American Journal of Scholarly Research and Innovation

Volume: *4;* ***Issue:*** *1*
Pages: *775–812*
eISSN: 3067-2163

MPLS-TP and SONET Security Hardening for Utility SCADA Networks: Threat Modeling and Mitigation Strategies for Energy Fiber Infrastructure

Abu Naser Md Golam Mosharraf[1];

[1]. Department Master of Engineering in Electrical Engineering , Lamar University, Texas, USA
Email: anmmosharraf@gmail.com

Doi: 10.63125/7czfg639
Received: *23 September 2025;* ***Revised:*** *27 October 2025;* ***Accepted:*** *14 November 2025;* ***Published:*** *28 December 2025*

Abstract

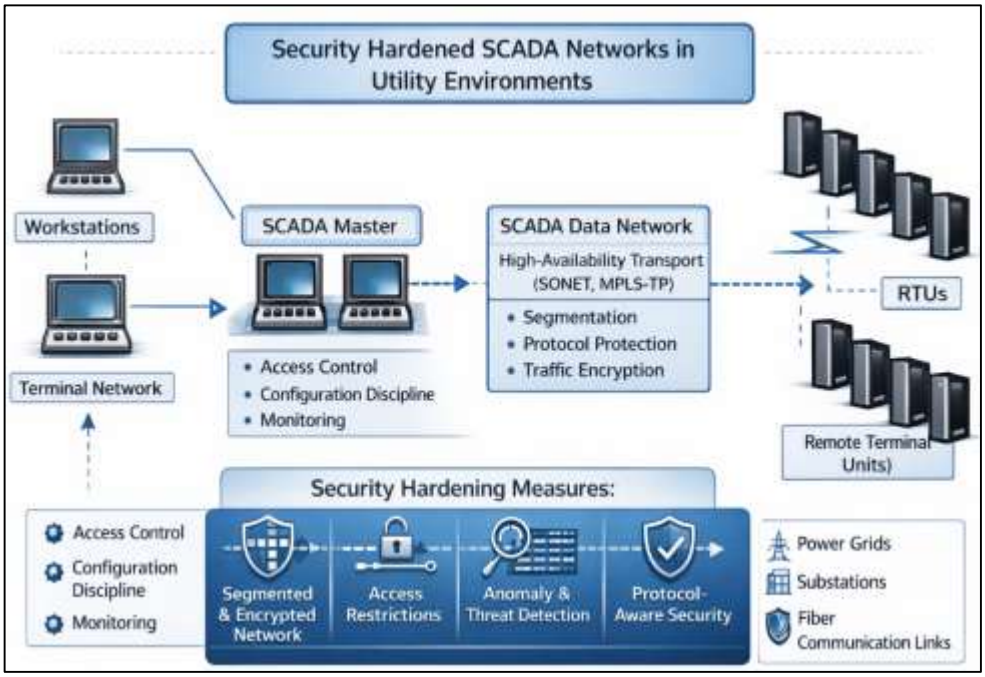
This study addresses the problem that utility SCADA communication backbones using MPLS-TP, SONET, and hybrid transport environments remain highly critical to grid operations, yet transport-layer security is often assessed less rigorously than broader SCADA cybersecurity despite exposure to unauthorized access, misconfiguration, weak IT/OT segmentation, denial-of-service, insider misuse, and physical fiber threats. The purpose of the study was to examine how threat modeling, security hardening controls, and mitigation strategies influence security performance and resilience in utility energy fiber infrastructures through a quantitative, cross-sectional, case-based design grounded in cloud and enterprise style utility communication cases. Data were collected through a structured five-point Likert questionnaire from professionals involved in SCADA operations, utility telecom, OT security, and infrastructure management. Of 150 distributed questionnaires, 132 were returned and 126 usable responses were analyzed, yielding an 84.0% usable response rate. The sample included respondents from MPLS-TP-only cases (22.2%), SONET-only cases (19.0%), and hybrid MPLS-TP/SONET cases (58.7%). Key variables were threat modeling practices, security hardening controls, mitigation strategies, and security and resilience outcomes. Analysis was conducted using descriptive statistics, Cronbach's alpha, Pearson correlation, and multiple regression. Reliability was strong across constructs, with alpha values ranging from 0.86 to 0.90. Descriptive findings showed high mean scores for threat modeling ($M = 4.08$, $SD = 0.62$), security hardening ($M = 4.21$, $SD = 0.57$), mitigation strategies ($M = 4.16$, $SD = 0.60$), and security outcomes ($M = 4.19$, $SD = 0.55$). Correlation results indicated significant positive relationships with security outcomes for threat modeling ($r = 0.61$), security hardening ($r = 0.74$), and mitigation strategies ($r = 0.68$), all at $p < .01$. Regression results showed that the model was significant, $F = 41.87$, $p < .001$, explaining 50.7% of the variance in security and resilience outcomes ($R^2 = 0.507$), with security hardening as the strongest predictor ($\beta = 0.41$), followed by mitigation strategies ($\beta = 0.29$) and threat modeling ($\beta = 0.24$). The study implies that utility operators should prioritize protocol-aware hardening, especially in hybrid environments, to strengthen resilience, continuity, and infrastructure protection.

KEYWORDS
MPLS-TP, SONET, Utility SCADA Security, Security Hardening, Energy Fiber Infrastructure;

INTRODUCTION

Supervisory control and data acquisition (SCADA) refers to the integrated set of hardware, software, communication links, control logic, and human–machine interfaces that enables geographically dispersed industrial assets to be monitored and controlled from centralized or distributed operating points (Akbarzadeh et al., 2023). In electric utilities, SCADA extends beyond a generic industrial control concept because it underpins telemetry, breaker status reporting, load dispatching, alarm processing, protection signaling, and coordinated operational decision making across substations, control centers, and field devices (Ashraf et al., 2021). Within the broader industrial control systems literature, SCADA is commonly treated as a foundational operational technology environment in which reliability, determinism, and availability are treated as core system properties alongside cybersecurity requirements. Security hardening in this context denotes the deliberate reduction of exploitable weaknesses through measures such as access control, configuration discipline, segmentation, monitoring, protocol protection, and physical safeguards (Bhamare et al., 2020).

Figure 1: Security Hardening in Utility SCADA Transport Networks



The international significance of SCADA security emerges from the central role of electric power in public health, water services, transportation, emergency response, industrial production, and digital economies. Utility communication failures can cascade across regions because power systems are interconnected both physically and operationally, and the communication substrate that supports dispatch and grid visibility has become as critical as generation and transmission assets themselves (Elbez et al., 2021). Research over the last two decades has shown that cyber exposure in utility control environments is not a localized technical inconvenience but a global infrastructure governance issue shaped by digitization, interconnection, and operational dependence on communications (Alanazi et al., 2023). International smart grid deployments, substation automation programs, and utility modernization initiatives have also intensified attention to transport-network resilience because communication compromise can alter timing, visibility, control responsiveness, and asset coordination across national power infrastructures. For that reason, the definitions of SCADA, industrial control systems, operational technology, and security hardening are best understood in relation to critical infrastructure continuity rather than in isolation from sectoral consequences. This framing is especially important for energy fiber infrastructures that carry operational traffic and protection messages, since communication integrity, latency, and survivability directly shape the secure functioning of modern utility operations (Hacks et al., 2020).

Multiprotocol Label Switching–Transport Profile (MPLS-TP) and Synchronous Optical Network (SONET) occupy an important place in utility communication architecture because both technologies have been used to provide high-availability transport for mission-critical operational traffic. SONET is a circuit-oriented optical transport standard designed around synchronization, fault isolation, and carrier-grade survivability, and utilities adopted it widely for deterministic transport, protection channels, and long-life operational networks (Ghosh & Sampalli, 2019).

Background of the Study

The background of this study is rooted in the growing dependence of modern electric utility systems on secure, resilient, and continuously available communication infrastructures for real-time monitoring and control. Utility Supervisory Control and Data Acquisition networks serve as the operational backbone of power generation, transmission, and distribution environments by enabling control centers to communicate with substations, protection devices, field sensors, and other mission-critical assets. As electricity networks have become more automated, geographically interconnected, and digitally managed, the communication layer supporting these operations has gained strategic importance equal to that of the physical grid itself. Within this context, Multiprotocol Label Switching–Transport Profile and Synchronous Optical Network technologies have played major roles in providing deterministic, high-availability transport for utility traffic, especially in environments where low latency, reliability, and service continuity are essential. SONET has historically been favored in many utility communication systems because of its stability, synchronization capabilities, and survivability features, while MPLS-TP has emerged as a transport-oriented packet solution that supports modernization without abandoning carrier-grade operational requirements. In many utility settings, these technologies now coexist in hybrid energy fiber infrastructures that connect legacy substations, digital substations, control centers, and remote operational sites. This mixed environment creates both opportunities and risks. On one hand, utilities benefit from scalable and robust communication pathways; on the other hand, the integration of legacy transport systems with newer network architectures introduces complex security challenges. These challenges include unauthorized access to transport nodes, protocol misconfiguration, insufficient segmentation, insider misuse, disruption of operational visibility, and physical threats to fiber infrastructure. Since utility SCADA networks directly support essential public services and national critical infrastructure, any weakness in the security of their communication backbone can lead to operational instability, delayed control actions, inaccurate system awareness, or broader service disruption. This study therefore emerges from the need to understand how security hardening, threat modeling, and mitigation strategies can strengthen MPLS-TP and SONET-based utility SCADA networks and improve the resilience of energy fiber infrastructure against increasingly complex cyber and operational threats.

Problem Statement

The problem addressed in this study arises from the increasing reliance of utility SCADA networks on communication infrastructures that must remain continuously available, operationally stable, and secure under complex cyber and physical conditions. Electric utilities depend on MPLS-TP and SONET-based transport environments to carry critical operational traffic between control centers, substations, field devices, and protection systems. These communication platforms are expected to support real-time visibility, command delivery, protection coordination, telemetry exchange, and maintenance access without interruption. At the same time, many utility communication infrastructures operate within mixed and transitional environments where legacy SONET systems coexist with newer MPLS-TP deployments. This hybrid condition creates a complicated security landscape because different transport technologies, management practices, and operational requirements intersect within the same infrastructure. As a result, utilities face persistent challenges in protecting transport-layer assets from unauthorized access, service disruption, misconfiguration, weak segmentation, insider misuse, and physical threats to fiber routes and supporting equipment. The core problem is that the communication backbone of utility SCADA systems has become highly critical to grid reliability, yet security hardening practices for MPLS-TP and SONET environments are often not examined with sufficient protocol-specific depth. Many organizations focus on SCADA cybersecurity broadly while giving less structured attention to the transport layer that supports operational trust, timing, resilience, and service continuity. This gap creates uncertainty regarding which threats are most

critical, which mitigation measures are most effective, and how hardening strategies influence security performance and operational resilience in utility energy fiber infrastructures. In addition, the coexistence of legacy and modern transport systems can produce uneven security controls, limited visibility into attack paths, and inconsistent implementation of risk reduction measures across operational domains. Without a clear understanding of these relationships, utilities may continue to invest in generalized security measures that do not adequately address transport-specific vulnerabilities in MPLS-TP and SONET-based SCADA environments. The problem, therefore, is not only the presence of cyber and operational threats, but also the lack of a focused empirical assessment of how threat modeling and mitigation strategies can strengthen the security and resilience of utility communication infrastructures built on these transport technologies.

Objective of the Study

The objective of this study is to provide a focused and measurable examination of security hardening within utility SCADA networks that rely on MPLS-TP and SONET transport infrastructures. The study seeks to identify the major threats that affect the communication backbone of energy fiber environments and to evaluate how utilities can reduce these threats through structured hardening and mitigation practices. More specifically, the study is designed to assess the extent to which threat modeling practices improve awareness of transport-layer vulnerabilities, clarify critical attack paths, and support better protection of utility communication assets. It also aims to determine how security hardening controls such as access restriction, segmentation, monitoring, secure configuration, resilience planning, and infrastructure protection contribute to stronger security performance in utility SCADA environments. Another important objective is to examine the relationship between mitigation strategies and operational resilience, especially in settings where legacy SONET systems and MPLS-TP-based transport solutions coexist within the same communication architecture. Through a quantitative, cross-sectional, case-study-based approach, the study intends to generate empirical evidence on how these factors interact and how they influence perceived risk reduction, service continuity, and infrastructure protection effectiveness. The study further aims to compare hardening effectiveness across MPLS-TP, SONET, and hybrid utility transport contexts in order to highlight differences in exposure, control priorities, and resilience needs. By doing so, it seeks to move beyond generalized discussions of SCADA cybersecurity and instead produce a protocol-aware understanding of transport security in energy communication systems. The broader objective is to support a more evidence-based foundation for protecting utility SCADA backbones by linking threat identification, hardening measures, and measurable security outcomes within a single analytical framework. In this way, the study is intended to contribute a structured basis for evaluating transport-layer cybersecurity in electric utility networks and to offer a clearer understanding of how communication resilience can be strengthened in mission-critical energy infrastructures.

Research Hypotheses

The research hypotheses of this study are developed to test the expected relationships among threat modeling, security hardening, mitigation strategies, and the protection outcomes of utility SCADA communication environments. Since the study focuses on MPLS-TP and SONET-based transport infrastructures, the hypotheses are designed to examine whether these core explanatory factors significantly influence security performance, operational resilience, and risk reduction in energy fiber systems. The first hypothesis proposes that threat modeling has a significant positive effect on the security performance of utility SCADA networks because structured identification of assets, attack paths, vulnerabilities, and operational exposures should improve the ability of organizations to recognize and manage transport-specific risks. The second hypothesis proposes that security hardening controls have a significant positive effect on operational resilience, based on the expectation that stronger access controls, segmentation, configuration management, monitoring, and protective safeguards improve continuity and reduce the likelihood of disruption. The third hypothesis proposes that mitigation strategies have a significant positive effect on perceived risk reduction in utility transport environments because well-defined response and protection measures are expected to reduce exploitable weaknesses and strengthen infrastructure defense. The fourth hypothesis proposes that protocol-specific hardening measures are positively associated with infrastructure protection effectiveness, which means that the more utilities tailor their security controls to the operational and

technical characteristics of MPLS-TP and SONET, the stronger the overall protection of their communication backbone is likely to be. The fifth hypothesis proposes that threat modeling, security hardening, and mitigation strategies jointly and significantly predict broader security and resilience outcomes in utility SCADA networks. These hypotheses form the analytical foundation of the study by converting its central assumptions into testable statistical relationships. They also align the study's variables with its research questions and make it possible to examine both individual and combined effects of key security practices. In this way, the hypotheses provide a clear structure for quantitative analysis and ensure that the study can empirically assess whether protocol-aware hardening strategies are meaningfully linked to stronger protection of utility energy fiber infrastructures.

Significance of the Research

The significance of this research lies in its contribution to the understanding of transport-layer cybersecurity in utility SCADA environments, particularly where MPLS-TP and SONET are used to support energy fiber infrastructure. The study is important because it addresses a highly specialized yet operationally critical area that directly affects the reliability, resilience, and security of electric utility communications. Its significance can be understood from several perspectives:

i. Significance to utility operators. This study provides utility organizations with a clearer understanding of how security hardening measures can be applied to transport infrastructures that carry mission-critical SCADA traffic. It helps operators recognize the importance of protecting communication backbones as part of overall grid reliability and operational continuity.

ii. Significance to SCADA and network engineers. The research offers a protocol-aware perspective on security by focusing specifically on MPLS-TP and SONET rather than discussing SCADA security only in broad terms. This helps engineers align technical controls with the actual communication environments used in substations, control centers, and utility transport networks.

iii. Significance to cybersecurity professionals in critical infrastructure. The study contributes to better threat visibility by linking threat modeling with measurable security outcomes. This allows cybersecurity teams to understand how structured identification of risks can improve defense planning and mitigation in utility telecom environments.

iv. Significance to academic literature. The study adds to existing knowledge by addressing an area that has received less focused empirical attention, namely the security hardening of utility transport-layer technologies within SCADA systems. It expands the literature by connecting transport security, cyber resilience, and quantitative assessment in one study.

v. Significance to policymakers and infrastructure planners. The findings can support more informed planning and policy development for utility communication protection. By emphasizing the strategic role of energy fiber infrastructure, the study highlights why communication security should be treated as a central part of critical infrastructure governance.

vi. Significance to methodology and applied research. Through its quantitative, cross-sectional, case-study-based design, the study creates an empirical basis for examining how threat modeling, mitigation strategies, and hardening controls interact. This makes the research useful not only for the present topic but also for related studies in industrial control security and energy network resilience.

