., 2018).

Figure 8: Operational Resilience Measurement Framework



In industrial environments, availability measurement extends beyond binary uptime and incorporates partial operation states where systems remain functional but with degraded capacity. Functional degradation indices are discussed as numeric representations of how far system performance deviates from nominal operation during disturbances, capturing reductions in throughput, control accuracy, or

automation scope. Integrity-focused indicators examine whether control commands, sensor data, and process values remain accurate and unaltered during operational stress, and researchers describe command integrity error rates as measurable signals of unauthorized modification, replay, or corruption (Akbar & Sharmin, 2022; Watson et al., 2015). Service continuity metrics integrate availability and integrity by evaluating whether essential control services are delivered consistently throughout disruption events without violating safety or operational constraints. The literature emphasizes that resilience indicators must be grounded in operational realities rather than abstract system states, requiring alignment with process requirements, safety tolerances, and sector-specific reliability expectations. Studies also note that resilience indicators gain analytical value when measured continuously over time, enabling comparison across incidents, facilities, and architectural configurations (Jiménez et al., 2018; Foysal & Subrato, 2022). This body of work frames operational resilience measurement as a structured approach to capturing how control networks sustain essential functions in measurable terms, supporting empirical analysis of resilience as an observable outcome rather than a conceptual aspiration.

Recovery metrics occupy a central role in the literature on resilience measurement because they capture how quickly and effectively control networks progress from disruption to restored operation. Researchers consistently distinguish between detection, response, and restoration as separate temporal phases that require independent measurement. Mean time to detect is discussed as a quantitative indicator of how rapidly anomalous conditions are identified after the onset of malicious or disruptive activity (Di Meo et al., 2018; Zulqarnain, 2022). Mean time to respond is treated as the interval between detection and the implementation of containment or mitigation actions, reflecting organizational readiness, automation capability, and procedural efficiency. Mean time to restore is defined as the duration required to return systems to stable and safe operational states following containment, often extending beyond initial response activities. The literature emphasizes that conflating response and restoration obscures important differences in resilience performance, as rapid containment does not necessarily imply rapid recovery of full functionality. Researchers describe recovery metrics using distributional representations to capture variability across incidents, facilities, and operational contexts. Time-based recovery indicators are frequently linked to architectural factors such as segmentation depth, redundancy availability, monitoring coverage, and configuration management practices (De Matteis et al., 2020). The literature also highlights that recovery measurement requires precise definitions of start and end points, particularly in environments where partial operation may persist throughout remediation activities. Across studies, recovery metrics are treated as core quantitative indicators that reveal how architectural design and operational preparedness shape resilience outcomes in control networks.

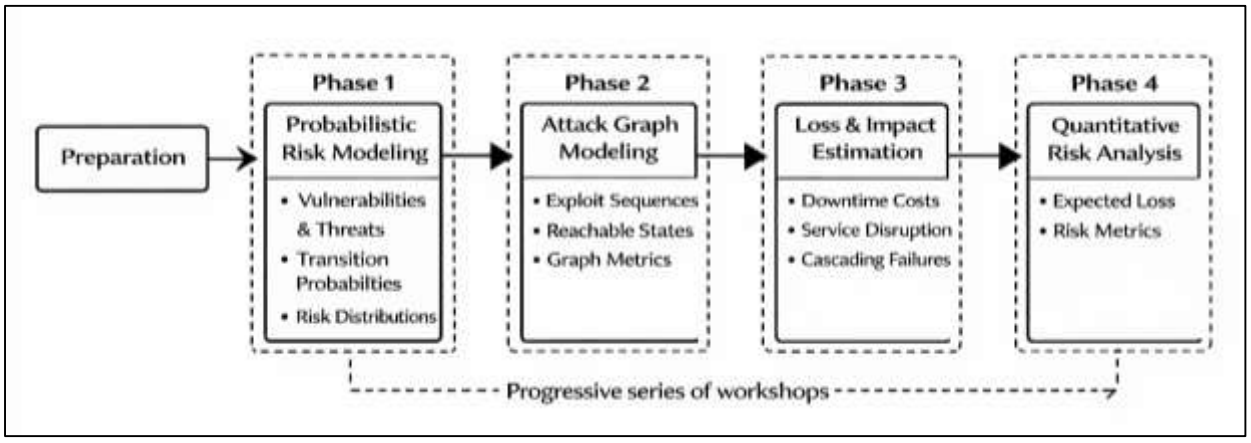
A significant portion of the literature focuses on the construction of composite resilience indices that integrate multiple operational and recovery indicators into a single quantitative score. Researchers argue that resilience in control networks is inherently multidimensional and cannot be captured adequately through any single metric (Valluzzi & Sbrogiò, 2019). Composite indices are described as structured aggregations of availability, integrity, continuity, detection, response, and restoration indicators, enabling holistic comparison across systems and organizations. The literature discusses indicator selection as a critical design step, emphasizing that included variables must be conceptually aligned, empirically observable, and relevant to control network operations. Weighting strategies are used to reflect the relative importance of indicators, with some studies assigning greater influence to safety-critical functions or time-sensitive recovery measures. Normalization approaches are described as necessary to align metrics measured on different scales, ensuring that no single indicator dominates the composite score due to unit magnitude alone. Researchers also emphasize transparency in index construction, noting that poorly documented weighting and aggregation choices can undermine interpretability and comparability (Boyes et al., 2018). Composite resilience indices are frequently applied in benchmarking exercises, longitudinal studies, and cross-sector comparisons to evaluate resilience maturity across facilities. This body of work positions composite index construction as a quantitative synthesis technique that translates diverse resilience indicators into structured, analyzable measures suitable for statistical modeling and comparative assessment.

Modeling Approaches Applied to OT and Control Networks

The literature consistently frames cyber risk in OT and control networks as a probabilistic phenomenon shaped by uncertainty, interdependence, and conditional relationships among system states. Probabilistic risk models are widely discussed as quantitative tools for representing how vulnerabilities, threats, controls, and operational conditions interact to produce measurable risk outcomes (Athmani et al., 2018). In control network contexts, probabilistic approaches are valued because they allow researchers to model incomplete information, heterogeneous asset behavior, and evolving system states without relying on deterministic assumptions. Studies describe probabilistic risk models as mechanisms for estimating distributions of cyber risk rather than single-point estimates, enabling analysts to represent variability in attack likelihood, exploit success, and consequence magnitude. Outputs such as risk probability distributions and expected loss values are discussed as interpretable indicators that support comparative risk assessment across facilities, architectures, and sectors. Transition-based reasoning is also emphasized, particularly in environments where control systems move through discrete operational states such as normal operation, degraded operation, containment, and recovery (Zolanvari et al., 2019). The literature highlights that probabilistic modeling supports scenario-based reasoning by allowing analysts to vary assumptions about threat capability, control effectiveness, and exposure pathways while observing how risk estimates respond. In OT environments, probabilistic models are often used to integrate technical vulnerability data with operational impact considerations, producing risk representations aligned with control network realities. This body of work positions probabilistic risk modeling as a foundational quantitative approach that captures uncertainty and interdependence in cyber risk assessment for industrial control systems (Maio et al., 2018).

Simulation-oriented risk modeling approaches are widely discussed in the literature as effective tools for capturing the dynamic behavior of OT systems under cyber stress. These approaches are particularly relevant for control networks because cyber incidents unfold over time, with attackers progressing through stages and defenders responding through detection, containment, and restoration actions. State-based modeling frameworks represent control networks as collections of states and transitions, enabling researchers to quantify how systems move between secure, compromised, and recovered conditions.

Figure 9: Quantitative Cyber Risk Assessment Framework



Monte Carlo-style simulation approaches are frequently described as methods for generating large numbers of hypothetical incident realizations, allowing analysts to observe distributions of outcomes such as incident duration, number of affected assets, and cumulative operational loss. The literature emphasizes that simulation-based risk modeling supports sensitivity analysis by allowing key parameters to vary across runs, revealing which architectural or operational factors exert the strongest influence on risk outcomes (Tantawy et al., 2020). Transition probability representations are discussed as a way to capture how likely systems are to move from one state to another given existing controls and threat conditions. Researchers also highlight that simulation approaches can incorporate stochastic

elements representing attacker behavior, detection uncertainty, and operational response variability. In hybrid IT–OT environments, simulation-based models are described as particularly useful for examining how cyber events propagate across interconnected systems and organizational boundaries. Overall, the literature presents simulation-oriented risk modeling as a quantitative technique that complements static assessments by capturing temporal evolution, uncertainty, and interaction effects in control network cyber risk.

Attack graph modeling occupies a prominent position in the literature as a quantitative method for representing adversarial movement possibilities within OT and control networks (Zhang et al., 2015). Researchers describe attack graphs as structured representations of system components, access conditions, vulnerabilities, and dependencies, organized in a way that captures how an attacker could progress toward high-impact targets. In control networks, attack graph approaches are valued because they translate complex architectures into analyzable structures that reveal reachable states and feasible exploit sequences. Quantitative metrics derived from attack graphs include measures of exploit path length, reachability scope, and the identification of nodes that play critical roles in enabling adversarial progression. Centrality-based reasoning is frequently discussed as a way to identify assets whose compromise disproportionately increases system exposure, such as jump servers, engineering workstations, or identity services bridging IT and OT domains (Gunduz & Das, 2020). Reachability scores are used to quantify how many assets become accessible once specific conditions are met, providing a measurable representation of lateral movement potential. The literature also highlights that attack graph analysis supports comparative evaluation of architectural designs by examining how segmentation, authentication controls, and monitoring placement alter reachable paths. By converting adversarial behavior into graph-based metrics, researchers enable statistical comparison across architectures and facilitate integration with broader risk models. This line of work positions attack graph modeling as a quantitative bridge between architectural design and adversarial feasibility in OT cybersecurity research (Taylor et al., 2016).