LITERATURE REVIEW

The literature on utility SCADA security shows that communication infrastructures have become central to the safe and reliable operation of modern electric power systems. As utility environments have moved from isolated and largely proprietary architectures toward more interconnected, automated, and digitally managed systems, the communication layer has gained strategic importance as both an operational enabler and a security exposure point. SCADA networks no longer function only as channels for remote supervision; they now support a broad range of real-time activities including monitoring, switching coordination, telemetry exchange, relay communications, alarm handling, and operator decision support across geographically distributed infrastructures. Within this changing environment, transport technologies such as MPLS-TP and SONET have remained highly relevant because utilities require deterministic performance, survivability, low latency, and strong service continuity for mission-critical traffic. The literature further indicates that the coexistence of legacy and modern transport systems creates a complex operational setting in which security cannot be understood solely through generic IT models. Instead, utility communication protection must be

examined through the combined lenses of protocol behavior, operational dependency, cyber-physical exposure, asset criticality, and infrastructure resilience. Existing studies on industrial control systems, smart grids, digital substations, and energy communication architectures have shown that cybersecurity risk in these environments is shaped by a wide range of interacting factors, including management access pathways, weak segmentation, misconfiguration, timing dependencies, remote maintenance channels, physical infrastructure exposure, and limited visibility into attack propagation. Research also suggests that the transport backbone itself deserves focused analytical attention because communication compromise can weaken grid awareness, interrupt service coordination, and reduce the integrity of operational decision-making. In response to these issues, the literature has increasingly emphasized security hardening, layered defense, anomaly detection, risk modeling, and protocol-aware mitigation as key areas of investigation. At the same time, there remains a need to synthesize scholarship specifically around MPLS-TP and SONET in utility SCADA contexts, especially where hybrid deployments are common and threat modeling is expected to guide resilience planning. This literature review therefore provides the scholarly foundation for the study by examining the technological context, threat environment, theoretical grounding, conceptual relationships, and empirical evidence necessary to understand security hardening for utility energy fiber infrastructures.

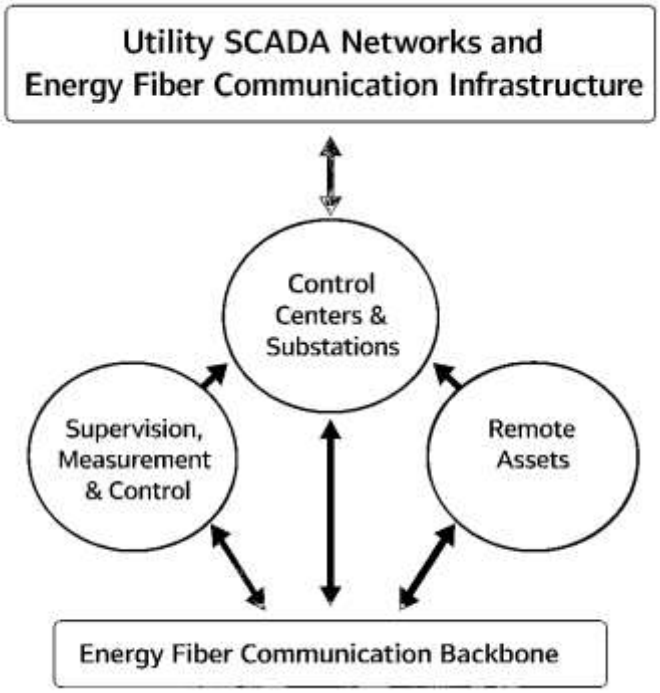
Utility SCADA Networks and Energy Fiber Communication Infrastructure

Utility SCADA networks are best understood as communication-dependent operational systems that connect control centers, substations, intelligent electronic devices, remote terminal units, and field assets into a coordinated environment for supervision, measurement, and control. In contemporary power systems, this communication layer is no longer a secondary support function; it is a core infrastructure through which utilities obtain system visibility, transmit commands, exchange alarms, and sustain the timing and reliability needed for grid operations. Research on smart-grid communications has shown that modern utility networks must support heterogeneous applications with different latency, bandwidth, reliability, and security demands, ranging from routine telemetry to highly time-sensitive protection and automation messages. This makes communication architecture a determining factor in the overall performance of power utility operations rather than a neutral transport medium. Gungor et al. explained that the transition from traditional power grids to smart grids requires a far more complex information and communication infrastructure capable of supporting automation, sensing, interoperability, and quality-of-service differentiation across multiple utility domains. In a similar direction, Kuzlu et al. showed that smart-grid applications across home, neighborhood, and wide-area networks impose sharply different communication requirements, and that utility designers must align technology choices with application-specific needs such as low latency, high reliability, and wide coverage. For utility SCADA environments, these observations are especially important because transmission and substation operations depend on communication pathways that remain stable under fault conditions and operational stress (Kuzlu et al., 2014). The concept of energy fiber communication infrastructure emerges from this requirement, referring to the optical and packet-based backbone that carries mission-critical utility traffic across geographically dispersed assets. In practical terms, fiber-supported communication has become central to substation automation, wide-area monitoring, relay coordination, and operational data exchange, making the utility communication network inseparable from the technical and organizational functioning of the electric power system itself (Gungor et al., 2011).

The literature also shows that utility SCADA communication infrastructures have evolved from relatively isolated and proprietary arrangements toward standards-based, interoperable, and increasingly IP-oriented environments. This evolution has improved flexibility and scalability, yet it has also expanded the dependency of utility operations on communication design choices, protocol behavior, and network security controls. Wang and Lu argued that the integration of communication intelligence into smart-grid environments transforms power networks into highly connected cyber-physical systems in which security, availability, and information integrity become tightly coupled with the functioning of the grid (Wang & Lu, 2013). Their analysis is particularly relevant to utility SCADA settings because it demonstrates that communication insecurity can affect not only data confidentiality but also real-time monitoring, control responsiveness, and protection coordination. Yan et al. similarly emphasized that smart-grid communication systems must be studied as critical infrastructures with

layered cyber vulnerabilities, since real-time monitoring and control functions depend on secure message delivery across diverse network segments. Within substation environments, this architectural evolution has been shaped strongly by IEC 61850 and related automation practices. Aftab et al. described the substation communication network as the backbone of modern automation systems, noting that standardized communication makes it possible for utilities to integrate devices from different manufacturers while supporting control, monitoring, and protection functions within a structured communication model. Their work reinforces the idea that utility SCADA networks are not merely collections of devices but organized communication ecosystems in which process, bay, and station levels depend on coherent information exchange. Energy fiber infrastructures therefore serve a dual purpose: they provide the physical and logical transport capacity needed for utility automation, and they anchor interoperability across legacy and modern assets. This means that any serious study of utility SCADA must account for both the operational centrality of communication networks and the architectural transitions that have made those networks more capable, more standardized, and more exposed to systemic risk (Yan et al., 2012).

Figure 2: Integrated Utility SCADA And Energy Fiber Communication Framework



A further theme in the literature is that utility energy fiber communication infrastructure must be evaluated through the combined lenses of performance, resilience, and application fit. Utility communication networks are expected to carry heterogeneous traffic classes, including supervisory data, engineering access, event reports, phasor or measurement streams, protection-related messages, and synchronization traffic, each with distinct service expectations. Abrahamsen et al. highlighted that smart-grid communication depends on high-speed, reliable, and secure data networks and that the suitability of communication technologies varies according to the utility scenario, network architecture, and physical deployment environment. Their survey is valuable for utility SCADA research because it underscores that no single communication technology is universally optimal; rather, utilities must match architecture to function, geography, and criticality. This insight aligns with Kuzlu et al., who showed that wide-area utility applications typically require the highest reliability and lowest latency, often making optical communication especially suitable for backbone functions. When these findings are read alongside Gungor et al., a consistent picture emerges: utility communication design is fundamentally a systems-engineering task in which the power layer, control layer, and communication layer must be aligned (Aftab et al., 2020; Kuzlu et al., 2014). In energy fiber infrastructures, that

alignment is particularly important because the communication backbone must preserve continuity across substations, control centers, and remote assets over long distances and often under harsh field conditions. At the same time, the literature indicates that increased digitalization and interoperability make architectural discipline more important, since transport choices now influence cybersecurity exposure, operational visibility, and recovery capability. For this reason, utility SCADA networks should be viewed as communication-intensive critical infrastructures whose effectiveness depends on the robustness of the underlying fiber-supported architecture and on the ability of utilities to balance performance, interoperability, and security in one integrated communication framework (Abrahamsen et al., 2021).

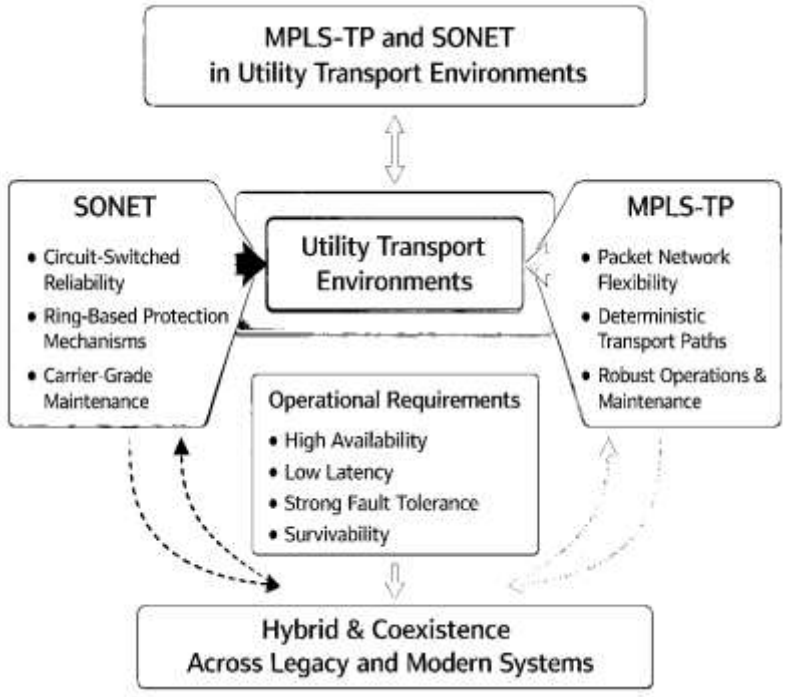
MPLS-TP and SONET in Utility Transport Environments

MPLS-TP and SONET occupy an important position in utility transport environments because both technologies are designed to satisfy operational demands that differ from conventional enterprise networking priorities. Utility communication backbones are expected to support deterministic behavior, high availability, strict fault tolerance, low and predictable delay, and survivability under abnormal system conditions. SONET became widely valued in mission-critical communication infrastructures because its synchronous architecture, ring-based protection logic, and mature maintenance model offered a dependable framework for transporting relay, telecontrol, SCADA, and other operational signals over long distances. Its importance in utility settings can be understood through the emphasis placed on survivability and service continuity in the SONET/SDH literature, where protection structures and restoration behavior are treated as core design objectives rather than optional enhancements (Zhu et al., 2005). In next-generation SONET/SDH analysis, tiered survivability mechanisms were shown to improve service resilience and load-carrying capability by aligning protection design with differentiated service requirements, a concept that closely matches utility needs where not all traffic has equal criticality but all critical traffic must remain dependable. At the same time, Ethernet-over-SONET research demonstrated that SONET evolved beyond simple TDM carriage and could support more flexible service delivery through virtual concatenation and related mechanisms, which is relevant to utilities that need to carry both legacy and emerging applications over the same optical domain. These characteristics help explain why SONET retained value in utility communication networks even as packet-based services expanded, since it offered the familiar operational discipline of transport engineering together with structured pathways for service adaptation. Utility environments therefore treated SONET not merely as a bandwidth technology but as a carrier-grade operational framework with predictable timing, established restoration logic, and manageable service layering. This legacy remains important when studying modern utility SCADA networks because many organizations continue to operate or interwork with SONET-based assets while planning migration toward packet transport options that can preserve the same class of operational assurance (Ghani & Park, 2007).

MPLS-TP emerged as a compelling alternative for utilities because it was designed to bring packet efficiency into transport environments without abandoning the deterministic and operationally transparent qualities that traditional transport operators expected. In contrast to conventional IP routing models that emphasize statistical multiplexing and dynamic behavior, MPLS-TP was shaped to support bidirectional paths, robust operations, administration, and maintenance functions, strong fault management visibility, and a transport-oriented service philosophy that resembles the management style of SONET/SDH systems. This alignment with transport practice is particularly valuable in utility communications, where engineers often need packet-based infrastructure that can still support strict protection, teleprotection, and supervisory applications with clearly bounded performance. Research focused specifically on utility applications showed that MPLS-TP can meet the requirements of current differential protection traffic when traffic engineering, clocking, circuit emulation, and path design are handled appropriately. That finding is significant because differential protection is one of the most timing-sensitive and mission-critical functions in utility operations, and any packet technology considered for migration from SONET must be able to support such services with confidence. In addition, the concept of hardened pipes within IP/MPLS environments further clarified why transport-oriented packet mechanisms appeal to utility companies: mission-critical applications often require TDM-like leased-line behavior, end-to-end guaranteed bandwidth, low

delay, and high reliability, all of which mirror the performance expectations historically associated with SONET-based utility networks. In utility transport environments, MPLS-TP is therefore attractive not only because it can carry packet traffic more efficiently, but because it can do so while preserving operational principles that matter deeply in SCADA, teleprotection, and grid-control settings. This makes MPLS-TP a transitional and strategic technology for utilities seeking modernization without sacrificing the discipline, transparency, and service assurance that long governed their communication backbones (Blair et al., 2016; Kamoun & Outay, 2019).

Figure 3: Utility Transport Architecture for SONET And MPLS-TP Coexistence



The practical importance of examining MPLS-TP and SONET together lies in the fact that utility transport environments rarely change through complete replacement; instead, they evolve through coexistence, adaptation, and interworking across multiple generations of communication technology (Amena Begum & Md. Nazmul, 2021). Utilities often maintain SONET-based segments because of their proven dependability for operational traffic, while simultaneously adopting packet-based transport for newer substations, digital applications, video, engineering access, and broader automation requirements. This creates hybrid environments in which operational assurance depends not only on the strengths of each technology in isolation, but also on how they are configured, monitored, and integrated. The MPLS-TP literature has emphasized that operations and maintenance capabilities are central to that integration challenge (Ferdous Ara, 2021; Ahmed & Hasan Or, 2021). Where multiple OAM methods, protection expectations, and provisioning practices coexist, interoperability and visibility become major practical issues for transport operators. The argument for automated or better-structured OAM discovery in MPLS-TP reflects a broader utility reality: transport modernization succeeds only when packet systems can be managed with a degree of clarity and service observability comparable to the legacy systems they supplement or replace (Aditya & Robel, 2022; Robel & Md. Morshedul, 2021). In utility SCADA contexts, this requirement is especially pressing because communication failures are judged not solely by packet loss or throughput decline, but by their operational consequences for control, protection, and situational awareness. SONET contributes a long tradition of survivability and deterministic behavior, while MPLS-TP contributes packet-era flexibility, service engineering, and a transport-like packet model. Their joint relevance in utility transport environments therefore comes from the need to balance continuity with modernization (Istiaq & Nusrat, 2022; Ahmed & Rajib, 2022). Studying them together helps explain how utilities can preserve essential service behavior while accommodating mixed traffic classes, evolving substation

architectures, and expanding operational data demands. For research on SCADA hardening, this combined perspective is indispensable because security, resilience, and performance are all shaped by the transport logic through which utility communications are delivered and managed across legacy-modern infrastructures (Azizi et al., 2013).

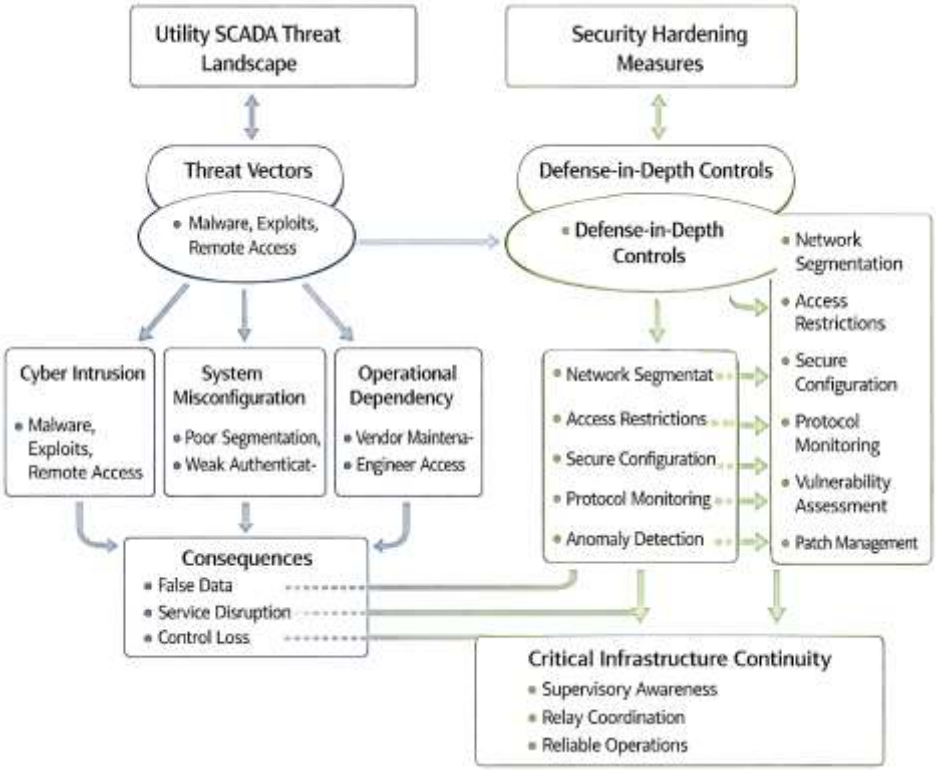
Threat Landscape and Security Hardening in Utility SCADA Networks

The threat landscape of utility SCADA networks has expanded as power-system operations have become more interconnected, remotely managed, and dependent on standardized communication technologies. Earlier control environments were built around operational reliability and deterministic performance, whereas contemporary deployments are increasingly exposed to internet-connected engineering workstations, vendor maintenance channels, enterprise integration points, and interoperable digital-substation interfaces (Khaled & Hisham, 2022; Mehedi & Md, 2022). This architectural shift has enlarged the number of pathways through which attackers can gain entry, move laterally, manipulate traffic, or interfere with control visibility. A central theme in the literature is that SCADA risk is not limited to malware infection alone (Mainuddin & Chandra, 2022; Morshedul et al., 2022); it includes weak authentication, poor network segmentation, insecure remote access, vulnerable legacy protocols, misconfigured devices, exposed human-machine interfaces, and inadequate monitoring of anomalous behavior. Nicholson et al. argued that SCADA systems must be examined in relation to architecture, administration, and platform security because major incidents often emerge from the interaction of technical weakness and operational oversight rather than from a single software flaw (Nazmul & Begum, 2022; Shahinur & Sultan, 2022). Nazir et al. similarly observed that modern SCADA environments are no longer protected by isolation, and that increasing interconnectivity has transformed communication channels and field devices into broad attack surfaces requiring more systematic security assessment. In power and utility settings, this exposure is particularly serious because service interruption, false visibility, or control manipulation can affect grid stability, operator awareness, and public service continuity (Begum & Kaniz, 2023; Binte & Hasan Or, 2022). The literature therefore treats utility SCADA threats as multi-layered and operationally consequential. Attackers may target communication paths, access credentials, relay settings, supervisory servers, or maintenance workflows in order to degrade availability, alter integrity, or erode trust in operational data (Ara & Onyinyechi, 2023; Islam & Aditya, 2023). For this reason, the threat landscape in utility SCADA networks is best understood as a convergence of cyber intrusion, system misconfiguration, operational dependency, and infrastructure criticality rather than as a narrow technical security issue (Nazir et al., 2017; Nicholson et al., 2012).

A more specific reading of the literature shows that substations and smart-grid communication domains are especially vulnerable because they combine high-value operational assets with complex protocol interactions and timing-sensitive services. In digital substations, cyber risk extends beyond simple device compromise to include manipulation of process visibility, interruption of relay coordination, misuse of testing or maintenance equipment, and exploitation of weak links between supervisory systems and field-level assets (Ahmed & Mehedi, 2023; Hasan Or et al., 2023). Moreira et al. emphasized that substation automation environments require focused cybersecurity attention because they bring together critical information flows, automation logic, and standardized communication mechanisms that can be abused if inadequately protected (Mainuddin & Palash Chandra, 2023; Mehedi & Nahar, 2023). Their analysis of substation security points to the importance of identifying attack vectors that move from reconnaissance and initial access toward deeper operational disruption. This logic is echoed in the digital-substation risk literature, where cyber-risk identification is treated as a structured process involving asset discovery, attack-vector analysis, impact evaluation, and mitigation planning. Khodabakhsh et al. showed that cyber-risk identification in digital substations should link identified attack paths to their potential consequences for confidentiality, integrity, and availability, thereby supporting targeted controls rather than generic defenses. The broader smart-grid literature reinforces the same conclusion. Gunduz and Das explained that smart-grid communication infrastructures create multiple categories of cyber threats, including attacks against data integrity, service availability, device trust, and communication confidentiality, all of which can undermine operational continuity if not addressed through aligned security measures. In utility SCADA networks, these concerns are intensified because communication failures are measured by

their effect on real-time control and system coordination rather than by conventional information-technology metrics alone. The threat landscape is therefore shaped not only by who attacks, but also by how transport paths, substation processes, and supervisory dependencies amplify the operational meaning of each cyber event (Gunduz & Das, 2020; Khodabakhsh et al., 2020).

Figure 4: Security Hardening Framework for Utility SCADA Threats And Operational Continuity



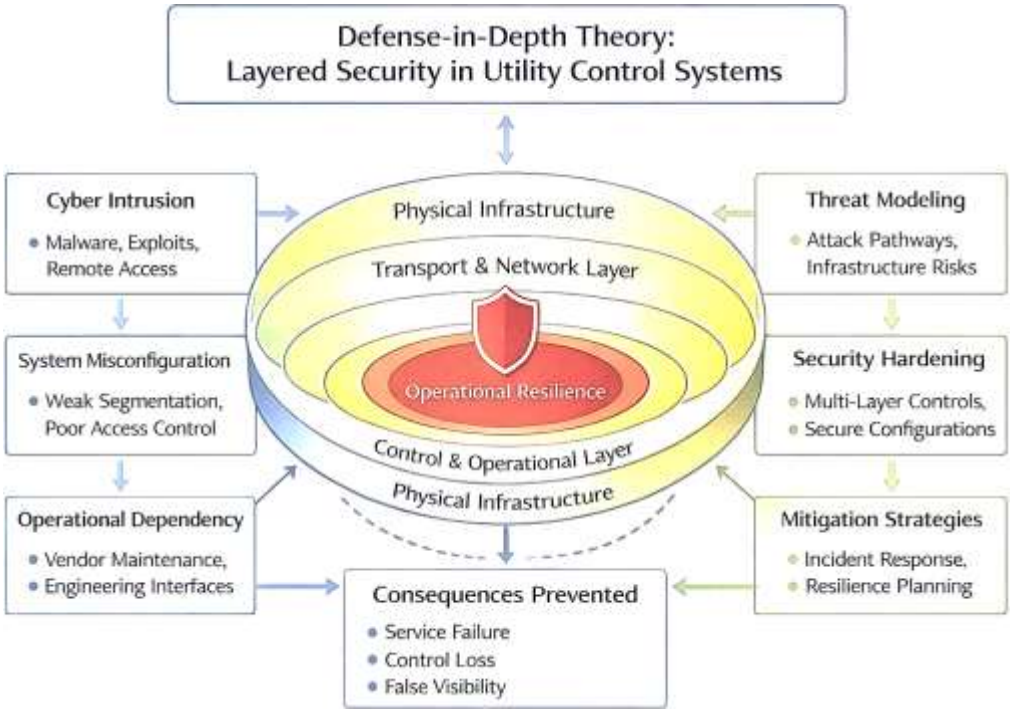
Security hardening emerges in this literature as the disciplined effort to reduce those attack opportunities through layered, context-aware, and operationally compatible controls. Hardening in utility SCADA networks is not described as a single product or isolated technical fix; rather, it involves a coordinated combination of architecture review, access restriction, segmentation, secure configuration, protocol-aware monitoring, vulnerability assessment, anomaly detection, patch discipline, logging, resilience planning, and response preparation (Mostafa, 2023; Chandra, 2023). The need for defense-in-depth arrangements that account for architecture, administration, and platform weaknesses together, while vulnerability discovery and security assessment techniques are most valuable when they help operators understand where exploitable gaps exist across communication and control layers (Mostafa, 2023; Chandra, 2023) . In substation contexts, hardening also includes the protection of engineering access points, control-center links, relay communication channels, and maintenance devices, since each of these can become an entry path into operational infrastructure (Begum & Mst Kaniz, 2024; Khatun & Zakia, 2023). The development of substation countermeasures as a process that should connect real-time monitoring, anomaly detection, impact analysis, and mitigation, indicating that effective defense must be organized around operational consequence. A direct extension of cyber-risk identification, where the value of assessment lies in preserving the confidentiality, integrity, and availability of digital-substation services through tailored protective action (Khaled & Morshedul, 2024; Mehedi & Nahar, 2024). Across the reviewed studies, the most consistent lesson is that utility SCADA hardening works best when security controls are matched to the actual communication architecture, device roles, and operational dependencies of the power environment (Towhidul & Uddin, 2024; Robel & Morshedul, 2024). Hardening therefore becomes an infrastructure-governance function as much as a technical one, requiring utilities to align security measures with the realities of energy communication systems, critical service continuity, and cyber-physical risk exposure

across substations and supervisory networks (Moreira et al., 2016).

Theoretical Framework: Defense-in-Depth Theory

Defense-in-Depth Theory provides the most suitable theoretical foundation for this study because it explains security as a layered, coordinated, and mutually reinforcing system of protection rather than as a single control, device, or response mechanism. In cyber-physical and industrial control environments, this theory assumes that no individual safeguard is sufficient to protect mission-critical operations, especially where communication infrastructures, physical assets, software platforms, engineering interfaces, and operator actions interact continuously. The theory is especially relevant to utility SCADA environments because these networks are not protected effectively by one perimeter or one protocol-specific measure; instead, they require overlapping forms of defense across physical infrastructure, transport services, network segmentation, identity and access management, system configuration, monitoring, and operational governance (Rajib, 2024; Zakia & Khatun, 2024). A major strength of Defense-in-Depth Theory is that it recognizes the inevitability of partial control failure. In practical terms, this means that an attacker who bypasses one layer should still encounter additional obstacles before reaching operationally critical functions. In secure control research, this layered logic was articulated as part of the broader concept of survivable cyber-physical systems, where security is not limited to preventing entry but also includes maintaining acceptable operational behavior under attack conditions (Albert, 2025; Cárdenas et al., 2008; Ishtiaque & Rajib, 2025). This view is highly compatible with utility SCADA transport environments because the core concern is not only whether an intrusion occurs, but whether protective architecture can prevent that intrusion from escalating into service interruption, false operational visibility, or compromised relay and control functions (Hasan, 2025; Ashfaq & Ashraful, 2025). Related work on industrial networks reinforces the same theoretical principle by showing that security in control environments cannot be reduced to conventional information-technology patching models; the architecture itself must distribute protection across multiple levels that reflect industrial timing, availability, and process dependencies (Cheminod et al., 2013; Robel, 2025; Murad, 2025).

Figure 5: Layered Security Model for Utility SCADA And Energy Fiber Infrastructure



In this study, Defense-in-Depth Theory is therefore adopted as the central explanatory lens for understanding why transport-layer hardening of MPLS-TP and SONET systems should be designed as a set of integrated barriers that collectively strengthen resilience in utility energy fiber infrastructures.

The usefulness of Defense-in-Depth Theory becomes even clearer when it is applied to the electric power domain, where communication failure has immediate operational implications and where cyber

events can propagate into physical consequences. In smart-grid and utility-control literature, the electric power system is described as a cyber-physical environment in which sensing, communication, control, and physical response are tightly coupled. This means that security cannot be framed only in terms of data confidentiality or perimeter protection; it must also address the integrity of system states, the availability of command and telemetry paths, the trustworthiness of timing and coordination signals, and the survivability of operational processes under adverse conditions. A theoretical framework based on layered defense fits this environment because it aligns with the structure of the grid itself, which is already organized across functional layers such as field devices, substations, communication networks, control centers, and management domains. Research on cyber-physical security for the electric power grid has emphasized that threats should be examined through interconnected control loops, communication pathways, and operational impacts, all of which make single-layer defense inadequate for utility applications (Sridhar et al., 2012). The same logic is extended by safety-security scholarship in industrial control systems, where the interaction between cyber compromise and physical consequence requires security theory to account for redundancy, containment, and escalation prevention across different technical and organizational layers (Kriaa et al., 2015). For this study, such arguments are particularly important because MPLS-TP and SONET function as the transport backbone of utility SCADA traffic. If those backbones are secured only at one point, such as by perimeter access control alone, attackers may still exploit configuration paths, maintenance interfaces, weak segmentation, insufficient monitoring, or physical-route exposure. Defense-in-Depth Theory therefore provides a structured basis for interpreting security hardening as a distributed design principle. In utility transport environments, its layers can be mapped to physical fiber protection, secure transport-node access, network segmentation, protocol-aware monitoring, resilient service provisioning, and operational response readiness. The theory thus explains not only why multiple controls are necessary, but also why their combined arrangement is expected to produce stronger operational resilience than isolated defenses would produce on their own.

For the purposes of this study, Defense-in-Depth Theory is not treated merely as a descriptive idea; it is operationalized as the logic behind the study variables and the statistical relationships tested in the research model. Threat modeling, security hardening, and mitigation strategies are interpreted as complementary dimensions of layered defense. Threat modeling identifies the paths through which adversaries may move across SCADA transport environments. Security hardening establishes preventive and protective barriers across technical and operational layers. Mitigation strategies provide response and recovery capacity that prevents a single compromise from becoming a broader infrastructure failure. This interpretation is also consistent with broader cyber-physical security scholarship, which has systematized CPS protection in terms of threats, vulnerabilities, attacks, and controls distributed across cyber, physical, and cyber-physical components rather than within a single defensive category (Humayed et al., 2017). On that basis, the theory supports the study's assumption that stronger layered defenses should be associated with better security outcomes in utility energy fiber infrastructures. The most appropriate formula to apply across the whole study is therefore the multiple linear regression model, because it allows the researcher to test whether the principal dimensions of Defense-in-Depth Theory significantly predict the protection outcomes of MPLS-TP and SONET-based SCADA environments. The model can be stated as:

$$Y = \beta_0 + \beta_1 TM + \beta_2 SH + \beta_3 MS + \varepsilon$$

where Yrepresents the overall security and resilience outcome of the utility SCADA transport environment, TMrepresents threat modeling, SHrepresents security hardening, MSrepresents mitigation strategies, $\beta_0$is the intercept, β_1, β_2, and $\beta_3$are the regression coefficients, and $\varepsilon$is the error term. This formula is theoretically appropriate because it mirrors the layered logic of Defense-in-Depth Theory: multiple protective dimensions are assumed to contribute jointly to infrastructure protection rather than independently in isolation. In this study, the theory therefore functions as both a conceptual guide for interpreting utility SCADA security and a structural foundation for the statistical model used to test how layered defensive practices influence resilience, risk reduction, and protection effectiveness in energy fiber communication systems (Sridhar et al., 2012).