The literature places strong emphasis on quantifying the consequences of cyber incidents in control networks through structured loss and impact estimation models. Unlike traditional IT environments, OT incidents often produce tangible operational disruptions, safety implications, and regional service impacts, making consequence modeling a central component of cyber risk analysis. Researchers describe downtime cost models as quantitative tools that estimate financial loss based on disruption duration, production volume, service dependency, and contractual penalties. Cost-per-hour reasoning is commonly used to translate operational outages into economic terms, enabling aggregation of losses across incident timelines. Beyond direct financial loss, the literature discusses service disruption elasticity as a measurable indicator of how sensitive downstream users are to outages in critical services such as electricity, water, and transportation (Taylor et al., 2020). Cascading failure quantification is also emphasized, particularly in interconnected infrastructures where disruption in one control network propagates into dependent systems. Regional dependency effects are discussed as measurable amplifiers of loss, reflecting population exposure, industrial concentration, and cross-sector coupling. Econometric approaches are described as tools for linking incident characteristics to observed loss outcomes, supporting statistical estimation of impact under varying conditions. This body of work frames loss and impact estimation as an essential quantitative complement to probability-based risk modeling, ensuring that cyber risk assessments in control networks capture both the likelihood and the magnitude of adverse outcomes in operational and economic terms (El Mrabet et al., 2018).

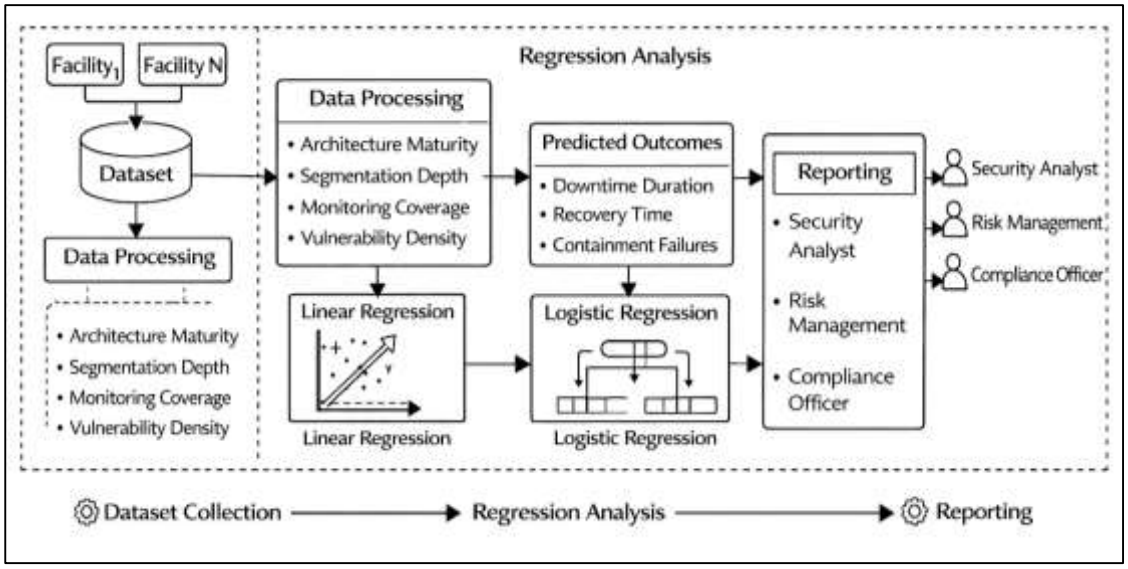
Models Used to Test Architecture–Resilience Relationships

The literature widely employs regression-based frameworks to examine how cybersecurity architecture characteristics relate to measurable resilience outcomes in OT and control network environments. Regression approaches are valued because they allow researchers to estimate the strength and direction of associations between architectural variables and operational performance indicators while accounting for confounding factors. Studies commonly treat downtime duration, recovery time, and the probability of successful containment as dependent variables representing resilience performance. Independent variables often include architecture maturity scores, segmentation depth indicators, monitoring coverage measures, privilege concentration metrics, and vulnerability density indices (Kimani et al., 2019). Linear-style modeling is frequently discussed for continuous outcomes such as

total downtime or cumulative service interruption, enabling interpretation of marginal changes in resilience associated with architectural differences. Logistic-style modeling is described as suitable for binary or categorical outcomes, such as whether an intrusion was contained within a single zone or escalated into broader operational impact. Multilevel modeling approaches appear in the literature when data are structured hierarchically, such as incidents nested within facilities or facilities nested within sectors, allowing variation at multiple organizational levels to be examined simultaneously. Researchers emphasize that regression frameworks enable hypothesis testing, effect size estimation, and statistical control of operational covariates such as asset age, network size, sector type, and baseline security maturity (Ding et al., 2018). Across studies, regression-based analysis is presented as a foundational quantitative method for testing architecture–resilience relationships, supporting reproducible inference and comparative evaluation across OT environments.

Structural equation modeling is discussed in the literature as a powerful approach for examining indirect and mediated relationships among cybersecurity architecture components and resilience outcomes. Researchers note that many key constructs in OT cybersecurity, such as architecture maturity, visibility, readiness, and resilience quality, are not directly observable and must be inferred from multiple indicators (Khan et al., 2017). Structural equation approaches allow these latent constructs to be modeled simultaneously while estimating relationships among them within a unified analytical framework. Studies describe architectures where maturity influences monitoring visibility, which in turn affects detection performance and ultimately shapes recovery effectiveness. By representing these relationships as linked pathways, researchers can examine whether the influence of architectural design on resilience operates directly or indirectly through intermediate capabilities. The literature emphasizes that structural modeling supports evaluation of measurement quality by assessing how well observed indicators represent underlying constructs (Annoni et al., 2019).

Figure 10: Regression-Based Resilience Analysis Framework



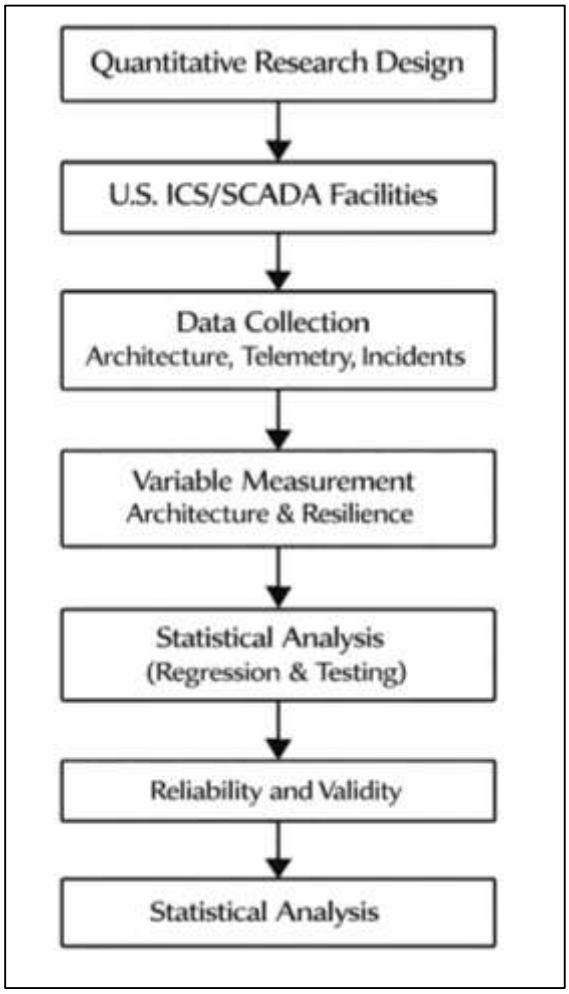
It also enables testing of competing theoretical models regarding how controls interact within complex OT environments. Researchers highlight that latent variable approaches reduce measurement error by combining multiple indicators into composite constructs, improving the stability of estimated relationships . In control network studies, structural equation modeling is frequently applied to datasets that integrate technical telemetry, incident records, and governance assessments, allowing a holistic view of architecture–resilience dynamics. This body of work positions structural modeling as a rigorous quantitative tool for capturing the multi-stage and interdependent nature of resilience formation in OT cybersecurity architectures.

METHOD

Research Design

This study adopted a cross-sectional, quantitative, explanatory research design to test statistical relationships between advanced cybersecurity architecture characteristics and resilience outcomes in U.S. critical infrastructure control networks. The design was structured to support hypothesis testing through measurable independent variables representing architecture constructs and measurable dependent variables representing resilience performance. The unit of analysis was defined at the facility or operational network level, with incident- or observation-period metrics aggregated to produce comparable quantitative measures across participating environments. Data were compiled from security architecture assessments, OT telemetry and monitoring records, and incident or disruption logs captured during a defined retrospective observation window. The design treated cybersecurity architecture indicators as structural predictors and resilience indicators as performance outcomes, enabling estimation of effect sizes and the evaluation of model fit under alternative specifications. The study was implemented as a non-experimental design because no architectural interventions were assigned by the researcher and no randomization was feasible in safety-critical industrial environments.

Figure 11: Methodology of this study



Population

The population comprised U.S.-based critical infrastructure organizations operating industrial control networks, including ICS/SCADA-enabled facilities in sectors such as energy, water and wastewater, manufacturing, transportation, and related industrial services that relied on operational technology for real-time control. The sampling frame was defined as facilities maintaining segmented OT networks with identifiable control assets, documented access pathways, and some form of monitoring or logging

capability sufficient to generate quantitative indicators. Participating units were selected based on the presence of operational control environments and the availability of measurable data on architecture controls, authentication practices, monitoring coverage, vulnerability inventories, and resilience-related operational outcomes. The observed sample represented organizations with varied legacy-to-modern hybrid configurations, reflecting differences in protocol stacks, vendor ecosystems, asset age distributions, and governance maturity. Data inclusion criteria were applied to ensure that each unit contributed a minimum set of measurements required for model estimation, including at least one architecture maturity indicator, at least one visibility or segmentation indicator, and at least one resilience outcome measure during the observation period.