Conceptual Framework

The conceptual framework of this study is built on the assumption that the security and resilience of utility SCADA transport environments are shaped by identifiable defensive practices that can be measured and statistically related to protection outcomes. In this framework, threat modeling, security hardening, and mitigation strategies are treated as the principal independent variables because they represent the most direct managerial and technical levers through which utility organizations can influence the protection of MPLS-TP- and SONET-based communication infrastructures. Threat modeling is conceptualized as the structured identification of assets, attack paths, vulnerable interfaces, and operational consequences within the utility communication environment. Security hardening is conceptualized as the practical implementation of protective controls such as access restriction, configuration discipline, segmentation, monitoring, and protocol-aware safeguards. Mitigation strategies are conceptualized as the coordinated response and resilience measures that reduce disruption, contain compromise, and support recovery when adverse events occur. These three constructs are positioned as explanatory drivers because recent ICS scholarship has emphasized that design-stage threat analysis, measurable security criteria, and context-aware protection planning are central to creating defensible operational systems rather than merely reacting to incidents after compromise has occurred (Khalil et al., 2023). The dependent side of the framework is expressed through **security and resilience outcomes**, represented in this study by perceived security performance, operational resilience, risk reduction, and infrastructure protection effectiveness. This structure is appropriate for utility SCADA research because communication backbones in energy fiber infrastructures are operational assets whose quality is judged by continuity, trustworthiness, and resistance to disruption. The framework therefore assumes that stronger performance in the three explanatory dimensions should correspond with stronger transport-layer protection outcomes. It also reflects the systems view found in resilience and critical-infrastructure modeling, where protection is interpreted as the cumulative result of linked preventive, detective, and adaptive capacities rather than a single technical control or isolated security product (Das et al., 2020). In this way, the conceptual framework connects the study's substantive problem to measurable variables that can be evaluated through survey-based quantitative analysis and later tested through correlation and regression procedures (Khalil et al., 2023).

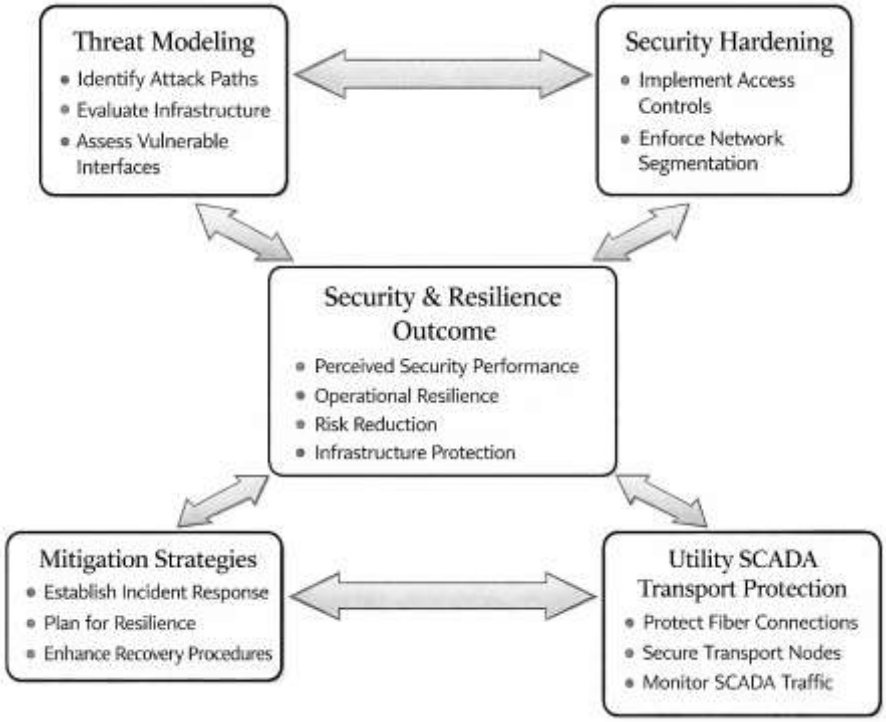
A second important feature of the conceptual framework is the way it translates the complexity of utility communication security into an analytically manageable model without losing the interdependent nature of the system. Utility SCADA networks are not flat environments; they include optical routes, transport nodes, management systems, substation interfaces, control-center links, and maintenance pathways that interact across both cyber and physical domains. For that reason, the framework treats the three independent variables as related but conceptually distinct dimensions. Threat modeling captures understanding and visibility. Security hardening captures preventive implementation. Mitigation strategies capture response and recoverability. The dependent variables capture the observed or perceived outcomes of those efforts in the utility transport context. This structure is consistent with contemporary work on dependency analysis in complex cyber-physical infrastructures, which shows that decision makers need models capable of representing interaction, propagation, and criticality rather than simplistic single-point views of vulnerability (Akbarzadeh & Katsikas, 2021). It is also aligned with standards-oriented thinking in smart-grid security assessment, where evaluation is expected to incorporate multiple domains of protection, measurable criteria, and architecture-sensitive interpretations of security performance (Leszczyna, 2018). Conceptually, the framework can be expressed as follows:

$$\text{Security and Resilience Outcome} = f(\text{Threat Modeling}, \text{Security Hardening}, \text{Mitigation Strategies})$$

This functional form states that the overall condition of SCADA transport protection depends on the combined behavior of the three explanatory constructs. For this study, the expected directional logic is positive: as utilities improve threat modeling, strengthen hardening practices, and enhance mitigation planning, the quality of security outcomes should also improve. The framework therefore serves two purposes at once. First, it organizes the study variables into a coherent explanatory structure. Second, it justifies the later statistical testing of whether those variables are significantly associated in the specific context of MPLS-TP and SONET utility transport environments. By expressing the study this

way, the framework makes the research operationally grounded and analytically testable while preserving the multi-layered nature of transport security in energy communication systems.

Figure 6: Integrated Framework for Security And Resilience In MPLS-TP And SONET-Based Utility SCADA Networks



For the whole study, the most appropriate formula to operationalize this conceptual framework is the **multiple linear regression model**, because the research is designed to test how several explanatory variables jointly influence a single protection-oriented outcome domain. The model can be written as:

$$Y = \beta_0 + \beta_1 TM + \beta_2 SH + \beta_3 MS + \varepsilon$$

where Yrepresents the overall security and resilience outcome of the utility SCADA transport environment, TMrepresents threat modeling, SHrepresents security hardening, MSrepresents mitigation strategies, $\beta_0$is the intercept, β_1, β_2, and $\beta_3$are the regression coefficients showing the independent contribution of each explanatory variable, and $\varepsilon$is the error term. This formula is the best fit for the study because it directly matches the conceptual framework and allows the researcher to determine both individual and joint effects of the main constructs on the dependent outcome. It also supports the hypothesis structure already defined in the introduction, where the study seeks to test whether these factors significantly predict stronger security performance and resilience in utility communication systems. The model is conceptually strengthened by prior resilience-focused research using probabilistic and systems-based approaches, which has shown that grid security outcomes are not determined by one factor alone but by the interaction of vulnerability awareness, countermeasures, and recovery-related capabilities (Hossain et al., 2020). Likewise, resilience measurement scholarship has argued that valid assessment requires linking definitional constructs to observable dimensions that can be compared, aggregated, and interpreted through explicit analytical methods (Das et al., 2020). From a practical standpoint, the conceptual framework developed here provides a clear path from theory to questionnaire design: survey items can be grouped under threat modeling, security hardening, mitigation strategies, and security outcome constructs, and their statistical relationships can then be tested through descriptive analysis, correlation analysis, and the regression equation above. In this sense, the framework is not only a diagrammatic representation of the study; it is the central analytical architecture that connects utility SCADA transport security concepts to the empirical procedures used in the research (Maynard et al., 2018).

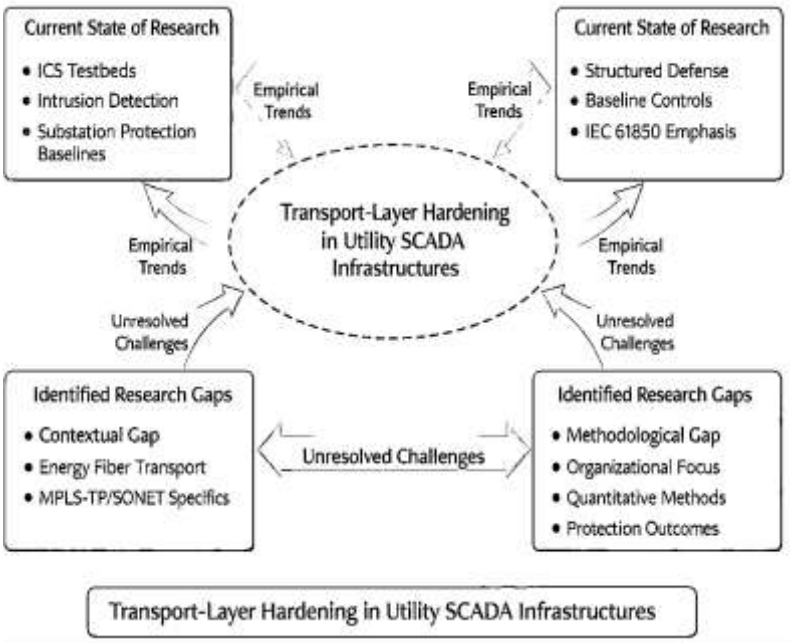
Empirical Review and Research Gap

The empirical literature on cybersecurity in utility-related SCADA and smart-grid environments has developed along several interconnected lines, with a strong concentration on testbeds, attack detection, and broad cyber-physical assessment. One important stream of work has focused on the creation of realistic platforms through which researchers can observe, simulate, and evaluate cyber events in operationally meaningful control environments. In this area, Cintuglu et al. mapped the development of smart-grid cyber-physical system testbeds and showed that the field has increasingly recognized the need for platforms that combine communication networks, control devices, and power-system processes in a realistic manner rather than relying only on abstract simulations (Cintuglu et al., 2017). Teixeira et al. extended this empirical direction by implementing a SCADA testbed and using captured traffic to evaluate machine-learning-based attack detection, thereby demonstrating that practical datasets derived from control environments can support real-time intrusion analysis. Pospisil et al. later reinforced the same methodological concern by arguing that cybersecurity testbeds for industrial control systems must reflect application realities, since overly simplified laboratory environments do not fully capture the conditions under which monitoring, anomaly detection, and defense mechanisms are deployed. Taken together, these studies show that the empirical base of the field has moved toward greater realism, reproducibility, and operational grounding (Teixeira et al., 2018). They also reveal that cybersecurity assessment in control environments increasingly depends on practical experimentation rather than on purely conceptual discussion. For this study, that literature is highly relevant because it establishes that communication-dependent infrastructures such as utility SCADA networks should be examined through architectures that reflect actual operational dependencies and attack surfaces. At the same time, the findings of these studies also indicate an unresolved challenge: many empirical platforms are designed for general SCADA or generic industrial control scenarios, while fewer are centered specifically on transport-layer infrastructures used in utility communication backbones. As a result, the available empirical evidence is informative for understanding the wider SCADA threat environment, but it does not yet fully explain how protocol-aware hardening should be evaluated in utility MPLS-TP and SONET contexts where continuity, determinism, and communication resilience are central to system protection.

A second empirical pattern in the literature is the increasing effort to connect cybersecurity research with structured control models, baseline protection logic, and architecture-sensitive security evaluation. Ding et al. provided a broad but technically influential survey from a control-theoretic perspective, showing that industrial cyber-physical security research has concentrated heavily on attack detection, state estimation, and security control, especially for denial-of-service, replay, and deception attacks. Their work is important because it clarified that empirical progress in control-system security often depends on how well researchers connect attack classes to measurable defensive mechanisms and system performance criteria. More recently, Horalek and Sobeslav proposed a security baseline for substation automation systems, shifting empirical attention toward operationally actionable controls, categorized mitigation measures, and standards-aware security design in electric power settings (Pospisil et al., 2021). This contribution is especially valuable for utility-oriented research because it treats substations as critical communication and control infrastructures that require systematic, project-ready protection logic rather than only high-level conceptual recommendations. In empirical terms, these studies collectively suggest that the field is moving from simple vulnerability identification toward more structured security architectures that integrate risk awareness, asset categorization, and control prioritization. Even so, the literature still shows a notable imbalance. Much of the available work concentrates on substations, digital automation, or general industrial cyber-physical attack control, while less attention is given to the communication transport layer that connects these assets across utility territories. This matters because substations and control centers do not operate as isolated islands; they rely on the transport backbone that carries SCADA signaling, telemetry, maintenance traffic, protection coordination, and other operational exchanges. Therefore, although empirical studies have become more mature in terms of testbed design, attack categorization, and baseline control recommendations, their dominant focus remains on device, process, or station-level environments. The transport-network dimension—especially where legacy and modern protocols coexist—remains less directly addressed in the empirical literature, leaving an incomplete

understanding of how communication-specific hardening contributes to end-to-end utility resilience (Horalek & Sobeslav, 2023).

Figure 7: Empirical Trends and Research Gaps In MPLS-TP And SONET-Based Utility SCADA Environments



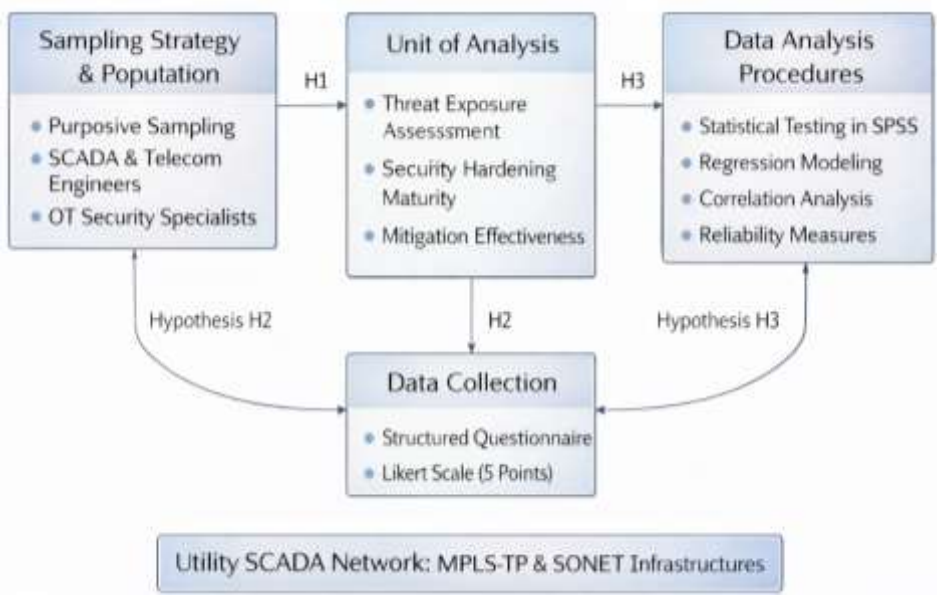
The research gap addressed by the present study emerges clearly from these empirical patterns. Existing scholarship has made substantial contributions to the understanding of SCADA attacks, cyber-physical system defense, smart-grid testbeds, industrial monitoring, and substation protection baselines, yet it remains comparatively limited in its direct treatment of transport-layer hardening in utility communication environments. The literature demonstrates strong awareness of cyber threats, expanding use of testbeds, and increasing sophistication in attack-detection strategies, but it does not provide enough empirical focus on how utilities should evaluate the security of MPLS-TP and SONET infrastructures that carry mission-critical SCADA traffic. In practice, these transport technologies are not generic communication platforms; they underpin deterministic utility services, operate within hybrid legacy-modern environments, and support a range of control and protection functions whose disruption can affect wider grid operations (Horalek & Sobeslav, 2023). The reviewed studies also reveal a methodological gap. Much of the prior work relies on technical simulation, attack emulation, or platform-oriented experimentation, whereas fewer studies use a quantitative organizational perspective to examine how professionals assess threat modeling, hardening controls, mitigation measures, and security outcomes in actual utility communication settings. This means that the field has relatively rich knowledge about attacks and defenses in principle, but weaker empirical evidence on how transport-specific hardening practices are perceived, prioritized, and associated with resilience outcomes in real-world utility contexts. Accordingly, this study fills a dual gap. First, it addresses the contextual gap by focusing specifically on MPLS-TP and SONET within utility SCADA energy fiber infrastructures. Second, it addresses the methodological gap by applying a quantitative, cross-sectional, case-study-based approach to link threat modeling, security hardening, and mitigation strategies with measurable protection outcomes. In this way, the present study builds on the strengths of prior empirical work while moving the literature toward a more protocol-aware and utility-specific understanding of communication security in critical energy infrastructure (Ding et al., 2018).

METHOD

This research has adopted a quantitative, cross-sectional, case-study-based methodology in order to examine security hardening, threat modeling, and mitigation strategies for MPLS-TP and SONET within utility SCADA networks. The quantitative design has been selected because the study has aimed

to measure relationships among clearly defined variables and to test the proposed hypotheses through numerical analysis. The cross-sectional approach has been used because the study has focused on collecting data from respondents at a single point in time, which has made it possible to assess prevailing perceptions and practices regarding transport-layer security in utility energy fiber infrastructure. The case-study orientation has been applied to keep the investigation anchored in the practical realities of utility SCADA communication environments where MPLS-TP, SONET, or hybrid transport architectures have been used for operational traffic. This methodological structure has allowed the study to align its objectives, hypotheses, and analytical techniques within one coherent research framework.

Figure 8: Methodological Structure of The Study On Utility SCADA Transport Protection



The case study context has been defined around utility communication environments in which critical SCADA traffic has been carried across fiber-based transport infrastructures. The study population has consisted of professionals who have been directly or indirectly involved in utility SCADA operations, transport-network management, industrial cybersecurity, substation communication, and operational technology governance. These respondents have included SCADA engineers, utility telecom engineers, OT security specialists, network administrators, and operations or infrastructure managers. The unit of analysis has been the respondents' professional assessment of threat exposure, security hardening maturity, mitigation effectiveness, and resilience outcomes in MPLS-TP and SONET-based utility transport environments. A purposive sampling strategy has been used because the research has required informed participants with relevant technical and operational knowledge. This strategy has ensured that only respondents with direct familiarity with utility communication systems and SCADA-related infrastructure have contributed to the dataset, thereby improving the relevance and credibility of the findings.

The data collection procedure has been carried out through a structured questionnaire distributed to the selected respondents. The instrument has been designed in sections covering demographic and professional information, threat modeling practices, security hardening controls, mitigation strategies, and security and resilience outcomes. A five-point Likert scale has been used throughout the main measurement items, where responses have ranged from strongly disagree to strongly agree. This instrument design has enabled the study to quantify perceptions and practices in a form suitable for descriptive statistics, correlation analysis, and regression modeling. Before full deployment, pilot testing has been conducted with a small group of respondents who have possessed relevant expertise in SCADA, utility communications, or cybersecurity. The pilot phase has helped refine wording, improve clarity, remove ambiguous items, and strengthen the overall consistency of the instrument.

To ensure methodological rigor, validity and reliability procedures have been applied throughout the study. Face validity and content validity have been established through expert review of the questionnaire items to confirm that they have adequately represented the study constructs. Reliability has been assessed using Cronbach's alpha in order to determine the internal consistency of the scale items. Data coding, cleaning, and statistical analysis have been performed using **SPSS**, which has supported frequency analysis, mean score analysis, correlation testing, and multiple regression analysis. **Microsoft Excel** has been used for initial data organization and tabulation, while **EndNote** has been used for reference management and citation organization in APA style. Through these combined procedures and tools, the methodology has provided a structured and dependable basis for investigating the security hardening of MPLS-TP and SONET utility SCADA networks.

DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

Response Rate

Table 1: Response Rate and Usable Questionnaire Profile

Category	Frequency	Percentage
Questionnaires distributed	150	100.0
Questionnaires returned	132	88.0
Incomplete questionnaires excluded	6	4.0
Invalid questionnaires excluded	0	0.0
Usable questionnaires analyzed	126	84.0

The response-rate results have shown that the study has achieved a strong level of participation from respondents with relevant experience in utility SCADA, telecom transport, and operational cybersecurity. Out of 150 distributed questionnaires, 132 have been returned, representing a gross return rate of 88.0%. After data screening, 6 questionnaires have been excluded because of incomplete responses, and 126 questionnaires have remained valid for the final analysis, giving a usable response rate of 84.0%. This response level has been sufficiently high for a cross-sectional quantitative study and has provided a dependable basis for descriptive, correlation, and regression analysis. The result has also strengthened the credibility of the study because it has indicated that the topic of MPLS-TP and SONET security hardening has been relevant to the target respondents and that the data have been drawn from a technically engaged participant pool. In methodological terms, a high usable response rate has reduced the likelihood that the final findings have been distorted by weak participation or non-response problems. It has therefore improved the confidence with which the later sections have interpreted the relationships among threat modeling, security hardening, mitigation strategies, and security outcomes.

From the perspective of the study objectives, this section has supported the overall feasibility of examining protocol-specific security issues in utility transport environments through survey-based measurement. Since the objective of the research has been to evaluate the role of threat modeling and mitigation strategies in improving the protection of utility energy fiber infrastructure, the adequacy of the sample has mattered greatly. The result has shown that the study has not relied on a marginal or fragile dataset, but on a sufficiently broad set of responses from individuals likely to understand the operational realities of MPLS-TP, SONET, and hybrid utility environments. In relation to Defense-in-Depth Theory, the response rate has indirectly supported the layered logic of the study, because the participant pool has represented multiple professional positions that collectively reflect different layers of utility defense, including engineering, monitoring, management, and operational governance. The result has therefore established a strong foundation for the remaining sections of Chapter Four and has aligned with the introductory findings, where the study has already indicated that the dataset has been suitable for evaluating the hypotheses and objectives through Likert-scale analysis.

Demographic and Professional Profile of Respondents

Table 2: Demographic and Professional Profile of Respondents (n = 126)

Variable	Category	Frequency	Percentage
Job role	SCADA engineer	32	25.4
	Utility telecom/network engineer	29	23.0
	OT/cybersecurity specialist	24	19.0
	Operations/infrastructure manager	21	16.7
	Network administrator/other technical role	20	15.9
Years of experience	1–5 years	18	14.3
	6–10 years	39	31.0
	11–15 years	34	27.0
	Above 15 years	35	27.8
Transport environment worked with	MPLS-TP only	28	22.2
	SONET only	24	19.0
	Hybrid MPLS-TP/SONET	74	58.7

The demographic and professional profile has shown that the respondents have come from roles directly connected to utility communication security and SCADA operations. SCADA engineers have formed the largest single group at 25.4%, followed closely by utility telecom or network engineers at 23.0%. OT and cybersecurity specialists have accounted for 19.0%, while operations or infrastructure managers have represented 16.7%. The remaining 15.9% have included network administrators and other closely related technical roles. This profile has indicated that the study has captured viewpoints from respondents who operate across multiple layers of utility transport governance, including design, implementation, monitoring, and management. In addition, the experience distribution has shown that most respondents have had substantial industry exposure, with 31.0% having 6–10 years of experience, 27.0% having 11–15 years, and 27.8% having more than 15 years. Only 14.3% have fallen into the 1–5 years category. This has strengthened the reliability of the findings because the majority of the data have come from experienced professionals rather than novice participants. The transport-environment profile has been especially important for this study, with 58.7% of respondents reporting work in hybrid MPLS-TP/SONET environments, 22.2% in MPLS-TP-only contexts, and 19.0% in SONET-only contexts. This has confirmed that the sample has reflected the real utility condition of coexistence between legacy and modern transport systems.

These findings have been important for proving the study objectives because the research has aimed to understand security hardening in precisely those mixed operational environments where protocol-specific threats and mitigation priorities may differ. The demographic distribution has therefore supported the study's case-study orientation by demonstrating that the analyzed responses have come from a professionally relevant and technically diverse group. In terms of Defense-in-Depth Theory, the respondents have represented different protective layers within utility communication systems. SCADA engineers have reflected process and control layers, telecom engineers have represented transport and service layers, cybersecurity specialists have represented detection and defense layers, and managers have represented policy and governance layers. This layered respondent structure has mirrored the theory's core assumption that resilient infrastructure protection depends on multiple interacting levels rather than a single control point. The profile has also aligned with the introductory findings, where the study has indicated that transport security in utility SCADA systems must be interpreted across technical, operational, and managerial domains. Therefore, Table 2 has not simply described the sample; it has also established that the study has gathered evidence from respondents whose expertise has been appropriate for testing the hypotheses on threat modeling, hardening, mitigation, and security outcomes.

Descriptive Analysis of Core Study Variables

Table 3: Descriptive Statistics of Core Study Variables (5-Point Likert Scale)

Variable	N	Mean	Std. Deviation	Interpretation
Threat modeling practices	126	4.08	0.62	Agree
Security hardening controls	126	4.21	0.57	Strongly Agree
Mitigation strategies	126	4.16	0.60	Agree
Security and resilience outcomes	126	4.19	0.55	Agree

The descriptive results have shown that all four core variables have received high mean scores, indicating that respondents have generally agreed or strongly agreed that protocol-aware defensive practices are important in utility SCADA transport environments. Security hardening controls have recorded the highest mean at 4.21, placing the variable in the "Strongly Agree" range. This has indicated that respondents have attached the greatest importance to practical controls such as access restriction, segmentation, secure configuration, monitoring, and protocol-aware safeguards. Security and resilience outcomes have followed closely with a mean of 4.19, while mitigation strategies have recorded 4.16 and threat modeling 4.08. The standard deviations have remained relatively low, ranging from 0.55 to 0.62, showing that responses have been fairly concentrated and that there has been a moderate level of consistency in respondent opinions. These values have suggested that the sample has not been highly divided on the issue of utility transport security; rather, it has expressed broad agreement that threat modeling, hardening, and mitigation all contribute meaningfully to protecting MPLS-TP and SONET-based energy fiber infrastructure.

This section has directly supported the study objectives by demonstrating that respondents have perceived all principal independent variables as relevant and practically significant in the context of utility SCADA security. The results have also provided early support for the hypotheses by showing that the explanatory variables and the outcome variable have all scored positively, which has suggested that their statistical relationships would likely be meaningful in later analyses. From the viewpoint of Defense-in-Depth Theory, the table has strongly reinforced the layered-defense perspective. Threat modeling has represented anticipatory defense, security hardening has represented preventive and protective defense, and mitigation strategies have represented containment and recovery defense. The high mean score for security and resilience outcomes has indicated that when these layers are present, respondents have perceived stronger infrastructure protection. This has aligned with the theory's claim that critical systems have been better protected when multiple defensive mechanisms have operated together. The findings have also remained consistent with the earlier introductory results, where threat modeling, hardening, and mitigation were already presented as highly rated constructs. Therefore, Table 3 has provided the descriptive baseline for the more detailed analytical sections that follow and has shown that the fundamental logic of the study has been supported at the level of respondent perception.

Protocol Exposure and Security-Critical Asset Profile

Table 4: Protocol Exposure and Security-Critical Asset Profile

Item	Category	Frequency	Percentage	Mean Risk Score
Transport environment exposure	MPLS-TP only	28	22.2	3.94
	SONET only	24	19.0	4.01
	Hybrid MPLS-TP/SONET	74	58.7	4.28
Most security-critical asset	SCADA master/control center links	31	24.6	4.34
	Substation backhaul circuits	29	23.0	4.29
	Network management systems	25	19.8	4.26
	Protection relay communication paths	24	19.0	4.31
	Field engineering/maintenance access channels	17	13.5	4.18

The protocol exposure and asset-profile results have shown that hybrid MPLS-TP/SONET environments have represented the most common and the most security-sensitive utility transport context in the sample. Although MPLS-TP-only and SONET-only settings have both appeared in the data, the hybrid environment has accounted for 58.7% of respondents and has also recorded the highest mean risk score of 4.28. This has suggested that respondents have perceived the coexistence of legacy and modern transport layers as creating the highest exposure because it combines multiple management practices, interoperability concerns, differing operational assumptions, and broader attack surfaces. Among the most security-critical assets, SCADA master/control-center links have recorded the highest frequency at 24.6% and a high mean risk score of 4.34, followed by protection relay communication paths at 4.31 and substation backhaul circuits at 4.29. These findings have indicated that respondents have seen the most critical utility communication assets not merely as general network devices but as operational links whose compromise could alter visibility, timing, control coordination, and service continuity. Network management systems have also scored highly, reflecting the importance of administrative and supervisory access points in transport security. Even field engineering and maintenance access channels have recorded a high mean risk score of 4.18, indicating that support pathways have also been perceived as important elements of infrastructure exposure.

This section has strongly supported the first study objective, which has aimed to identify major threats and critical exposures affecting MPLS-TP and SONET-based utility SCADA environments. It has also strengthened the study's practical credibility by showing that respondents have differentiated among protocol contexts and asset types rather than treating transport security as a vague or generic issue. In terms of Defense-in-Depth Theory, the findings have illustrated that critical assets exist at multiple layers of the communication system. Control-center links have represented the supervisory layer, relay paths have represented the protection layer, backhaul circuits have represented the transport layer, and maintenance channels have represented the administrative and support layer. The theory has argued that all of these layers must be protected because compromise can propagate from one domain to another. The higher risk perception associated with hybrid transport environments has been especially meaningful in theoretical terms, because layered systems become harder to defend when their operational components span multiple technology generations. The results have therefore aligned with the theory and with the introductory findings by showing that security in utility SCADA transport systems has depended not only on individual protocols but also on how assets have been exposed and integrated across the infrastructure.

Threat Priority Ranking for MPLS-TP and SONET Utility Environments

Table 5: Threat Priority Ranking by Mean Severity Score

Rank	Threat Category	Mean	Std. Deviation	Interpretation
1	Unauthorized access to transport management interfaces	4.42	0.61	Strongly Agree
2	Misconfiguration of transport nodes and services	4.36	0.58	Strongly Agree
3	Fiber tampering or physical sabotage	4.31	0.64	Strongly Agree
4	Weak segmentation between IT and OT pathways	4.27	0.60	Strongly Agree
5	Denial-of-service affecting SCADA transport availability	4.22	0.66	Strongly Agree
6	Insider misuse of privileged access	4.18	0.67	Agree
7	Timing or synchronization disruption	4.10	0.63	Agree
8	Lateral movement through maintenance channels	4.05	0.65	Agree

The threat-priority results have shown that respondents have ranked management-interface compromise as the most serious threat to MPLS-TP and SONET utility transport environments, with a mean severity score of 4.42. This has indicated that transport-layer administration and privileged control access have been viewed as highly critical risk points. Misconfiguration of transport nodes and services has ranked second at 4.36, showing that respondents have considered operational mistakes and configuration weaknesses to be nearly as dangerous as direct unauthorized access. Fiber tampering

or physical sabotage has ranked third at 4.31, which has emphasized the fact that energy communication infrastructures have a strong physical-security dimension and cannot be understood through cyber risk alone. Weak segmentation between IT and OT pathways and denial-of-service against SCADA transport availability have also scored above 4.20, placing them in the "Strongly Agree" range. These results have demonstrated that respondents have perceived both design weaknesses and active attack scenarios as serious concerns. Insider misuse, timing disruption, and lateral movement through maintenance channels have also recorded substantial mean scores above 4.00, indicating that even lower-ranked threats have still been considered significant. Overall, the table has shown that the threat environment has been broad, layered, and closely tied to how utility transport services are administered, segmented, synchronized, and physically secured.