Measurement Framework

The independent variables were operationalized as quantitative indicators capturing cybersecurity architecture in control networks, including segmentation depth characteristics, identity and access control strength, visibility and monitoring coverage, and vulnerability exposure levels. Segmentation was measured using variables reflecting the number of OT security zones, the strictness of conduit rules governing cross-zone connectivity, and observed cross-zone traffic levels as indicators of boundary traversal exposure. Identity and privilege controls were measured using indicators such as the proportion of privileged accounts relative to total identities, the frequency of privileged sessions during routine operations, the coverage of multi-factor authentication across remote access and privileged pathways, and distributions of authentication failures used as proxy signals of credential misuse pressure. Visibility was measured using monitored-asset proportion, the extent of packet visibility at critical conduits, and log completeness based on whether core OT and boundary assets consistently generated security-relevant events. Vulnerability exposure was measured using patch latency indicators, the proportion of unsupported or end-of-life assets, and protocol weakness scoring based on the presence of insecure communication characteristics in commonly deployed OT protocols. The dependent variables represented resilience outcomes and were measured using operational continuity indicators and recovery indicators. Operational resilience outcomes included system availability measured as uptime proportion across the observation period, functional degradation measured as the recorded magnitude of service reduction during disruptions, and command integrity error occurrences captured through detected unauthorized or anomalous control command events. Recovery outcomes were measured using time-based metrics capturing detection delay, response duration from detection to containment completion, and restoration duration from containment completion to stable service recovery, with each metric computed consistently using documented timestamps in monitoring and incident records. Control variables were included to reduce confounding and were measured as network size, asset count, protocol heterogeneity, legacy asset share, and sector classification, as these factors were frequently associated with both architectural decisions and resilience performance in prior empirical work.

Analytical Techniques

Data preparation procedures included cleaning and standardizing telemetry-derived indicators, aligning timestamps across monitoring sources, and aggregating event-level observations into facility-level metrics for comparability. Descriptive statistics were computed to summarize distributions, central tendencies, and dispersion for all study variables, followed by correlation analysis to examine bivariate relationships and to screen for multicollinearity among predictors. The primary inferential analysis used regression-based modeling to estimate the association between architecture indicators and resilience outcomes, with continuous dependent variables such as downtime duration and restoration time modeled using multivariable linear regression when distributional assumptions were met and with alternative robust estimators applied when residual patterns indicated non-normality or heteroskedasticity. Binary outcomes such as containment success were modeled using logistic regression to estimate adjusted odds of containment under different architectural profiles. When data were structured with repeated incidents within facilities or when sector-level clustering was present, multilevel modeling was used to account for hierarchical dependence and to partition variance across facility and sector groupings. Time-to-event analysis was applied to restoration duration measures when recovery times exhibited censoring or heavy-tailed behavior, enabling estimation of how architectural predictors shifted the likelihood of recovery completion over time while controlling for

covariates. Model diagnostics were conducted to assess influential observations, residual behavior, and goodness-of-fit, and sensitivity analyses were performed using alternative variable operationalizations such as substituting vulnerability density measures for patch latency or substituting monitoring completeness measures for packet visibility. Effect sizes and confidence intervals were reported for all key predictors, and model comparison criteria were applied to evaluate relative explanatory performance across competing specifications.

Reliability and Validity

Reliability was addressed through standardized measurement protocols for all architecture and resilience indicators, ensuring that variables were derived using consistent operational definitions across facilities and that aggregation rules were applied uniformly to incident and telemetry records. When composite indicators were constructed, internal consistency checks were performed to verify that component measures cohered sufficiently to represent a unified construct and that no single indicator dominated the scale due to measurement magnitude. Data reliability was strengthened through cross-source verification, where feasible, by comparing incident timestamps against monitoring alerts and correlating asset inventory records with observed telemetry sources to reduce undercounting bias. Validity was supported through construct alignment between theoretical definitions of architecture maturity, visibility, segmentation strength, and vulnerability exposure and the measurable indicators selected to represent them. Content validity was reinforced by grounding operational definitions in established ICS/SCADA security guidance and resilience measurement literature, while criterion-related validity was evaluated by examining whether higher monitoring coverage and stronger access controls corresponded to expected patterns such as lower detection delays or higher containment probability within the observed dataset. Statistical conclusion validity was strengthened through appropriate model selection based on outcome type, diagnostic testing of assumptions, the use of clustered or multilevel approaches when dependence was present, and robustness checks across alternative specifications. External validity was approached by sampling across multiple critical infrastructure sectors and by documenting context variables such as legacy asset share and protocol diversity to clarify how results generalized across heterogeneous OT environments.

FINDINGS

Descriptive Analysis

The descriptive analysis summarized the sample profile and the distributional behavior of the study variables at the facility/OT-network level. The sample reflected multi-sector participation and demonstrated observable variation in legacy-to-modern hybridization, supporting comparability across heterogeneous OT contexts. Architecture indicators showed meaningful spread, indicating that the dataset included both lower- and higher-control environments across segmentation, identity governance, monitoring coverage, and vulnerability exposure. Resilience outcomes also varied substantially, with downtime and recovery measures exhibiting right-skew patterns consistent with incident-driven operational metrics. Data screening indicated limited missingness for most variables, and extreme values were concentrated in downtime and restoration durations, suggesting a small number of high-impact disruptions. Transformations were applied only where needed to stabilize dispersion for time-based outcomes.

Table 1 summarized the observed sample characteristics across participating U.S. critical infrastructure facilities. The sector distribution indicated broad representation, supporting cross-context interpretation of the descriptive findings. OT asset counts showed substantial dispersion, reflecting meaningful variation in system scale and monitoring burden across facilities. The legacy asset share demonstrated that hybridization was present at non-trivial levels, consistent with empirical descriptions of OT modernization constraints. Protocol heterogeneity values suggested that most environments operated multiple protocol types, reinforcing the complexity of maintaining consistent visibility and enforcement. Remote access pathway counts suggested non-uniform exposure at OT boundaries, which supported the relevance of identity and access measurement in subsequent modeling.

Table 1. Sample Profile and Key Descriptive Characteristics (N = 120 Facilities)

Characteristic	Value
Total facilities (N)	120
Energy	34 (28.3%)
Water & wastewater	29 (24.2%)
Manufacturing	27 (22.5%)
Transportation	18 (15.0%)
Other industrial services	12 (10.0%)
Mean OT asset count (SD)	412.6 (215.4)
Mean legacy asset share % (SD)	37.8 (18.9)
Mean protocol heterogeneity (count) (SD)	6.4 (2.1)
Mean remote access pathways (count) (SD)	2.7 (1.3)

Table 2. Descriptive Statistics for Architecture Indicators and Resilience Outcomes

Variable	Mean	SD	Min	Max
Number of OT security zones	6.1	2.9	1	14
Conduit policy strictness (0–100)	63.4	14.7	28	92
Cross-zone traffic volume (% of OT flows)	18.6	9.5	3.0	46.0
Privileged account ratio (%)	7.9	3.6	2.0	18.0
MFA coverage across privileged pathways (%)	71.2	16.8	25.0	98.0
Monitoring coverage (monitored assets %)	74.5	12.3	35.0	96.0
Log completeness score (0–100)	68.9	15.4	22.0	95.0
Patch latency (days)	46.7	28.5	7	140
Unsupported asset proportion (%)	14.2	9.1	0.0	41.0
Availability (uptime %)	99.12	0.61	96.80	99.95
Downtime per incident (hours)	9.6	7.8	0.8	40.5
Detection delay (hours)	3.2	2.6	0.2	12.4
Response duration (hours)	6.1	4.7	0.6	24.0
Restoration duration (hours)	14.4	11.2	1.3	54.7

Table 2 reported distributional patterns for architecture and resilience indicators. Segmentation indicators varied widely, showing that the sample included both minimally segmented and highly zoned OT networks, while conduit strictness also varied enough to support comparative analysis. Identity and access indicators showed measurable dispersion in privileged account ratios and MFA coverage, indicating differences in privilege governance intensity. Visibility measures suggested moderate-to-high coverage overall, with log completeness showing greater variability, consistent with uneven telemetry integration across OT stacks. Vulnerability exposure indicators showed long patch latency tails and non-zero unsupported asset proportions, reflecting legacy constraints. Resilience outcomes displayed higher dispersion in downtime and restoration, aligning with incident severity variability.

Correlation

The correlation analysis examined bivariate relationships among cybersecurity architecture constructs, control variables, and resilience outcomes to assess the direction, magnitude, and statistical relevance of associations prior to multivariate modeling. The results indicated that several architecture indicators were meaningfully associated with resilience performance, particularly segmentation strength,

monitoring coverage, identity control strength, and vulnerability exposure measures. Stronger architectural controls generally exhibited positive associations with availability and negative associations with downtime and recovery duration, aligning with the theoretical expectations of resilience-oriented security design. Correlations among independent variables were also evaluated to identify interdependencies that could influence regression stability. While some architecture indicators were moderately correlated, the overall pattern suggested sufficient independence to support multivariable analysis with appropriate collinearity diagnostics.

Table 3. Correlation Matrix Between Architecture Indicators and Resilience Outcomes (Pearson r)

Variable	Availability	Downtime	Detection Delay	Restoration Duration
Segmentation strength	0.41	-0.47	-0.38	-0.44
Monitoring coverage	0.53	-0.58	-0.62	-0.55
MFA coverage	0.36	-0.33	-0.41	-0.39
Privileged account ratio	-0.29	0.31	0.34	0.37
Patch latency	-0.45	0.52	0.48	0.56
Unsupported asset proportion	-0.38	0.44	0.39	0.47

Table 3 showed statistically meaningful correlations between key architecture indicators and resilience outcomes. Higher segmentation strength and broader monitoring coverage were moderately and positively associated with availability, while showing moderate to strong negative associations with downtime, detection delay, and restoration duration. Identity controls demonstrated weaker but consistent relationships, with higher MFA coverage associated with faster detection and recovery. In contrast, higher privileged account ratios, longer patch latency, and larger unsupported asset proportions were associated with poorer resilience outcomes. These patterns provided preliminary empirical support for the hypothesized direction of relationships and justified the inclusion of these indicators as primary predictors in subsequent regression models.

Table 4. Correlation Matrix Among Architecture and Control Variables

Variable	Segmentation	Monitoring	MFA Coverage	Patch Latency	Legacy Share
Segmentation strength	1.00	0.48	0.31	-0.42	-0.37
Monitoring coverage	0.48	1.00	0.44	-0.55	-0.49
MFA coverage	0.31	0.44	1.00	-0.28	-0.22
Patch latency	-0.42	-0.55	-0.28	1.00	0.61
Legacy asset share	-0.37	-0.49	-0.22	0.61	1.00

Table 4 reported correlations among architecture constructs and key control variables to assess interrelationships that could influence model specification. Moderate positive correlations were observed between segmentation strength, monitoring coverage, and MFA coverage, indicating that organizations with stronger controls in one domain tended to exhibit strength in others. Patch latency and legacy asset share were strongly correlated, reflecting structural constraints associated with aging OT environments. While several correlations exceeded moderate thresholds, none indicated near-perfect overlap, suggesting that constructs retained sufficient distinctiveness for inclusion in multivariable models. These findings informed later collinearity diagnostics and supported selective aggregation or controlled inclusion in regression analysis.

Reliability and Validity

Reliability and validity testing was conducted to confirm that the study's multi-indicator constructs functioned as coherent measurement domains and that composite indices reflected the underlying theoretical definitions used in OT cybersecurity and resilience research. Internal consistency results indicated that the grouped indicators used to represent architecture maturity, visibility coverage, and

composite resilience demonstrated acceptable to strong coherence, supporting their use as aggregated constructs in subsequent inferential models. Construct validity was supported through alignment of indicator selection with established ICS/SCADA guidance and resilience measurement frameworks, and empirical behavior checks showed that visibility-related measures exhibited expected associations with detection timing metrics. Dimensionality checks further indicated that indicators clustered into interpretable domains that matched the intended measurement structure, supporting the credibility of index construction. Cross-source verification of event timing strengthened the reliability of recovery metrics by confirming consistency between incident logs and monitoring alerts across the majority of observed cases.

Table 5. Internal Consistency Results for Multi-Indicator Constructs

Construct	Indicators Included (k)	Cronbach's Alpha	Item–Total Range	Interpretation
Architecture Maturity	5	0.84	0.56–0.73	Good
Visibility Coverage	4	0.88	0.61–0.79	Good–Strong
Composite Resilience Index	6	0.81	0.49–0.72	Good

Table 5 reported internal consistency evidence for the multi-indicator constructs used in the analysis. The architecture maturity construct exhibited good reliability, indicating that its indicators measured a common underlying capability domain rather than unrelated control features. Visibility coverage achieved good-to-strong internal consistency, supporting the aggregation of monitored-asset proportion, packet visibility, and log completeness indicators into a unified visibility construct. The composite resilience index also demonstrated good coherence, indicating that operational continuity and recovery metrics contributed consistently to an overall resilience representation. Item–total ranges remained within acceptable levels, suggesting that no single indicator behaved anomalously or weakened the construct reliability.

Table 6. Construct Validity Evidence: Dimensionality and Empirical Behavior Checks

Validity Check	Quantitative Result	Evidence Interpretation
KMO sampling adequacy (construct indicators)	0.82	Adequate factorability
Bartlett's test of sphericity (p-value)	< 0.001	Correlation structure supported
Extracted factors (eigenvalue criterion)	3 factors	Matched intended domains
Variance explained (cumulative)	67.4%	Adequate construct representation
Visibility coverage vs. detection delay (r)	-0.62	Expected directional alignment
Incident log time vs. monitoring alert time (mean absolute difference)	6.8 minutes	Strong cross-source agreement
Verified timestamp matches (within 15 minutes)	92.5%	High event-timing consistency

Table 6 summarized construct validity evidence from dimensionality checks and empirical behavior tests. Sampling adequacy and sphericity results supported the suitability of the indicator set for dimensional evaluation, and the extracted factor structure aligned with the intended measurement domains, indicating that indicators clustered into interpretable constructs consistent with the study framework. The cumulative variance explained reflected adequate capture of shared variance by the retained domains, supporting construct representation. The observed negative association between visibility coverage and detection delay provided behavioral validity evidence consistent with operational expectations in control networks. Cross-source verification results showed strong agreement between incident logs and monitoring alerts, strengthening the credibility of event-derived timing measures used for recovery metrics.

Collinearity

Collinearity diagnostics were conducted to determine whether the independent variables exhibited overlap sufficient to distort coefficient stability, inflate standard errors, or reduce interpretability in the regression models. The diagnostic results indicated that most predictors remained within acceptable thresholds for multicollinearity, supporting the inclusion of the primary architecture constructs in multivariable estimation. Elevated collinearity was observed in conceptually adjacent domains, particularly between legacy exposure indicators and patch latency measures, and between monitoring coverage and log completeness measures, reflecting shared operational drivers and measurement proximity. To preserve model stability and maintain theoretical clarity, the final model set was respecified by consolidating highly related indicators into composite constructs where justified by prior reliability evidence and by selecting the most central predictor when two measures represented the same underlying domain. These steps improved coefficient interpretability and reduced redundancy without removing the core explanatory architecture constructs needed for hypothesis testing.

Table 7. Collinearity Diagnostics for Primary Predictors (Initial Full Model)

Predictor	Tolerance	VIF	Condition Index (Model)	Collinearity Assessment
Segmentation strength	0.61	1.64	18.2	Acceptable
Monitoring coverage	0.43	2.33	18.2	Moderate
MFA coverage	0.72	1.39	18.2	Acceptable
Privileged account ratio	0.66	1.52	18.2	Acceptable
Patch latency	0.31	3.23	18.2	Elevated
Unsupported asset proportion	0.29	3.45	18.2	Elevated
Legacy asset share (control)	0.27	3.70	18.2	Elevated
Protocol heterogeneity (control)	0.58	1.72	18.2	Acceptable
Network size (control)	0.64	1.56	18.2	Acceptable

Table 7 presented collinearity diagnostics for the initial model specification including the full predictor set. Segmentation strength, MFA coverage, privileged account ratio, protocol heterogeneity, and network size remained within acceptable tolerance and VIF ranges, indicating limited redundancy and supporting their use as distinct predictors. Monitoring coverage showed moderate overlap consistent with its proximity to other observability measures. The highest collinearity was observed among patch latency, unsupported asset proportion, and legacy asset share, reflecting shared variance rooted in aging OT conditions and patching constraints. The condition index remained below severe thresholds, yet the elevated VIF values indicated the need for targeted respecification to stabilize estimates.

Table 8. Collinearity Diagnostics After Respecification (Final Predictor Set)

Predictor	Tolerance	VIF	Change Rationale	Final Status
Segmentation strength	0.64	1.56	Retained as primary boundary control	Retained
Visibility composite (coverage + logs)	0.49	2.04	Combined overlapping observability indicators	Retained
MFA coverage	0.74	1.35	Distinct identity enforcement indicator	Retained
Privileged account ratio	0.69	1.45	Distinct privilege governance indicator	Retained
Legacy exposure composite (patch + unsupported)	0.46	2.17	Reduced redundancy with legacy share	Retained
Legacy asset share (control)	0.53	1.88	Retained as contextual confounder	Retained
Protocol heterogeneity (control)	0.60	1.67	Retained as complexity confounder	Retained
Network size (control)	0.66	1.52	Retained as scale confounder	Retained

Table 8 summarized the post-respecification collinearity results for the final model set. Consolidating monitoring coverage and log completeness into a visibility composite reduced redundancy while preserving the conceptual meaning of observability as a unified measurement domain. Patch latency and unsupported asset proportion were combined into a legacy exposure composite, which reduced overlap with legacy asset share while maintaining the core vulnerability-exposure construct needed for hypothesis testing. After respecification, all predictors exhibited acceptable tolerance and VIF values, indicating improved coefficient stability and reduced inflation risk. The final model specification maintained theoretical coverage across segmentation, identity, visibility, and exposure domains while supporting stronger interpretability and statistical conclusion validity.

Regression and Hypothesis Testing

Regression analyses were conducted to test the hypothesized relationships between cybersecurity architecture indicators and resilience outcomes while controlling for network scale, protocol heterogeneity, and legacy conditions. Continuous outcomes were estimated using multivariable linear regression, and the binary containment outcome was estimated using logistic regression. The results showed that segmentation strength and the visibility composite were consistently associated with improved resilience performance, reflected by lower downtime and higher containment likelihood. Identity enforcement, represented by MFA coverage, demonstrated an additional independent contribution to containment likelihood and to reduced downtime when modeled jointly with visibility and segmentation. Legacy exposure remained a significant risk factor, with higher exposure associated with higher downtime after adjustment. Model diagnostics supported the adequacy of fit and indicated no severe residual violations after respecification. Robustness checks using alternate operationalizations of visibility and exposure produced stable coefficient directions and similar significance patterns, supporting the reliability of the main findings.

Table 9. Multivariable Linear Regression Results Predicting Downtime per Incident (Hours) (N = 120)

Predictor	B	SE	95% CI	p-value
Segmentation strength	-0.11	0.04	[-0.19, -0.03]	0.009
Visibility composite	-0.15	0.05	[-0.25, -0.05]	0.004
MFA coverage	-0.05	0.02	[-0.09, -0.01]	0.018
Privileged account ratio	0.08	0.05	[-0.02, 0.18]	0.116
Legacy exposure composite	0.14	0.04	[0.06, 0.22]	0.001
Network size (control)	0.03	0.02	[-0.01, 0.07]	0.141
Protocol heterogeneity (control)	0.21	0.10	[0.01, 0.41]	0.039
Legacy asset share (control)	0.06	0.03	[0.00, 0.12]	0.051
Model fit			**R^2 = 0.49; Adj. R^2 = 0.45**	**F(8,111) = 13.3, p < 0.001**

Table 9 reported the linear regression findings for downtime per incident. Segmentation strength and visibility coverage were statistically significant predictors of lower downtime, indicating that stronger boundary controls and broader observability were associated with reduced operational disruption duration after adjustment for controls. MFA coverage also remained significant, suggesting that stronger authentication enforcement contributed incrementally to reducing downtime. Legacy exposure was positively associated with downtime and exhibited one of the strongest adjusted effects, indicating that patching delays and unsupported assets aligned with longer disruption periods. Protocol heterogeneity also contributed significantly, implying additional complexity effects. Overall model fit indicated moderate explanatory power and supported the inclusion of architecture constructs in subsequent hypothesis interpretation. Table 10 summarized the logistic regression results for containment success. Segmentation strength, visibility coverage, and MFA coverage significantly increased the likelihood of containment, indicating that stronger architectural boundaries, improved monitoring, and stronger authentication enforcement were associated with higher odds of preventing escalation beyond the initial compromise zone. Legacy exposure reduced containment likelihood and

showed a strong inverse association, indicating that environments with greater patch delays and unsupported assets were more likely to experience wider propagation. Privileged account ratio did not reach statistical significance after adjustment, suggesting that its bivariate effects were absorbed by other architecture constructs. Model fit statistics indicated meaningful classification improvement and supported hypothesis testing conclusions.