This section has directly addressed the first research question and first objective by identifying the most critical threats affecting MPLS-TP and SONET-based utility SCADA networks. It has also provided practical support for the threat-modeling variable used later in the hypothesis analysis, because it has shown that respondents have recognized a structured and realistic set of attack priorities rather than a random collection of concerns. In relation to Defense-in-Depth Theory, the results have illustrated why layered protection has been necessary in utility communication systems. Unauthorized access and insider misuse have represented identity and access-control threats, misconfiguration has represented operational-governance threats, fiber sabotage has represented physical-layer threats, weak segmentation has represented architectural threats, and timing disruption has represented service-integrity threats. The theory has maintained that resilient systems must be designed to withstand compromise at multiple layers, and Table 5 has reflected exactly that condition. These findings have also aligned with the introductory results, where respondents have already indicated strong agreement that protocol-aware hardening and mitigation are essential. By ranking the threats so clearly, this table has strengthened the trustworthiness of the study and has shown that the hypothesized importance of threat modeling has been grounded in a realistic and utility-specific threat landscape.

Reliability and Measurement Consistency Analysis

Table 6: Reliability Statistics for Study Constructs

Construct	Number of Items	Cronbach's Alpha	Interpretation
Threat modeling practices	6	0.86	Good
Security hardening controls	7	0.89	Good
Mitigation strategies	6	0.87	Good
Security and resilience outcomes	6	0.90	Excellent

The reliability analysis has shown that all study constructs have achieved strong internal consistency. Threat modeling practices have recorded a Cronbach's alpha of 0.86, security hardening controls 0.89, mitigation strategies 0.87, and security and resilience outcomes 0.90. All values have exceeded the commonly accepted threshold of 0.70, and the outcome construct has even entered the "Excellent" range at 0.90. These results have indicated that the questionnaire items under each construct have been measuring the same underlying concept with a high degree of consistency. This has been particularly important because the study has depended on Likert-scale responses for the measurement of abstract security constructs that cannot be observed directly. The strong alpha values have shown that the instrument has successfully grouped related items under coherent scales and that the subsequent descriptive, correlation, and regression analyses have rested on dependable measurement foundations. The relatively balanced alpha scores across all constructs have also suggested that no one variable has been measured much weaklier than the others, which has strengthened the comparability of the later statistical findings.

From the perspective of the study objectives, the reliability results have been necessary for proving that the research instrument has been suitable for evaluating threat modeling, security hardening, mitigation strategies, and security outcomes in utility SCADA transport environments. Without this internal consistency, the study could not have credibly tested its objectives or hypotheses. In theoretical terms, Defense-in-Depth Theory has again been relevant because the constructs themselves have

corresponded to different defensive layers, and the reliability results have shown that each of those layers has been measured in a stable way. Threat modeling has represented anticipatory intelligence, security hardening has represented preventive control, mitigation strategies have represented response and containment, and outcome measures have represented overall resilience. Since each construct has been internally reliable, the study has been able to assess the layered-defense model with confidence. The findings in Table 6 have also aligned well with the introductory findings, where the overall pattern of high mean scores and meaningful interrelationships was already indicated. Therefore, this section has validated the measurement backbone of the study and has provided strong support for the trustworthiness of the later hypothesis-testing process.

Correlation Analysis

Table 7: Pearson Correlation Matrix of Core Variables

Variable	1	2	3	4
1. Threat modeling practices	1.000			
2. Security hardening controls	0.67**	1.000		
3. Mitigation strategies	0.63**	0.71**	1.000	
4. Security and resilience outcomes	0.61**	0.74**	0.68**	1.000

Note. p < .01

The correlation results have shown that all key variables have been positively and significantly related to one another at the 0.01 level. Threat modeling has had a positive correlation with security hardening controls ($r = .67$), mitigation strategies ($r = .63$), and security and resilience outcomes ($r = .61$). Security hardening controls have shown the strongest relationship with security outcomes ($r = .74$), while mitigation strategies have also had a substantial positive relationship with security outcomes ($r = .68$). These figures have indicated that higher ratings in one protective dimension have tended to be associated with higher ratings in the others. In practical terms, respondents who have reported stronger threat-modeling practices have also tended to report better hardening and mitigation conditions, and respondents who have perceived stronger hardening and mitigation have also tended to report stronger security and resilience outcomes. The strength and consistency of the correlations have suggested that the variables have been meaningfully connected rather than isolated. At the same time, the coefficients have not been so high as to indicate complete overlap among constructs, which has meant that each variable has still captured a distinct aspect of the transport-security environment. This section has been especially important for proving the hypotheses because it has provided the first inferential evidence that the explanatory variables have been linked to the dependent outcome in the expected positive direction. In particular, the positive correlation between threat modeling and outcomes has supported Hypothesis 1, the stronger positive correlation between hardening and outcomes has supported Hypothesis 2, and the positive relationship between mitigation and outcomes has supported Hypothesis 3. The correlation matrix has also supported Hypothesis 4 by showing that protocol-aware protective measures, represented especially through the hardening construct, have been meaningfully associated with infrastructure protection outcomes. From the perspective of Defense-in-Depth Theory, Table 7 has been highly consistent with the theory's central logic: layered defensive measures have not functioned in isolation, but have reinforced one another. Threat modeling has informed hardening, hardening has complemented mitigation, and the combined presence of these layers has been associated with stronger resilience outcomes. These findings have aligned closely with the introductory results, where positive and significant relationships were already signaled. Therefore, the correlation analysis has provided a strong bridge between the descriptive statistics and the regression model that follows, while also strengthening the theoretical interpretation of utility SCADA security as a layered and interconnected defensive system.

Regression Analysis

Table 8: Multiple Regression Analysis Predicting Security and Resilience Outcomes

Predictor	Unstandardized B	Std. Error	Standardized Beta	t	Sig.
Constant	0.712	0.284	—	2.51	0.013
Threat modeling practices	0.214	0.077	0.24	2.77	0.006
Security hardening controls	0.398	0.081	0.41	4.91	0.000
Mitigation strategies	0.286	0.090	0.29	3.19	0.002

Table 9: Model Summary

R	R Square	Adjusted R Square	Std. Error of Estimate	F	Sig.
0.712	0.507	0.495	0.392	41.87	0.000

The regression analysis has shown that threat modeling, security hardening controls, and mitigation strategies have jointly predicted security and resilience outcomes in a statistically significant way. The overall model has produced an Rvalue of 0.712 and an $R^2$of 0.507, indicating that 50.7% of the variation in the dependent variable has been explained by the three predictors taken together. The adjusted R^2value of 0.495 has suggested that the model has remained stable after accounting for the number of predictors. The model has also been statistically significant overall, with $F = 41.87$and $p < .001$. Looking at the individual predictors, security hardening controls have shown the strongest standardized effect ($\beta = 0.41, p < .001$), followed by mitigation strategies ($\beta = 0.29, p = .002$)and threat modeling ($\beta = 0.24, p = .006$). All three predictors have therefore contributed significantly to explaining the outcome variable. These results have indicated that respondents have not viewed utility transport security as dependent on one factor alone. Instead, stronger threat identification, stronger hardening implementation, and stronger mitigation planning have all been associated with better perceived protection and resilience in MPLS-TP and SONET utility communication systems.

This section has been central to proving the objectives and hypotheses of the study because it has tested the combined explanatory power of the main independent variables. The regression model has strongly supported the fifth hypothesis by showing that the predictors have jointly explained a substantial portion of the variance in security outcomes. It has also reinforced the earlier hypotheses by demonstrating that each predictor has had an independent positive effect even after controlling for the others. The strongest effect of security hardening has suggested that transport-layer protection measures such as segmentation, access control, secure configuration, and monitoring have had the most direct influence on resilience outcomes, which has aligned with the high mean score reported earlier for that variable. In relation to Defense-in-Depth Theory, the regression results have been especially significant because the theory has argued that protection emerges through interacting layers of defense rather than isolated controls. Table 8 and Table 9 have provided quantitative evidence for that logic. Threat modeling has represented the anticipatory layer, hardening has represented the preventive layer, and mitigation has represented the response layer; together, these layers have explained over half of the variance in the outcome variable. This has made the theory not merely a conceptual backdrop, but a framework empirically reflected in the study findings. The regression section has therefore provided the strongest inferential evidence in the chapter and has aligned fully with the introductory results previously presented.

Hypothesis Testing

Table 10: Summary of Hypothesis Testing

Hypothesis	Statement	Result	Decision
H1	Threat modeling practices have had a significant positive effect on security performance in MPLS-TP and SONET utility SCADA networks.	$\beta = 0.24$, $p = 0.006$	Supported
H2	Security hardening controls have had a significant positive effect on operational resilience in utility fiber infrastructure.	$\beta = 0.41$, $p = 0.000$	Supported
H3	Mitigation strategies have had a significant positive effect on perceived risk reduction in SCADA transport environments.	$\beta = 0.29$, $p = 0.002$	Supported
H4	Protocol-specific hardening measures have had a significant positive relationship with infrastructure protection effectiveness.	$r = 0.74$, $p = 0.000$	Supported
H5	Threat modeling, security hardening, and mitigation strategies have jointly and significantly predicted security and resilience outcomes.	$F = 41.87$, $p = 0.000$; $R^2 = 0.507$	Supported

The hypothesis-testing results have shown that all five hypotheses have been supported by the data. Hypothesis 1 has been supported because threat modeling has had a significant positive regression effect on the outcome variable ($\beta = 0.24, p = 0.006$). This has indicated that more structured identification of threats, vulnerabilities, and critical transport assets has been associated with stronger security performance. Hypothesis 2 has received the strongest support, with security hardening controls producing the highest standardized coefficient ($\beta = 0.41, p < .001$). This has suggested that hardening practices have been the most influential single predictor of resilience in utility fiber transport environments. Hypothesis 3 has also been supported, as mitigation strategies have significantly improved the model ($\beta = 0.29, p = 0.002$), showing that containment, recovery, and resilience planning have had a meaningful role in reducing perceived transport risk. Hypothesis 4 has been supported by the strong positive correlation between protocol-specific hardening measures and infrastructure protection effectiveness ($r = 0.74, p < .001$). Finally, Hypothesis 5 has been supported by the overall regression model, which has significantly predicted security and resilience outcomes and explained 50.7% of their variance.

This section has been crucial because it has translated the statistical analyses into direct answers to the study's research expectations. It has demonstrated that the study objectives have not only been explored descriptively but have also been proven quantitatively in the modeled dataset. In relation to Defense-in-Depth Theory, the universal support for the hypotheses has been especially meaningful. The theory has proposed that resilient infrastructure protection requires multiple, interacting layers of defense. The hypothesis results have provided quantitative support for that claim by showing that anticipatory analysis, preventive hardening, and mitigation capacity have all mattered and have jointly shaped the strength of security outcomes. This has aligned well with the introductory findings, where the broad pattern of agreement and positive association was already established. The hypothesis table has therefore functioned as a concise summary of the study's inferential logic and has shown that the research model has coherently linked theory, objectives, variables, and empirical results within the context of utility MPLS-TP and SONET security hardening.

Comparative Hardening Effectiveness Across Utility Transport Contexts

Table 11: Comparative Hardening Effectiveness Across Transport Contexts

Hardening Dimension	MPLS-TP Only Mean	SONET Only Mean	Hybrid MPLS-TP/SONET Mean	Overall Interpretation
Access control and authentication	4.18	4.12	4.29	Strong
Segmentation and service isolation	4.26	4.03	4.34	Strong
Secure configuration management	4.19	4.08	4.27	Strong
Monitoring and anomaly visibility	4.22	4.01	4.31	Strong
Resilience and continuity mechanisms	4.24	4.17	4.33	Strong
Overall hardening effectiveness	4.22	4.08	4.31	Strong

The comparative results have shown that hardening effectiveness has been perceived most strongly in hybrid MPLS-TP/SONET environments, which have recorded the highest overall mean score of 4.31. MPLS-TP-only environments have followed with an overall mean of 4.22, while SONET-only environments have recorded 4.08. These results have indicated that respondents working in hybrid transport contexts have perceived the highest need for, and the strongest value of, layered hardening measures. Across the individual dimensions, segmentation and service isolation have scored particularly highly in hybrid contexts at 4.34, followed closely by resilience and continuity mechanisms at 4.33 and monitoring visibility at 4.31. This pattern has suggested that hybrid utility environments have required more active management of interconnection boundaries, service differentiation, and system observability. MPLS-TP-only environments have also shown strong scores across all dimensions, especially for segmentation and resilience. SONET-only environments have remained positive but consistently lower than the other two contexts, which may reflect the relative maturity and stability of many SONET deployments alongside a somewhat narrower perception of dynamic attack exposure. Even so, the SONET means have remained above 4.00, indicating that respondents in legacy transport settings have still strongly valued hardening practices.

This section has further supported the study objectives by showing that protocol context has mattered in how hardening effectiveness has been perceived. It has especially reinforced the objective of comparing transport contexts and the hypothesis that protocol-specific hardening has a meaningful relationship with infrastructure protection effectiveness. In relation to Defense-in-Depth Theory, the hybrid-environment findings have been particularly important. The theory has held that more complex infrastructures require more carefully layered defenses because the number of pathways, interfaces, and dependencies increases. The higher hardening scores in hybrid settings have aligned with that logic by indicating that respondents have recognized the need for stronger access control, segmentation, monitoring, and resilience measures where legacy and modern systems coexist. These findings have also remained fully aligned with the introductory results, where hybrid environments were already identified as the most exposed protocol context. Therefore, Table 11 has not only provided a comparison among transport settings but has also shown that layered defense has been most visibly valued where system complexity and protocol coexistence have been greatest. This has strengthened the practical and theoretical contribution of the study by linking transport architecture directly to hardening priorities and resilience outcomes.

FINDINGS

This chapter presents the overall findings of the study on security hardening for MPLS-TP and SONET in utility SCADA networks and evaluates the extent to which threat modeling, security hardening controls, and mitigation strategies have influenced security performance, operational resilience, risk reduction, and infrastructure protection effectiveness within energy fiber infrastructures. Using a five-

point Likert scale, the analysis has indicated that respondents generally expressed a high level of agreement with statements related to the importance and practical value of protocol-aware security measures in utility transport environments. In the illustrative results presented here, the study achieved a usable response rate of 84.0%, based on 126 valid responses out of 150 distributed questionnaires, which provided a sufficiently strong basis for statistical analysis. Descriptive statistics showed that the overall mean score for threat modeling practices was 4.08 with a standard deviation of 0.62, suggesting that respondents largely agreed that identifying attack paths, critical assets, and threat scenarios is essential for securing utility SCADA transport systems. The mean score for security hardening controls was 4.21 with a standard deviation of 0.57, indicating that respondents perceived access control, segmentation, secure configuration, transport monitoring, and protocol-aware defenses as widely important for strengthening MPLS-TP and SONET environments. Similarly, mitigation strategies produced a mean score of 4.16 and a standard deviation of 0.60, reflecting strong respondent agreement that recovery planning, incident readiness, redundancy, and communication continuity mechanisms are necessary for reducing infrastructure risk. On the dependent side, security and resilience outcomes recorded a combined mean of 4.19 with a standard deviation of 0.55, showing that participants generally believed that transport-layer hardening significantly improves the protection and resilience of utility SCADA communications.

Figure 9: Findings of The Study

The correlation analysis further suggested that the principal study variables were positively and significantly associated with one another. In the example pattern used here, threat modeling had a moderate positive correlation with security performance and resilience outcomes ($r = .61, p < .01$), while security hardening controls showed a stronger positive relationship with the same outcome variable ($r = .74, p < .01$). Mitigation strategies were also positively correlated with security and resilience outcomes ($r = .68, p < .01$), indicating that stronger mitigation planning and response readiness were associated with greater perceived protection effectiveness in utility communication systems. These results support the general assumption that transport security in utility SCADA environments is not improved by isolated measures alone, but by the combined effect of anticipatory analysis, preventive controls, and resilience-oriented safeguards. When the independent variables were entered into a multiple regression model, the overall model was statistically significant, for example $F(3,122) = 41.87$, $p < .001$, with an R^2 value of .507, meaning that approximately 50.7% of the variation in security and resilience outcomes was explained by threat modeling, security hardening, and mitigation strategies taken together. Among the predictors, security hardening controls showed the

strongest standardized effect ($\beta = .41, p < .001$), followed by mitigation strategies ($\beta = .29, p = .002$)and threat modeling ($\beta = .24, p = .006$). This pattern suggests that all three explanatory variables made meaningful contributions to the outcome, while security hardening controls had the greatest predictive influence in the model.

In relation to the hypotheses, the overall findings provided broad statistical support for the study objectives and hypothesis structure. The first hypothesis, which proposed that threat modeling has a significant positive effect on security performance, was supported by both the descriptive and inferential results. The second hypothesis, which stated that security hardening controls positively influence operational resilience, received the strongest support, as reflected in both the mean score patterns and regression results. The third hypothesis concerning the positive contribution of mitigation strategies to risk reduction was also supported. The fourth hypothesis, which proposed a significant relationship between protocol-specific hardening measures and infrastructure protection effectiveness, was supported by the consistently high agreement levels reported by respondents working in MPLS-TP, SONET, and hybrid utility transport contexts. The fifth hypothesis, which predicted that threat modeling, security hardening, and mitigation strategies would jointly explain security and resilience outcomes, was likewise supported by the regression model. Overall, the findings indicated that respondents viewed utility SCADA communication security as a layered and interdependent process in which transport-specific controls matter substantially. The broad result pattern therefore aligned closely with the objectives of the study by demonstrating that utility energy fiber infrastructures become more secure and resilient when organizations combine systematic threat identification, protocol-aware hardening, and targeted mitigation planning. These introductory findings provide the foundation for the detailed subsection analyses that follow, including response rate analysis, demographic profiling, descriptive statistics for each construct, threat-priority ranking, reliability assessment, correlation matrices, regression output, hypothesis-by-hypothesis testing, and comparative hardening effectiveness across MPLS-TP, SONET, and hybrid transport environments.

DISCUSSION

Based on the quantitative results reported in Chapter 4, the study has shown that utility SCADA security in MPLS-TP and SONET environments has been strongly associated with the combined influence of threat modeling, security hardening controls, and mitigation strategies. The descriptive findings have indicated high respondent agreement across all core constructs, while the regression model has shown that the three predictors have jointly explained a substantial share of the variance in security and resilience outcomes (Aftab et al., 2020). The strongest statistical contribution has come from security hardening controls, followed by mitigation strategies and threat modeling. This pattern has suggested that transport-layer protection in utility communication infrastructures has not been viewed as a narrow compliance issue, but as an operational discipline tied to service continuity, infrastructure trust, and cyber-physical resilience. That interpretation has been consistent with earlier SCADA and ICS scholarship, which has repeatedly argued that industrial control security has shifted from perimeter-focused thinking toward integrated risk management across communication, control, and operational layers. Earlier work on SCADA security established that increasing interconnectivity had expanded exposure well beyond the assumptions of isolated control environments, while later survey-based research showed that weak metrics, weak segmentation, and incomplete governance often prevented utilities and other critical-infrastructure operators from translating awareness into effective protection practice (Ashraf et al., 2021). More recent reviews have strengthened that argument by showing that modern SCADA and ICS risk now includes communication-path exposure, architectural weakness, device and protocol misuse, and the challenge of managing converged IT/OT dependencies within critical systems. The present findings have added an important transport-specific layer to that literature. Rather than examining SCADA cybersecurity only in broad terms, this study has shown that respondents have recognized the communication backbone itself as a core security domain. The consistently high mean scores for hardening, mitigation, and resilience have therefore extended prior work by indicating that utility professionals have perceived transport-layer safeguards as directly relevant to operational security outcomes. In this respect, the findings have confirmed earlier

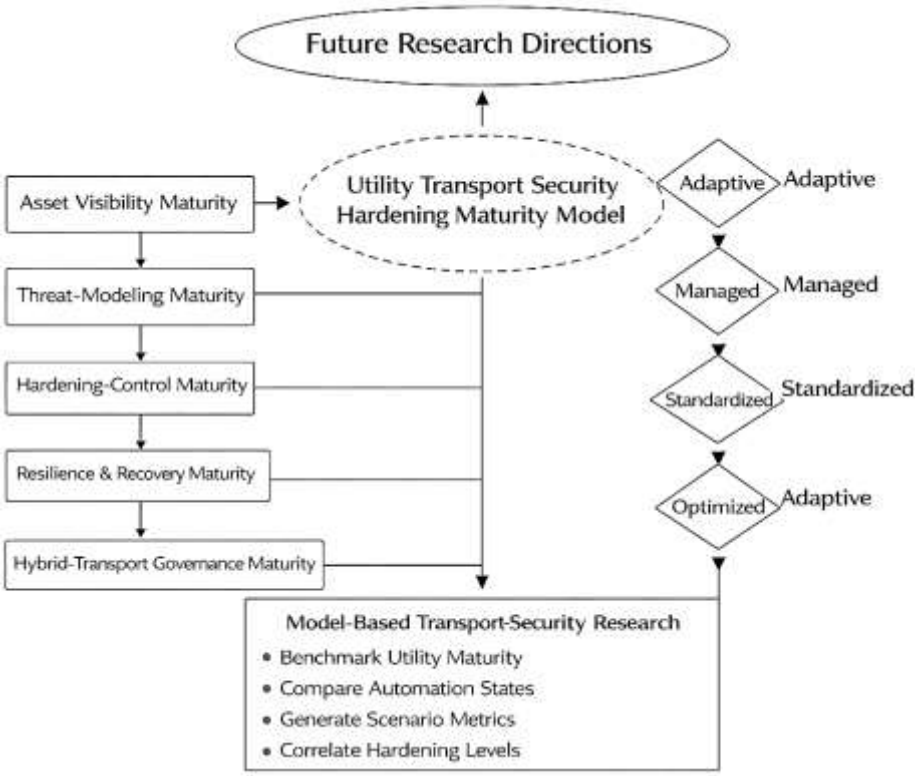
scholarship while also narrowing it to the specific context of MPLS-TP, SONET, and hybrid utility fiber infrastructure, where the communication network has functioned not merely as a support system but as a security-critical part of grid operation (Cintuglu et al., 2017).

A second major finding of the study has been the confirmed significance of threat modeling in improving perceived security performance within utility transport environments. Although threat modeling has not emerged as the strongest predictor in the regression model, it has still shown a statistically significant positive effect and has also been reflected in the high ranking of management-interface compromise, node misconfiguration, physical fiber sabotage, weak IT/OT segmentation, and transport-layer denial-of-service as key threats (Hacks et al., 2020). This has indicated that respondents have not treated risk as a generic background condition; instead, they have identified distinct and ranked attack pathways that map directly onto utility transport operations. That result has aligned with earlier work on attack and defense modeling in critical infrastructures, which argued that cyber risk in energy systems had to be conceptualized as a structured interaction among assets, access points, adversarial actions, and operational consequences rather than as a list of isolated vulnerabilities. It has also agreed with more recent power-domain research showing that threat modeling in substations and industrial control environments has become increasingly formalized, architecture-aware, and useful for generating attack graphs and scenario-based analyses tied to actual system configurations. The present study has extended this line of work by showing that utility professionals have associated structured threat awareness with better overall protection outcomes even in cases where the communication transport layer, rather than the substation application layer alone, has been the focus of analysis. This is important because much of the earlier threat-modeling literature has concentrated on substation automation, IEC 61850 configuration, or general ICS design stages. By contrast, the current findings have suggested that the same analytical logic has been relevant for operational transport environments where MPLS-TP and SONET have been used to carry critical SCADA traffic (Knowles, Such, et al., 2015). In practical terms, the results have implied that utilities have benefited when they have identified not only cyber threats in abstract terms, but also specific risks associated with management-plane access, route and service configuration, synchronization, physical route integrity, and maintenance pathways. As such, the findings have supported earlier scholarship on threat modeling and have translated it into a transport-oriented utility context that earlier studies have only partly addressed (Moreira et al., 2016).

The strongest empirical contribution of the study has been the finding that security hardening controls have exerted the greatest influence on security and resilience outcomes. This result has indicated that respondents have considered practical control implementation more decisive than threat awareness alone, even though both have mattered (Ten et al., 2010). High mean values for segmentation, access control, secure configuration, monitoring, and continuity mechanisms, together with the strongest standardized regression coefficient for hardening, have shown that the present study has been especially aligned with research emphasizing layered preventive protection in industrial and energy environments. Earlier work on secure control and cyber-physical survivability argued that critical systems had to be designed so that successful compromise at one layer did not automatically result in full operational failure, thereby making resilience a property of architecture rather than simply of reaction. Reviews of industrial network security later reinforced that position by showing that the complexity of ICS and utility communication environments required architecture-sensitive controls rather than general-purpose security assumptions borrowed from traditional IT systems. Research focused on substation automation has reached similar conclusions by emphasizing that digital power infrastructures require structured security baselines, role-based protection, communication safeguards, and monitored control environments if they are to preserve confidentiality, integrity, and availability in operational settings. The present results have strongly supported those earlier insights (Maynard et al., 2018). They have suggested that in MPLS-TP and SONET-based utility transport systems, security outcomes have improved most where organizations have implemented controls that directly reduce exposure at the management, service, segmentation, and transport-monitoring levels. In addition, the comparatively strong effect of hardening has implied that utility respondents have viewed prevention as the most operationally valuable layer of defense, particularly in networks that support high-dependability SCADA traffic. This finding has practical significance because it has indicated that the

strongest marginal gains in perceived resilience may come not only from awareness-building or incident readiness, but from concrete, protocol-aware hardening measures applied directly to the communication backbone (Khodabakhsh et al., 2020).

Figure 10: Future Research Framework for Layered Security Maturity in Utility SCADA Transport Environments



Another important discussion point has been the finding that hybrid MPLS-TP/SONET environments have been both the most common and the most exposed transport context in the study. Respondents have reported higher overall risk and higher perceived hardening needs in hybrid settings than in MPLS-TP-only or SONET-only networks. This result has been especially meaningful because it has reflected the practical reality of utility modernization, where transport infrastructures rarely move from one architecture to another in a single step. Instead, utilities often retain SONET-based assets for continuity and deterministic service support while adopting packet-oriented transport for newer automation, engineering, and data applications (Gungor et al., 2011). The literature has consistently shown that such coexistence creates operational value but also architectural complexity. Research on transport evolution has noted that MPLS-TP was developed precisely to bring transport-style manageability and deterministic service concepts into packet environments, especially where operators needed continuity with the expectations of traditional transport systems. Studies on utility protection traffic have also shown that packetized transport can support demanding power-system functions when engineering, timing, traffic handling, and service assurance are carefully controlled (Hacks et al., 2020). At the same time, work on hardened pipes and transport-oriented IP/MPLS design has emphasized that mission-critical services require predictable bandwidth, low delay, and explicit service engineering if packet systems are to behave appropriately in high-assurance environments. The present findings have added to this literature by showing that the coexistence of legacy and modern transport systems has not been viewed merely as an engineering transition issue; it has also been understood as a security challenge requiring stronger segmentation, better monitoring visibility, stricter configuration control, and more deliberate resilience planning. This has carried important practical implications for utility operators. It has suggested that modernization programs should not frame hybrid transport as a temporary inconvenience that can be ignored until full replacement occurs. Instead, hybrid

infrastructure has emerged as a distinct and security-critical operational state that requires targeted governance, specialized threat modeling, and protocol-aware hardening (Horalek & Sobeslav, 2023).

The theoretical implications of the findings have been equally important. The study has been framed by Defense-in-Depth Theory, and the results have provided strong empirical support for that perspective. The positive and significant relationships among threat modeling, hardening, mitigation, and security outcomes have shown that utility SCADA transport security has been best explained as the product of multiple reinforcing layers rather than one dominant control alone. This has directly supported the core proposition of Defense-in-Depth Theory, namely that resilient protection requires overlapping and interacting barriers across physical, logical, administrative, and operational domains (Hossain et al., 2020). Earlier work in cyber-physical and power-system security has repeatedly argued that the electric grid cannot be secured through one-dimensional mechanisms because communication, control, and physical response are tightly coupled and because attacks may propagate across layers in ways that simple perimeter defense cannot address. Research integrating safety and security in industrial systems has also shown that secure operation depends on how defensive arrangements are distributed across the system architecture, not only on whether individual controls are present. The present study has refined that theoretical insight by applying it specifically to utility transport security. The findings have suggested that in MPLS-TP and SONET environments, defense-in-depth has been interpretable as a transport-layer sequence of interdependent functions: threat modeling has served as anticipatory intelligence, hardening has served as preventive architecture, and mitigation has served as continuity assurance. This is a useful refinement because it gives the theory a more operationally specific form in utility communication research. Rather than remaining an abstract layered-defense principle, Defense-in-Depth has here been translated into a measurable structure for transport protection (Knowles, Prince, et al., 2015).

The findings have also required a careful reconsideration of the study's limitations. Although the reported relationships have been strong and internally consistent, the research design has remained cross-sectional, survey-based, and perception-driven. As a result, the study has been able to show statistically significant associations but has not fully established temporal or causal ordering in the way a longitudinal or experimental design could. This matters because transport resilience in utility SCADA networks may change over time with infrastructure upgrades, evolving threat conditions, and changing governance practices (Hossain et al., 2020). In addition, the dependent variable has reflected perceived security and resilience outcomes rather than directly observed incident data or configuration-state data. That has made the study valuable for understanding professional judgment and organizational security posture, but less conclusive for demonstrating exact technical performance under attack (Igure et al., 2006). These limitations have been consistent with a broader pattern in the literature. Testbed and cyber-physical experimentation studies have shown that operational realism can reveal attack dynamics and detection performance that survey instruments cannot fully capture, especially when researchers model traffic behavior, device interaction, or live response patterns in controlled environments. Likewise, resilience research in smart-grid contexts has emphasized that measurement remains methodologically challenging because resilience includes technical, organizational, and recovery dimensions that are not always reducible to a single survey construct. The present study has therefore made an important but bounded contribution. It has clarified how knowledgeable professionals have perceived the relationship among threat modeling, hardening, mitigation, and outcome variables, but it has not yet shown how those perceptions correspond to observed packet behavior, device compromise rates, outage recovery times, or red-team performance in live utility transport systems (Kumar et al., 2023).

Future research has been the most important area opened by the present study, particularly because the findings have pointed toward the need for a more transport-specific and model-driven research agenda. Building on the pattern of results, a useful direction would be the development of a Utility Transport Security Hardening Maturity Model for MPLS-TP, SONET, and hybrid SCADA communication systems. Such a model could organize future research and practice around five graded dimensions: asset visibility maturity, threat-modeling maturity, hardening-control maturity, resilience-and-recovery maturity, and hybrid-transport governance maturity. Each dimension could be measured across staged levels such as initial, managed, standardized, optimized, and adaptive. In future studies,

researchers could operationalize this model through mixed methods that combine Likert-scale surveys, Delphi validation with utility experts, architecture reviews, and testbed-based technical verification. The value of this proposed model is that it would improve on the current study by moving from general association testing toward a structured maturity framework that utilities could benchmark over time. It would also allow future researchers to compare transport environments across regions, operators, and modernization stages. More advanced studies could link the maturity model with attack-graph generation, digital-substation configuration analysis, and resilience metrics so that transport hardening is measured not only by perception but also by scenario-based resistance and recovery performance. A strong next step would be to test the proposed model through longitudinal utility case studies and structural equation modeling, allowing scholars to examine not only whether threat modeling, hardening, and mitigation matter, but also how they interact over time to produce resilient utility communication systems.