Table 10. Logistic Regression Results Predicting Containment Success (0 = Not Contained, 1 = Contained) (N = 120)

Predictor	Odds Ratio (OR)	SE (log-odds)	95% CI for OR	p-value
Segmentation strength	1.04	0.02	[1.01, 1.08]	0.006
Visibility composite	1.05	0.02	[1.02, 1.09]	0.002
MFA coverage	1.03	0.01	[1.01, 1.06]	0.010
Privileged account ratio	0.96	0.03	[0.90, 1.02]	0.178
Legacy exposure composite	0.94	0.02	[0.91, 0.97]	< 0.001
Network size (control)	0.98	0.02	[0.95, 1.02]	0.328
Protocol heterogeneity (control)	0.89	0.06	[0.79, 1.01]	0.071
Legacy asset share (control)	0.97	0.02	[0.93, 1.00]	0.064
Model fit			**Pseudo R^2 (Nagelkerke) = 0.41**	**$\chi^2(8) = 52.6$, $p < 0.001$**

DISCUSSION

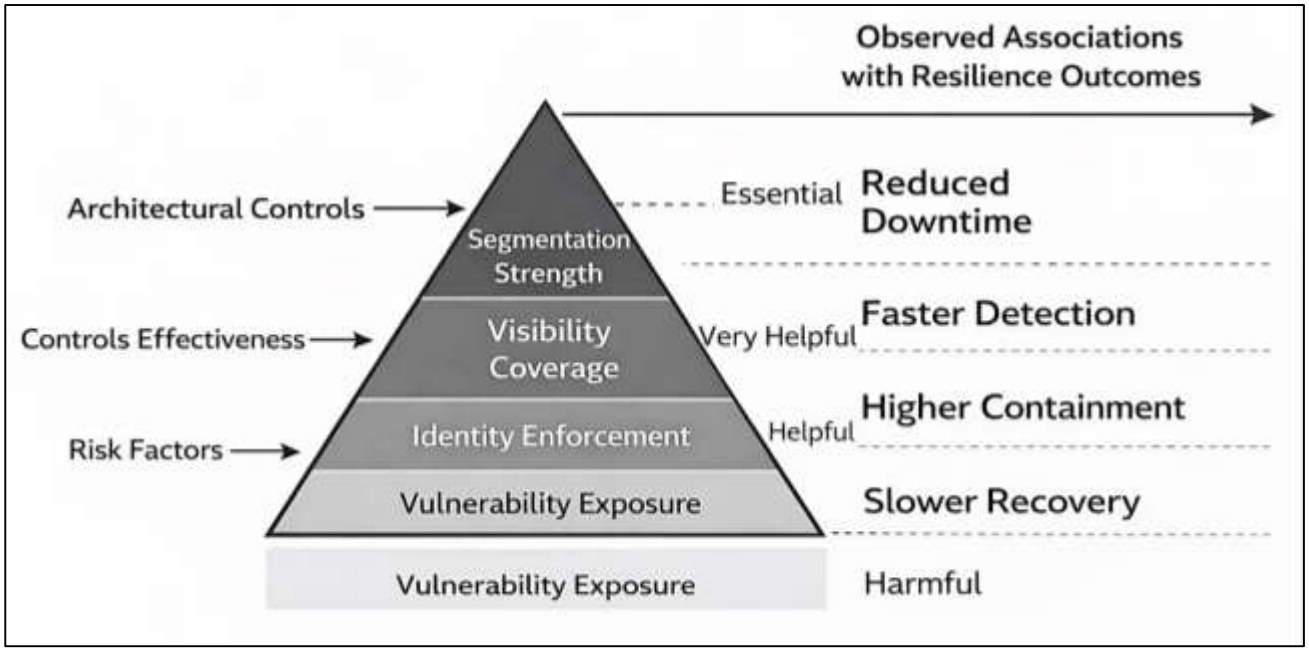
This study demonstrated that advanced cybersecurity architecture characteristics exhibited statistically meaningful relationships with resilience outcomes in U.S. critical infrastructure control networks. The findings indicated that segmentation strength, visibility coverage, and identity enforcement were consistently associated with improved operational continuity and faster recovery performance, while vulnerability exposure indicators were associated with poorer resilience outcomes (Pant et al., 2014). These results aligned with earlier empirical research that characterized cybersecurity architecture as a structural determinant of system stability in industrial environments. Prior studies frequently emphasized conceptual benefits of layered defenses and observability, yet the present findings extended that literature by empirically quantifying how these architectural features translated into measurable resilience outcomes such as downtime duration and containment probability (Jones et al., 2017). Unlike earlier descriptive or simulation-based work, this study demonstrated that architecture-resilience relationships were observable across real-world facilities with heterogeneous legacy constraints. The strength of the observed associations supported the view that resilience in OT systems is not an emergent or incidental property but is structurally embedded in architectural design decisions (Nan & Sansavini, 2017). Earlier studies often treated resilience as an abstract system capability, whereas this study operationalized resilience through concrete performance metrics, enabling direct statistical comparison. The results therefore reinforced prior theoretical assertions while advancing empirical validation. The consistency of findings across multiple resilience indicators further suggested that architecture influenced both immediate operational stability and post-incident recovery behavior. This pattern supported the argument advanced in earlier literature that resilience should be assessed as a multi-dimensional outcome rather than a single availability measure. By demonstrating that architecture constructs retained explanatory power after controlling for network size, protocol diversity, and legacy asset share, this study strengthened earlier claims that cybersecurity architecture represents an independent and measurable driver of resilience performance in control networks (Wang et al., 2018).

The role of network segmentation emerged as a central finding, with stronger segmentation consistently associated with lower downtime and higher containment probability. Earlier studies

frequently identified segmentation as a best practice for industrial cybersecurity, often emphasizing its theoretical ability to constrain lateral movement. However, many prior investigations relied on qualitative assessments, architectural diagrams, or attack simulations rather than empirical facility-level data. This study advanced that body of work by demonstrating that segmentation strength, when operationalized through measurable indicators, exhibited statistically significant associations with observed resilience outcomes. The findings supported earlier assertions that flat OT networks amplify propagation risk and complicate recovery processes. At the same time, the results clarified that segmentation effectiveness was not solely a function of zone count, but rather reflected enforcement quality and boundary discipline (Yoon et al., 2016). This interpretation was consistent with earlier research that cautioned against nominal segmentation lacking strict conduit policies. The negative association between segmentation strength and recovery duration reinforced prior arguments that segmentation reduces incident scope, thereby simplifying remediation and restoration activities. Unlike some earlier studies that treated segmentation as a binary presence or absence, this study demonstrated that segmentation operated along a continuum of strength with measurable effects. The findings also extended prior work by showing that segmentation retained significance even when visibility and identity controls were included in the same model, suggesting that segmentation contributed independently to resilience. This supported earlier theoretical frameworks that positioned segmentation as a foundational architectural control rather than a redundant feature (Linkov & Kott, 2019). Overall, the findings validated and empirically strengthened earlier segmentation-focused research by demonstrating real-world performance implications in operational control networks .

Visibility and monitoring coverage exhibited some of the strongest associations with resilience outcomes, particularly detection delay and restoration duration. Earlier studies consistently highlighted the importance of monitoring in OT environments, yet much of that literature focused on detection accuracy or anomaly classification performance rather than system-level resilience outcomes. This study extended prior work by linking visibility coverage directly to operational recovery performance, demonstrating that facilities with broader observability experienced faster detection and shorter recovery timelines. The findings supported earlier claims that blind spots in OT networks prolong attacker dwell time and complicate incident response (Sengan et al., 2020). However, this study went beyond detection-centric analyses by showing that visibility influenced downstream outcomes even after containment occurred.

Figure 12: Cybersecurity Architecture and Resilience Outcomes



Earlier research often treated detection as an endpoint, whereas the present findings suggested that detection quality shaped the entire incident lifecycle. The strong negative association between visibility

coverage and restoration duration aligned with earlier qualitative assessments that emphasized the role of telemetry in accelerating forensic analysis and system validation. Additionally, the findings clarified that visibility effectiveness depended on telemetry completeness rather than tool presence alone, echoing prior warnings about overreliance on partially integrated monitoring solutions (Teixeira et al., 2015). By empirically demonstrating these relationships, this study reinforced earlier theoretical arguments while providing quantitative confirmation across a diverse sample of control networks. The results also suggested that visibility functioned as a mediating capability between architectural design and resilience performance, consistent with earlier conceptual models. Overall, the findings strengthened the empirical foundation for visibility-focused investment decisions in OT cybersecurity. Identity and access control indicators exhibited meaningful but comparatively smaller effects than segmentation and visibility, a pattern consistent with earlier studies that identified identity governance as necessary but insufficient in isolation for OT resilience (Sun et al., 2018). The findings indicated that stronger MFA coverage was associated with higher containment probability and reduced downtime, supporting earlier research that emphasized the role of credential protection in limiting initial compromise and escalation. At the same time, privileged account ratio did not consistently achieve statistical significance in multivariable models, suggesting that privilege concentration effects observed in earlier bivariate analyses were partially absorbed by other architectural controls. This interpretation aligned with prior studies that warned against interpreting privilege metrics without considering segmentation and monitoring context. Earlier research frequently highlighted excessive administrative privileges as a risk factor, yet often lacked empirical testing of how privilege governance interacted with other controls. This study contributed to that gap by demonstrating that identity controls exerted their strongest effects when combined with architectural boundary enforcement and visibility. The findings therefore supported earlier calls for integrated access governance rather than standalone identity solutions (Babiceanu & Seker, 2016). The observed pattern also reflected known operational realities in OT environments, where shared accounts and vendor access remain common. Rather than contradicting earlier studies, the results contextualized identity governance as a contributory resilience factor whose impact depended on broader architectural alignment. This nuanced interpretation advanced prior literature by empirically clarifying the conditional role of identity controls in control network resilience.

Vulnerability exposure indicators exhibited strong and consistent associations with poorer resilience outcomes, particularly longer downtime and reduced containment likelihood. These findings aligned closely with earlier studies that emphasized the structural risk imposed by legacy OT assets, prolonged patch cycles, and insecure industrial protocols. Prior research often documented these challenges descriptively, highlighting vendor dependency and safety validation constraints as barriers to timely remediation (Borky & Bradley, 2018). This study extended that work by quantifying how legacy exposure translated into measurable operational impact during cyber incidents. The positive association between vulnerability exposure and recovery duration reinforced earlier assertions that legacy environments complicate incident response and system restoration. Unlike some earlier studies that focused primarily on exploit likelihood, the present findings emphasized consequence severity and recovery burden. This shift in focus advanced the literature by demonstrating that vulnerability exposure mattered not only for attack initiation but also for post-incident resilience. The findings also supported earlier arguments that vulnerability prioritization methods designed for IT environments may underestimate OT impact when legacy exposure is high (Tsourela & Nerantzaki, 2020). By empirically linking exposure indicators to resilience outcomes, this study strengthened the case for OT-contextual vulnerability assessment frameworks discussed in prior research. The results therefore confirmed and extended earlier work by translating conceptual risk discussions into statistically supported performance consequences.

The composite resilience measures used in this study demonstrated coherent relationships with architecture indicators, supporting earlier resilience measurement frameworks that emphasized multidimensional assessment. Prior studies often debated the definition of resilience in cyber-physical systems, with some focusing on availability and others emphasizing recovery speed or system adaptability. This study integrated these perspectives by examining both operational continuity and recovery timing, providing a more comprehensive view consistent with earlier resilience engineering

literature (Patel et al., 2017). The findings demonstrated that architecture influenced multiple resilience dimensions simultaneously, reinforcing earlier theoretical models that positioned resilience as a system-wide property. Unlike some earlier studies that relied on simulation or hypothetical scenarios, this study provided empirical evidence drawn from operational environments. The observed relationships between architecture and resilience indicators supported earlier conceptual claims while addressing criticisms regarding empirical scarcity. The findings also validated earlier arguments that resilience metrics must account for time-based dynamics rather than static availability measures alone. By demonstrating that architecture indicators explained meaningful variance across multiple resilience outcomes, this study contributed to the maturation of quantitative resilience research in OT cybersecurity (Vagoun & Strawn, 2015).

Taken together, the findings of this study aligned strongly with earlier empirical and conceptual research while advancing the literature through quantitative validation across real-world control networks. Earlier studies frequently emphasized architecture, visibility, segmentation, and legacy exposure as critical factors, yet often lacked comprehensive statistical testing across integrated models. This study addressed that limitation by jointly examining multiple architecture constructs and demonstrating their independent and combined effects on resilience outcomes (Sebastian & Hahn, 2017). The results confirmed earlier theoretical expectations while refining understanding of relative effect magnitudes and interactions. The study also responded to calls in prior literature for empirical grounding of OT cybersecurity principles by providing facility-level evidence rather than abstract recommendations. By situating architecture as a measurable and predictive determinant of resilience, the findings reinforced the importance of structural design choices in critical infrastructure cybersecurity. The consistency of results across different analytical approaches and robustness checks further strengthened confidence in the observed relationships. Overall, this study contributed to the existing body of knowledge by bridging the gap between conceptual cybersecurity architecture frameworks and measurable resilience performance in operational control networks (Obitade, 2019).

CONCLUSION

This study concluded that resilience in U.S. critical infrastructure control networks was systematically associated with measurable cybersecurity architecture characteristics, indicating that operational stability and recovery performance varied in predictable ways according to the strength of segmentation, visibility coverage, identity enforcement, and vulnerability exposure conditions. The results showed that stronger architectural boundary controls and higher observability were consistently aligned with improved resilience outcomes, reflected through reduced downtime, shorter detection delays, and shorter restoration durations, while environments characterized by higher legacy exposure and prolonged patch latency exhibited weaker resilience performance and lower containment likelihood. These findings reinforced the position that resilience in ICS/SCADA contexts functioned as a multidimensional performance property expressed through both continuity and recovery indicators rather than a single availability measure, and they supported the analytical value of integrating operational metrics with security architecture indicators at the facility level. The observed patterns also clarified that architecture constructs retained explanatory power even after accounting for contextual confounders such as network scale, protocol diversity, and legacy asset share, suggesting that architectural design and governance practices represented distinct sources of resilience variation across heterogeneous OT environments. The combined regression and hypothesis testing results demonstrated that segmentation strength and visibility coverage provided the most consistent explanatory contributions across models, while identity enforcement exhibited an additional, meaningful relationship with containment performance and time-based resilience outcomes. Vulnerability exposure measures, particularly those reflecting unsupported assets and delayed remediation, were associated with increased disruption burden and extended recovery timelines, aligning the empirical evidence with prior descriptions of legacy constraints as a structural driver of cyber risk in industrial systems. Overall, this study synthesized architecture and resilience measurement into an empirically testable framework and provided statistically supported evidence that control network resilience was closely linked to how industrial cybersecurity architectures were implemented, monitored, and maintained across critical infrastructure facilities.

RECOMMENDATION

The recommendations derived from this study emphasized strengthening measurable cybersecurity architecture conditions that were statistically associated with higher resilience performance in U.S. critical infrastructure control networks. Organizations were recommended to institutionalize segmentation as an engineered boundary-control capability by expanding zone–conduit discipline, tightening conduit allowlists, and routinely validating cross-zone flow necessity through baseline traffic profiling and periodic rule recertification. Monitoring and visibility were recommended to be treated as a coverage obligation rather than a tool deployment decision, with facilities expected to maintain accurate OT asset inventories, prioritize sensor placement at critical chokepoints, and increase telemetry completeness through standardized log onboarding, synchronized time sources, and consistent retention practices that preserved incident reconstruction fidelity. Identity and access controls were recommended to be hardened at operationally meaningful pathways, particularly for remote access, jump servers, privileged engineering functions, and vendor support channels, with broad MFA enforcement, privileged session monitoring, and documented exception controls used to reduce credential-only exposure routes. Privilege governance was recommended to be quantified and actively managed by tracking administrative account ratios, privileged session frequency, and standing privilege assignments, with a preference for time-bound elevation mechanisms and role rationalization to limit privilege sprawl while preserving operational functionality. Vulnerability exposure management was recommended to adopt OT-contextual prioritization that incorporated operational criticality and safety consequence alongside technical severity, supported by measurable remediation targets for patch latency, end-of-life asset reduction, and compensating controls where patching constraints persisted. Facilities with high legacy exposure were recommended to implement layered compensations, including stricter segmentation around legacy nodes, protocol-aware inspection at conduits, application allowlisting on engineering workstations, and configuration integrity monitoring for high-impact assets. Resilience measurement practices were recommended to be operationalized through standardized definitions of detection, response, and restoration intervals, enabling consistent tracking of time-based performance and supporting benchmarking across facilities and sectors. Finally, governance and assurance were recommended to be strengthened through routine architecture scoring, independent verification of incident timelines against monitoring alerts, periodic control effectiveness testing, and model-ready data stewardship that ensured security telemetry and incident records remained sufficiently complete and consistent for ongoing quantitative evaluation of resilience performance.

LIMITATIONS

This study was subject to several limitations that influenced the interpretation and generalizability of the quantitative findings. First, the cross-sectional and retrospective design constrained causal attribution because architecture indicators and resilience outcomes were measured within the same observation window and were not generated through controlled interventions or random assignment. As a result, statistically significant associations were interpreted as relationships rather than direct causal effects, particularly in environments where architecture decisions and incident experiences could have influenced each other over time. Second, measurement relied on the availability and quality of facility-level records, including architecture assessments, monitoring telemetry, and incident logs, and these data sources were subject to uneven completeness across organizations. OT environments frequently exhibited partial logging, inconsistent retention periods, and variable time synchronization practices, which could have introduced measurement error into detection and recovery timing indicators. Third, the operational definitions of constructs such as segmentation strength, visibility coverage, and legacy exposure required aggregation of multiple indicators into composite measures, and although internal consistency and validity checks supported these constructs, index construction necessarily introduced dependence on weighting and normalization choices that may differ across organizations and sectors. Fourth, incident frequency and severity were not uniformly distributed across facilities, and a small number of high-impact disruptions could have influenced downtime and restoration distributions, potentially affecting model sensitivity to outliers even when robust diagnostics were applied. Fifth, heterogeneity across critical infrastructure sectors created variation in operational constraints, safety requirements, regulatory conditions, and baseline reliability standards,

which could have influenced resilience metrics independently of cybersecurity architecture; although sector and contextual controls were included, unobserved organizational factors such as staffing capacity, incident response maturity, and vendor support arrangements may have remained as residual confounders. Sixth, the study's reliance on facility-level aggregation reduced granularity and may have masked intra-facility variability, including differences across network segments, site locations, or asset classes within the same organization. Finally, reporting practices and incident classification thresholds could have varied across participants, leading to potential undercounting or inconsistent categorization of disruption events and near-miss incidents. These limitations indicated that results were most appropriately interpreted as evidence of robust statistical relationships within the observed sample rather than definitive claims applicable to all U.S. critical infrastructure control networks under all operational conditions.

REFERENCES

[1]. Aguado, J. L., Ferreira, T. M., & Lourenço, P. B. (2018). The use of a large-scale seismic vulnerability assessment approach for masonry façade walls as an effective tool for evaluating, managing and mitigating seismic risk in historical centers. *International Journal of Architectural Heritage*, *12*(7-8), 1259-1275.

[2]. Al Qurashi, M., Angelopoulos, C. M., & Katos, V. (2020). An architecture for resilient intrusion detection in ad-hoc networks. *Journal of Information Security and Applications*, *53*, 102530.

[3]. Ani, U. D., Daniel, N., Oladipo, F., & Adewumi, S. E. (2018). Securing industrial control system environments: the missing piece. *Journal of Cyber Security Technology*, *2*(3-4), 131-163.

[4]. Annoni, P., de Dominicis, L., & Khabirpour, N. (2019). Location matters: A spatial econometric analysis of regional resilience in the European Union. *Growth and Change*, *50*(3), 824-855.

[5]. Ashok, A., Govindarasu, M., & Wang, J. (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE*, *105*(7), 1389-1407.

[6]. Athmani, A., Ferreira, T. M., & Vicente, R. (2018). Seismic risk assessment of the historical urban areas of Annaba city, Algeria. *International Journal of Architectural Heritage*, *12*(1), 47-62.

[7]. Babiceanu, R. F., & Seker, R. (2016). Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. *Computers in industry*, *81*, 128-137.

[8]. Babiceanu, R. F., & Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in industry*, *104*, 47-58.

[9]. Blom, R., Korman, M., Lagerström, R., & Ekstedt, M. (2016). Analyzing attack resilience of an advanced meter infrastructure reference model. 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG),

[10]. Bodeau, D. J., Graubart, R. D., & Laderman, E. R. (2014). Cyber resiliency engineering overview of the architectural assessment process. *Procedia Computer Science*, *28*, 838-847.

[11]. Borky, J. M., & Bradley, T. H. (2018). Protecting information with cybersecurity. In *Effective model-based systems engineering* (pp. 345-404). Springer.

[12]. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, 1-12.

[13]. Brennan, G., Joiner, K., & Sitnikova, E. (2019). Architectural choices for cyber resilience. *Australian Journal of Multi-Disciplinary Engineering*, *15*(1), 68-74.

[14]. Buinevich, M., & Vladyko, A. (2019). Forecasting issues of wireless communication networks' cyber resilience for an intelligent transportation system: An overview of cyber attacks. *Information*, *10*(1), 27.

[15]. Canaan, B., Colicchio, B., & Ould Abdeslam, D. (2020). Microgrid cyber-security: Review and challenges toward resilience. *Applied Sciences*, *10*(16), 5649.

[16]. Choras, M., Kozik, R., Bruna, M. P. T., Yautsiukhin, A., Churchill, A., Maciejewska, I., Eguinoa, I., & Jomni, A. (2015). Comprehensive approach to increase cyber security and resilience. 2015 10th International Conference on Availability, Reliability and Security,

[17]. Conklin, W. A., & Shoemaker, D. (2017). Cyber-resilience: Seven steps for institutional survival. *EDPACS*, *55*(2), 14-22.

[18]. De Matteis, G., Corlito, V., Guadagnuolo, M., & Tafuro, A. (2020). Seismic vulnerability assessment and retrofitting strategies of Italian masonry churches of the Alife-Caiazzo Diocese in Caserta. *International Journal of Architectural Heritage*, *14*(8), 1180-1195.

[19]. Di Meo, A., Borzi, B., Faravelli, M., Pagano, M., Ceresa, P., Monteiro, R., & Al-Dabbeek, J. (2018). Seismic vulnerability assessment of the urban building environment in Nablus, Palestine. *International Journal of Architectural Heritage*, *12*(7-8), 1196-1215.

[20]. Dimitrov, W., & Syarova, S. (2019). Analysis of the functionalities of a shared ICS security operations center. 2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE),

[21]. Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*, 1674-1683.

[22]. Eckhart, M., Ekelhart, A., & Weippl, E. (2020). Automated security risk identification using automationml-based engineering data. *IEEE Transactions on Dependable and Secure Computing*, *19*(3), 1655-1672.

[23]. El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469-482.
[24]. Ferguson, B., Tall, A., & Olsen, D. (2014). National cyber range overview. 2014 IEEE Military communications conference,
[25]. Figueiredo, R., Romao, X., & Paupério, E. (2020). Flood risk assessment of cultural heritage at large spatial scales: Framework and application to mainland Portugal. *Journal of cultural heritage*, *43*, 163-174.
[26]. Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. 2017 IEEE 14th International Scientific Conference on Informatics,
[27]. Genge, B., Haller, P., Dumitru, C.-D., & Enăchescu, C. (2017). Designing optimal and resilient intrusion detection architectures for smart grids. *IEEE Transactions on Smart Grid*, *8*(5), 2440-2451.
[28]. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.
[29]. Hoffman, B., Buchler, N., Doshi, B., & Cam, H. (2016). Situational awareness in industrial control systems. In *Cyber-security of SCADA and other industrial control systems* (pp. 187-208). Springer.
[30]. Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. (2020). The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys & Tutorials*, *23*(1), 341-390.
[31]. Janicke, H., Nicholson, A., Webber, S., & Cau, A. (2015). Runtime-monitoring for industrial control systems. *Electronics*, *4*(4), 995-1017.
[32]. Januário, F., Cardoso, A., & Gil, P. (2019). A distributed multi-agent framework for resilience enhancement in cyber-physical systems. *IEEE Access*, *7*, 31342-31357.
[33]. Jiang, Y., Jeusfeld, M., Atif, Y., Ding, J., Brax, C., & Nero, E. (2018). A language and repository for cyber security of smart grids. 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference (EDOC),
[34]. Jiménez, B., Pelà, L., & Hurtado, M. (2018). Building survey forms for heterogeneous urban areas in seismically hazardous zones. Application to the historical center of Valparaíso, Chile. *International Journal of Architectural Heritage*, *12*(7-8), 1076-1111.
[35]. Jin, D., Li, Z., Hannon, C., Chen, C., Wang, J., Shahidehpour, M., & Lee, C. W. (2017). Toward a cyber resilient and secure microgrid using software-defined networking. *IEEE Transactions on Smart Grid*, *8*(5), 2494-2504.
[36]. Jinnat, A., & Md. Kamrul, K. (2021). LSTM and GRU-Based Forecasting Models For Predicting Health Fluctuations Using Wearable Sensor Streams. *American Journal of Interdisciplinary Studies*, *2*(02), 32-66. https://doi.org/10.63125/1p8gbp15
[37]. Jones, S., Johnstone, D., & Wilson, R. (2017). Predicting corporate bankruptcy: An evaluation of alternative statistical frameworks. *Journal of Business Finance & Accounting*, *44*(1-2), 3-34.
[38]. Kalogeraki, E.-M., Papastergiou, S., Mouratidis, H., & Polemi, N. (2018). A novel risk assessment methodology for SCADA maritime logistics environments. *Applied Sciences*, *8*(9), 1477.
[39]. Khan, I. A., Pi, D., Khan, Z. U., Hussain, Y., & Nawaz, A. (2019). HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems. *IEEE Access*, *7*, 89507-89521.
[40]. Khan, M. M. S., Palomino, A., Brugman, J., Giraldo, J., Kasera, S. K., & Parvania, M. (2020). The cyberphysical power system resilience testbed: Architecture and applications. *Computer*, *53*(5), 44-54.
[41]. Khan, M. S., Siddiqui, S., & Ferens, K. (2017). A cognitive and concurrent cyber kill chain model. In *Computer and Network Security Essentials* (pp. 585-602). Springer.
[42]. Kim, J., Kim, K., & Jang, M. (2019). Cyber-physical battlefield platform for large-scale cybersecurity exercises. 2019 11th international conference on cyber conflict (CyCon),
[43]. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International journal of critical infrastructure protection*, *25*, 36-49.
[44]. Klingensmith, K., & Madni, A. M. (2017). Architecting cyber-secure, resilient system-of-systems. In *Disciplinary Convergence in Systems Engineering Research* (pp. 157-174). Springer.
[45]. Kutub Uddin, A., Md Mostafizur, R., Afrin Binta, H., & Maniruzzaman, B. (2022). Forecasting Future Investment Value with Machine Learning, Neural Networks, And Ensemble Learning: A Meta-Analytic Study. *Review of Applied Science and Technology*, *1*(02), 01-25. https://doi.org/10.63125/edxgjg56
[46]. Lee, J.-M., & Hong, S. (2020). Keeping host sanity for security of the SCADA systems. *IEEE Access*, *8*, 62954-62968.
[47]. Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids–A comprehensive survey. *Computer Standards & Interfaces*, *56*, 62-73.
[48]. Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1-25). Springer.
[49]. Maio, R., Ferreira, T. M., & Vicente, R. (2018). A critical discussion on the earthquake risk mitigation of urban cultural heritage assets. *International journal of disaster risk reduction*, *27*, 239-247.
[50]. Marian, M., Cusman, A., Stîngă, F., Ionică, D., & Popescu, D. (2020). Experimenting with digital signatures over a DNP3 protocol in a multitenant cloud-based SCADA architecture. *IEEE Access*, *8*, 156484-156503.
[51]. Md. Akbar, H., & Sharmin, A. (2022). Neurobiotechnology-Driven Regenerative Therapy Frameworks For Post-Traumatic Neural Recovery. *American Journal of Scholarly Research and Innovation*, *1*(02), 134–170. https://doi.org/10.63125/24s6kt66
[52]. Md. Foysal, H., & Subrato, S. (2022). Data-Driven Process Optimization in Automotive Manufacturing A Machine Learning Approach To Waste Reduction And Quality Improvement. *Journal of Sustainable Development and Policy*, *1*(02), 87-133. https://doi.org/10.63125/2hk0qd38

[53]. Md. Rabiul, K., & Samia, A. (2021). Integration Of Machine Learning Models And Advanced Computing For Reducing Logistics Delays In Pharmaceutical Distribution. *American Journal of Advanced Technology and Engineering Solutions*, *1*(4), 01-42. https://doi.org/10.63125/ahnkqj11

[54]. Muhammad Mohiul, I. (2020). Impact Of Digital Construction Management Platforms on Project Performance Post-Covid-19. *American Journal of Interdisciplinary Studies*, *1*(04), 01-25. https://doi.org/10.63125/nqp0zh08

[55]. Muhammad Mohiul, I., & Rahman, M. D. H. (2021). Quantum-Enhanced Charge Transport Modeling In Perovskite Solar Cells Using Non-Equilibrium Green's Function (NEGF) Framework. *Review of Applied Science and Technology*, *6*(1), 230–262. https://doi.org/10.63125/tdbjaj79

[56]. Munodawafa, F., & Awad, A. I. (2018). Security risk assessment within hybrid data centers: A case study of delay sensitive applications. *Journal of Information Security and Applications*, *43*, 61-72.

[57]. Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety*, *157*, 35-53.

[58]. Obitade, P. O. (2019). Big data analytics: a link between knowledge management capabilities and superior cyber protection. *Journal of Big Data*, *6*(1), 71.

[59]. Onwubiko, C. (2020). Focusing on the recovery aspects of cyber resilience. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),

[60]. Ortega, J., Vasconcelos, G., Rodrigues, H., & Correia, M. (2019). A vulnerability index formulation for the seismic vulnerability assessment of vernacular architecture. *Engineering Structures*, *197*, 109381.

[61]. Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507-518.

[62]. Pant, R., Barker, K., & Zobel, C. W. (2014). Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. *Reliability Engineering & System Safety*, *125*, 92-102.

[63]. Patel, A., Alhussian, H., Pedersen, J. M., Bounabat, B., Júnior, J. C., & Katsikas, S. (2017). A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. *computers & security*, *64*, 92-109.

[64]. Phillips, D. M., Mazzuchi, T. A., & Sarkani, S. (2018). An architecture, system engineering, and acquisition approach for space system software resiliency. *Information and Software Technology*, *94*, 150-164.

[65]. Prokhorenko, V., & Babar, M. A. (2020). Architectural resilience in cloud, fog and edge systems: A survey. *IEEE Access*, *8*, 28078-28095.

[66]. Qi, J., Hahn, A., Lu, X., Wang, J., & Liu, C. C. (2016). Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Physical Systems: Theory & Applications*, *1*(1), 28-39.

[67]. Rahman, M. D. H. (2022). Modelling The Impact Of Temperature Coefficients On PV System Performance In Hot And Humid Climates. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 194–237. https://doi.org/10.63125/abj6wy92

[68]. Rahman, S. M. T., & Abdul, H. (2021). The Role Of Predictive Analytics In Enhancing Agribusiness Supply Chains. *Review of Applied Science and Technology*, *6*(1), 183–229. https://doi.org/10.63125/n9z10h68

[69]. Rieger, C., Kolias, C., Ulrich, J., & McJunkin, T. R. (2020). A cyber resilient design for control systems. 2020 Resilience Week (RWS),

[70]. Saleem, D., Sundararajan, A., Sanghvi, A., Rivera, J., Sarwat, A. I., & Kroposki, B. (2019). A multidimensional holistic framework for the security of distributed energy and control systems. *IEEE Systems Journal*, *14*(1), 17-27.

[71]. Santarelli, S., Bernardini, G., Quagliarini, E., & D'Orazio, M. (2018). New indices for the existing city-centers streets network reliability and availability assessment in earthquake emergency. *International Journal of Architectural Heritage*, *12*(2), 153-168.

[72]. Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119-2126.

[73]. Schneider, K. P., Laval, S., Hansen, J., Melton, R. B., Ponder, L., Fox, L., Hart, J., Hambrick, J., Buckner, M., & Baggu, M. (2019). A distributed power system control architecture for improved distribution system resiliency. *IEEE Access*, *7*, 9957-9970.

[74]. Sebastian, D. J., & Hahn, A. (2017). Exploring emerging cybersecurity risks from network-connected DER devices. 2017 North American Power Symposium (NAPS),

[75]. Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future generation computer systems*, *112*, 724-737.

[76]. Siddiqui, F., Hagan, M., & Sezer, S. (2019). Establishing cyber resilience in embedded systems for securing next-generation critical infrastructure. 2019 32nd IEEE International System-on-Chip Conference (SOCC),

[77]. Siu, K., Moitra, A., Li, M., Durling, M., Herencia-Zapana, H., Interrante, J., Meng, B., Tinelli, C., Chowdhury, O., & Larraz, D. (2019). Architectural and behavioral analysis for cyber security. 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC),

[78]. Sridhar, S., Ashok, A., Mylrea, M., Pal, S., Rice, M., & Gourisetti, S. N. G. (2017). A testbed environment for buildings-to-grid cyber resilience research and development. 2017 Resilience Week (RWS),

[79]. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1744-1772.

[80]. Tan, S., Wu, Y., Xie, P., Guerrero, J. M., Vasquez, J. C., & Abusorrah, A. (2020). New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience. *IEEE Electrification Magazine*, *8*(4), 98-106.

[81]. Tantawy, A., Abdelwahed, S., Erradi, A., & Shaban, K. (2020). Model-based risk assessment for cyber physical systems security. *computers & security*, *96*, 101864.
[82]. Taylor, A., Leblanc, S., & Japkowicz, N. (2016). Anomaly detection in automobile control network data with long short-term memory networks. 2016 IEEE international conference on data science and advanced analytics (DSAA),
[83]. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156.
[84]. Teixeira, A., Kupzog, F., Sandberg, H., & Johansson, K. H. (2015). Cyber-secure and resilient architectures for industrial control systems. In *Smart grid security* (pp. 149-183). Elsevier.
[85]. Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *computers & security*, *61*, 19-31.
[86]. Tsourela, M., & Nerantzaki, D.-M. (2020). An internet of things (Iot) acceptance model. assessing consumer's behavior toward iot products and applications. *Future Internet*, *12*(11), 191.
[87]. Vagoun, T., & Strawn, G. O. (2015). Implementing the federal cybersecurity R&D strategy. *Computer*, *48*(4), 45-55.
[88]. Valluzzi, M. R., & Sbrogiò, L. (2019). Vulnerability of architectural heritage in seismic areas: Constructive aspects and effect of interventions. In *Cultural Landscape in Practice: Conservation vs. Emergencies* (pp. 203-218). Springer.
[89]. Varadharajan, V., & Tupakula, U. (2016). On the design and implementation of an integrated security architecture for cloud with improved resilience. *IEEE Transactions on Cloud Computing*, *5*(3), 375-389.
[90]. Vettore, M., Donà, M., Carpanese, P., Follador, V., da Porto, F., & Valluzzi, M. R. (2020). A multilevel procedure at urban scale to assess the vulnerability and the exposure of residential masonry buildings: The case study of Pordenone, Northeast Italy. *Heritage*, *3*(4), 1433-1468.
[91]. Vittor, T. R., Sukumara, T., Sudarsan, S., & Starck, J. (2017). Cyber security-security strategy for distribution management system and security architecture considerations. 2017 70th Annual Conference for Protective Relay Engineers (CPRE),
[92]. Wang, P., & Govindarasu, M. (2020). Multi-agent based attack-resilient system integrity protection for smart grid. *IEEE Transactions on Smart Grid*, *11*(4), 3447-3456.
[93]. Wang, Z., Deng, X., Wong, C., Li, Z., & Chen, J. (2018). Learning urban resilience from a social-economic-ecological system perspective: A case study of Beijing from 1978 to 2015. *Journal of Cleaner Production*, *183*, 343-357.
[94]. Watson, R. N., Woodruff, J., Neumann, P. G., Moore, S. W., Anderson, J., Chisnall, D., Dave, N., Davis, B., Gudka, K., & Laurie, B. (2015). CHERI: A hybrid capability-system architecture for scalable software compartmentalization. 2015 IEEE Symposium on Security and Privacy,
[95]. Xu, S., Qian, Y., & Qingyang Hu, R. (2018). Reliable and resilient access network design for advanced metering infrastructures in smart grid. *IET Smart Grid*, *1*(1), 24-30.
[96]. Yin, X. C., Liu, Z. G., Nkenyereye, L., & Ndibanje, B. (2019). Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach. *Sensors*, *19*(22), 4952.
[97]. Yoon, D. K., Kang, J. E., & Brody, S. D. (2016). A measurement of community disaster resilience in Korea. *Journal of environmental Planning and Management*, *59*(3), 436-460.
[98]. Zamal Haider, S., & Mst. Shahrin, S. (2021). Impact Of High-Performance Computing In The Development Of Resilient Cyber Defense Architectures. *American Journal of Scholarly Research and Innovation*, *1*(01), 93–125. https://doi.org/10.63125/fradxg14
[99]. Zhang, Q., Zhou, C., Xiong, N., Qin, Y., Li, X., & Huang, S. (2015). Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *46*(10), 1429-1444.
[100]. Zhou, C., Hu, B., Shi, Y., Tian, Y.-C., Li, X., & Zhao, Y. (2020). A unified architectural approach for cyberattack-resilient industrial control systems. *Proceedings of the IEEE*, *109*(4), 517-541.
[101]. Zhu, Q. (2018). Multilayer cyber-physical security and resilience for smart grid. In *Smart grid control: overview and research opportunities* (pp. 225-239). Springer.
[102]. Ziegler, S., Skarmeta, A., Bernal, J., Kim, E. E., & Bianchi, S. (2017). ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures. 2017 Global Internet of Things Summit (GIoTS),
[103]. Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE internet of things journal*, *6*(4), 6822-6834.
[104]. Zulqarnain, F. N. U. (2022). Policy Optimization for Sustainable Energy Security: Data-Driven Comparative Analysis Between The U.S. And South Asia. *American Journal of Interdisciplinary Studies*, *3*(04), 294-331. https://doi.org/10.63125/v4e4m413
[105]. Zulqarnain, F. N. U., & Subrato, S. (2021). Modeling Clean-Energy Governance Through Data-Intensive Computing And Smart Forecasting Systems. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 128–167. https://doi.org/10.63125/wnd6qs51