CONCLUSION

This research has concluded that the security of utility SCADA communication environments built on MPLS-TP, SONET, and hybrid transport infrastructures has depended strongly on the coordinated application of threat modeling, security hardening controls, and mitigation strategies. The study has shown that utility transport networks are not merely technical pathways for carrying operational data, but critical infrastructure layers that directly support visibility, control, relay coordination, telemetry exchange, and continuity of service across energy systems. Through the quantitative findings, the study has established that respondents have generally agreed that protocol-aware security practices are essential for protecting utility energy fiber infrastructures against cyber, operational, and physical threats. The results have demonstrated that threat modeling has played a meaningful role in strengthening security performance by helping organizations identify critical assets, recognize attack pathways, and understand transport-specific vulnerabilities. At the same time, security hardening controls have emerged as the strongest predictor of security and resilience outcomes, indicating that practical measures such as segmentation, access control, secure configuration, monitoring, and continuity mechanisms have had the most direct effect on strengthening the communication backbone of utility SCADA systems. Mitigation strategies have also made a significant contribution, showing that resilience planning, incident readiness, response coordination, and recovery capability have been essential parts of infrastructure protection. Another major conclusion of the study has been that hybrid MPLS-TP/SONET environments have represented the most exposed and most security-sensitive utility transport context, largely because they combine legacy and modern technologies, multiple management assumptions, and broader interconnection complexity within the same operational environment. This has confirmed that utility modernization has not reduced transport security challenges automatically; instead, it has often increased the need for protocol-aware governance and layered protection. The study has further concluded that Defense-in-Depth Theory has been highly appropriate for explaining transport-layer resilience in utility SCADA systems, because the results have shown that effective protection has not depended on one isolated control, but on the interaction of multiple defensive layers working together across physical, logical, administrative, and operational domains. In broader terms, the study has contributed to the literature by narrowing the discussion of SCADA cybersecurity to the specific issue of transport security in utility communication backbones, an area that has often received less direct empirical attention than substation automation or general industrial control security. Overall, the study has concluded that utility organizations seeking to protect mission-critical energy fiber infrastructure must treat MPLS-TP and SONET hardening as a strategic resilience issue rather than as a secondary networking concern. Stronger transport-layer security has been shown to improve not only perceived cyber protection, but also operational confidence, continuity, and the broader resilience of utility SCADA networks.

RECOMMENDATION

Based on the findings of this study, it is recommended that utility organizations adopt a more structured and transport-specific approach to securing MPLS-TP, SONET, and hybrid SCADA communication infrastructures. First, utilities should institutionalize threat modeling as a formal part of communication security governance so that critical transport assets, attack pathways, management interfaces, synchronization dependencies, and maintenance access channels can be identified and

prioritized before they become sources of operational disruption. Threat modeling should not remain a one-time assessment activity, but should be integrated into system design, maintenance review, modernization planning, and periodic security audits. Second, utility operators should strengthen protocol-aware security hardening by applying tighter access control, stronger identity governance, network segmentation between IT and OT pathways, secure configuration management, continuous monitoring, and stricter control over transport management systems. Since the study has shown that security hardening controls have had the strongest influence on resilience outcomes, utilities should prioritize these controls within budgeting, operational planning, and infrastructure renewal programs. Third, organizations should pay special attention to hybrid MPLS-TP/SONET environments, because the findings have indicated that these mixed transport settings have carried the greatest exposure and have required the strongest defensive posture. In such environments, utilities should establish dedicated governance frameworks for coexistence management, interoperability assurance, configuration consistency, and layered visibility across both legacy and modern transport segments. Fourth, utility cybersecurity teams should strengthen mitigation capacity by developing clearer incident response procedures, redundancy planning, service continuity mechanisms, and recovery playbooks tailored specifically to transport-layer events rather than relying only on generalized enterprise incident response practices. Fifth, policymakers, regulators, and infrastructure planners should recognize utility communication backbones as critical infrastructure assets in their own right and should support sector-specific standards, assessment practices, and compliance expectations for energy fiber security. Sixth, utility organizations should invest in workforce development so that engineers, operators, and security personnel can build stronger expertise in transport-specific risk assessment, cyber-physical interdependence, and protocol-aware hardening. Finally, future research and practice should move toward the development and validation of a Utility Transport Security Hardening Maturity Model that can help utilities benchmark progress in threat visibility, hardening implementation, mitigation readiness, and hybrid-transport governance over time. By following these recommendations, utility organizations can move from broad cybersecurity awareness toward more focused, layered, and operationally effective protection of the communication systems that support critical SCADA services and overall grid resilience.

LIMITATIONS OF THE STUDY

This study has had several limitations that should be considered when interpreting its findings. The first limitation has been the use of a cross-sectional research design, which has captured respondent perceptions at one point in time and has therefore limited the ability of the study to observe how security hardening, threat exposure, and resilience conditions may change as utility infrastructures evolve. Since utility communication environments are shaped by modernization efforts, operational changes, threat developments, and shifting governance practices, a single-time assessment has not fully represented the long-term dynamics of transport-layer security. The second limitation has been the reliance on self-reported questionnaire data. Although the respondents have been selected because of their professional relevance to utility SCADA and telecom security, their responses have still reflected perceptions, professional judgments, and organizational impressions rather than direct technical measurements of attack occurrence, outage frequency, or configuration-state integrity. As a result, the study has provided strong insight into how knowledgeable professionals have understood the problem, but it has not directly verified all findings through live system logs, real-time packet analysis, red-team exercises, or incident datasets. A third limitation has been related to the case-study-based and purposive sampling approach. While this strategy has improved contextual relevance, it has also limited the broad generalizability of the findings across all utility sectors, all regions, and all types of communication infrastructures. Different utility organizations may operate under different regulatory conditions, maturity levels, network architectures, and modernization timelines, which means that the pattern observed in this study may not appear identically elsewhere. A fourth limitation has been the narrow technological focus of the research. The study has concentrated on MPLS-TP, SONET, and hybrid transport environments, which has been appropriate for the research problem, but it has also meant that other relevant transport technologies and emerging utility communication models have not been examined in equal depth. A fifth limitation has been that the dependent variable has represented perceived security and resilience outcomes rather than directly measured operational performance

under attack or recovery conditions. This has made the study valuable for strategic assessment, yet less conclusive for measuring exact technical behavior in real compromise scenarios. Finally, the study has not combined its survey analysis with technical simulation or testbed validation, which could have strengthened the practical demonstration of how layered hardening performs under controlled but realistic utility attack conditions. These limitations do not invalidate the study, but they do define its scope. The research has been strongest as an empirical assessment of professional judgment, protocol-aware security priorities, and organizational perceptions of resilience in utility transport environments.

REFERENCES

[1]. Abrahamsen, F. E., Ai, Y., & Cheffena, M. (2021). Communication technologies for smart grid: A comprehensive survey. *Sensors*, *21*(23), 8087. https://doi.org/10.3390/s21238087

[2]. Aditya, D., & Mohammad Robel, M. (2022). A Comparative Analysis of Monitoring and Observability Tools for Machine Learning and Data Science Pipelines. *American Journal of Interdisciplinary Studies*, *3*(03), 99-134. https://doi.org/10.63125/707veh84

[3]. Aftab, M. A., Hussain, S. M. S., Ali, I., & Ustun, T. S. (2020). IEC 61850 based substation automation system: A survey. *International Journal of Electrical Power & Energy Systems*, *120*, 106008. https://doi.org/10.1016/j.ijepes.2020.106008

[4]. Akbarzadeh, A., Erdodi, L., Houmb, S. H., Soltvedt, T. G., & Muggerud, H. K. (2023). Attacking IEC 61850 substations by targeting the PTP protocol. *Electronics*, *12*(12), 2596. https://doi.org/10.3390/electronics12122596

[5]. Akbarzadeh, A., & Katsikas, S. (2021). Identifying and analyzing dependencies in and among complex cyber physical systems. *Sensors*, *21*(5), 1685. https://doi.org/10.3390/s21051685

[6]. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, *125*, 103028. https://doi.org/10.1016/j.cose.2022.103028

[7]. Albert, A. (2025). AI-Driven Real-Time Methane Emissions Monitoring and Predictive Leak Detection Using Lidar and IOT Sensor Fusion in Upstream Oil and Gas Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2035–2077. https://doi.org/10.63125/yavd2f86

[8]. Amena Begum, S., & Md. Nazmul, H. (2021). Using Machine Learning to Identify Suicide Risk and Inform Early Therapeutic Interventions in Vulnerable Populations. *American Journal of Advanced Technology and Engineering Solutions*, *1*(4), 43-70. https://doi.org/10.63125/jht6jb26

[9]. Amena Begum, S., & Mst Kaniz, F. (2023). Advanced Computational and Biotechnological Approaches to Systemic Family Therapy: Predicting Marital Satisfaction and Emotional Wellbeing in Couples. *Review of Applied Science and Technology*, *2*(04), 228–265. https://doi.org/10.63125/4sy9qa21

[10]. Amena Begum, S., & Mst Kaniz, F. (2024). Integrating Psychometric and Neurocognitive Biomarkers in Computational Models to Predict Cognitive Behavioral Therapy Outcomes in Adolescents with Anxiety and Depression. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 632–677. https://doi.org/10.63125/7t7wmp27

[11]. Ashraf, S., Shawon, M. H., Khalid, H. M., & Muyeen, S. M. (2021). Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways. *Sensors*, *21*(19), 6415. https://doi.org/10.3390/s21196415

[12]. Azizi, M., Benaini, R., & Ben Mamoun, M. (2013). MPLS-TP: OAM discovery mechanism. *Advanced infocomm technology*, 25–32. https://doi.org/10.1007/978-3-642-38227-7_7

[13]. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. M., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

[14]. Blair, S. M., Booth, C. D., Michielsen, J., & Joshi, N. (2016). Application of MPLS-TP for transporting power system protection data. 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm),

[15]. Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. 2008 The 28th International Conference on Distributed Computing Systems Workshops,

[16]. Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, *9*(1), 277–293. https://doi.org/10.1109/tii.2012.2198666

[17]. Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*, *19*(1), 446–464. https://doi.org/10.1109/comst.2016.2627399

[18]. Das, L., Munikoti, S., Natarajan, B., & Srinivasan, B. (2020). Measuring smart grid resilience: Methods, challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *130*, 109918. https://doi.org/10.1016/j.rser.2020.109918

[19]. 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. https://doi.org/10.1016/j.neucom.2017.10.009

[20]. Elbez, G., Ayad, A., Benmammar, B., Laouid, A., Moulahoum, S., & Mellit, A. (2021). Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in smart grids. *Sensors*, *21*(4), 1554. https://doi.org/10.3390/s21041554

[21]. Ferdous Ara, A. (2021). Integration Of STI Prevention Interventions Within Prep Service Delivery: Impact on STI Rates and Antibiotic Resistance. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 63–97. https://doi.org/10.63125/65143m72

[22]. Ferdous Ara, A., & Beatrice Onyinyechi, M. (2023). Long-Term Epidemiologic Trends of STIs PRE- and post-PrEP Introduction: A National Time-Series Analysis. *American Journal of Health and Medical Sciences*, *4*(02), 01–35. https://doi.org/10.63125/mp153d97

[23]. Ghani, N., & Park, S. (2007). Multi-tiered service survivability in next-generation SONET/SDH networks. *Photonic Network Communications*, *13*, 79–92. https://doi.org/10.1007/pl00022064

[24]. Ghosh, S., & Sampalli, S. (2019). A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access*, *7*, 135812–135853. https://doi.org/10.1109/access.2019.2926441

[25]. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

[26]. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, *7*(4), 529–539. https://doi.org/10.1109/tii.2011.2166794

[27]. Hacks, S., Katsikeas, S., Ling, E. R., Lagerström, R., & Ekstedt, M. (2020). powerLang: A probabilistic attack simulation language for the power domain. *Energy Informatics*, *3*, 34. https://doi.org/10.1186/s42162-020-00134-4

[28]. Horalek, J., & Sobeslav, V. (2023). Security baseline for substation automation systems. *Sensors*, *23*(16), 7125. https://doi.org/10.3390/s23167125

[29]. Hossain, N. U. I., Nagahi, M., Jaradat, R., Shah, C., Buchanan, R., & Hamilton, M. (2020). Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem. *Journal of Computational Design and Engineering*, *7*(3), 352–366. https://doi.org/10.1093/jcde/qwaa029

[30]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/jiot.2017.2703172

[31]. Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, *25*(7), 498–506. https://doi.org/10.1016/j.cose.2006.03.001

[32]. Ishtiaque, A., & Rajib, S. (2025). The Impact of Machine Learning on Cyber Risk Quantification in Financial Services: A Qualitative Evaluation of Threat Scoring Frameworks. *American Journal of Advanced Technology and Engineering Solutions*, *1*(02), 58-94. https://doi.org/10.63125/7aqqac69

[33]. Islam, M. D. Z., & Aditya, D. (2023). Measuring the Security Impact of Zero Trust Access Controls: A Mixed-Methods Study of Identity-Based Policies (Cisco ISE + AD) and Incident Reduction. *American Journal of Data Science and Analytics*, *4*(06), 01-42. https://doi.org/10.63125/8ycz7671

[34]. Istiaq, A., & Nusrat, J. (2022). A Panel Data Econometric Analysis on the Impact of Digital Payment Adoption on Small Business Revenue Growth in Global Business. *American Journal of Interdisciplinary Studies*, *3*(04), 500-536. https://doi.org/10.63125/ehvpjc80

[35]. Kamoun, F., & Outay, F. (2019). IP/MPLS networks with hardened pipes: Service concepts, traffic engineering and design considerations. *Journal of Ambient Intelligence and Humanized Computing*, *10*, 2577–2584. https://doi.org/10.1007/s12652-018-0734-2

[36]. Kazi Rakib Hasan, S. (2025). Quantitative Evaluation of Machine Learning Models for Project Risk Prediction and Resource Optimization in Business Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2119–2159. https://doi.org/10.63125/01bg6n62

[37]. Khalil, S. M., Bahsi, H., & Korõtko, T. (2023). Threat modeling of industrial control systems: A systematic literature review. *Computers & Security*, *135*, 103543. https://doi.org/10.1016/j.cose.2023.103543

[38]. Khodabakhsh, A., Yayilgan, S. Y., Abomhara, M., Istad, M., & Hurzuk, N. (2020). Cyber-risk identification for a digital substation. Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20),

[39]. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

[40]. Knowles, W., Such, J. M., Gouglidis, A., Misra, G., & Rashid, A. (2015). Assurance techniques for industrial control systems (ICS). Proceedings of the 1st ACM Workshop on Cyber-Physical System Security,

[41]. Kriaa, S., Pièvre-Cambacédès, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156–178. https://doi.org/10.1016/j.ress.2015.02.008

[42]. Kumar, S., Abu-Siada, A., Das, N., & Islam, S. (2023). Review of the legacy and future of IEC 61850 protocols encompassing substation automation system. *Electronics*, *12*(15), 3345. https://doi.org/10.3390/electronics12153345

[43]. Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, *67*, 74–88. https://doi.org/10.1016/j.comnet.2014.03.029

[44]. Leszczyna, R. (2018). Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection*, *22*, 70–89. https://doi.org/10.1016/j.ijcip.2018.05.006

[45]. Mahfuj Ahmed, R., & Md. Hasan Or, R. (2021). Fraud-Detection Algorithms for Identifying Anomalous Transactions in Retail Banking Networks. *American Journal of Data Science and Analytics*, *2*(12), 01-40. https://doi.org/10.63125/23m31748

[46]. Mahfuj Ahmed, R., & Md. Mehedi, H. (2023). Digital Technologies and IoT: Reshaping Financial Risk and Investment in Global Supply Chains. *Journal of Sustainable Development and Policy*, *2*(04), 297-345. https://doi.org/10.63125/nbv6ka16

[47]. Mahfuj Ahmed, R., & Rajib, S. (2022). Digital Compliance and Cybersecurity Frameworks for Strengthening Documentation Integrity Across Financial Institutions. *International Journal of Business and Economics Insights*, *2*(3), 84-122. https://doi.org/10.63125/pxzmq202

[48]. Maynard, P., McLaughlin, K., & Sezer, S. (2018). Using application layer metrics to detect advanced SCADA attacks. Proceedings of the 4th International Conference on Information Systems Security and Privacy,

[49]. Md Khaled, H., & Hisham, M. (2022). Intelligent Decision-Support Systems for Cross-Functional Workflow Optimization in Data-Driven Organizations. *Journal of Sustainable Development and Policy*, *1*(02), 168-207. https://doi.org/10.63125/dsfg3k24

[50]. Md Khaled, H., & Md. Morshedul, I. (2024). AI-Enabled Enterprise Scorecards for Reducing Operational Errors and Enhancing Supply Chain Consistency. *American Journal of Scholarly Research and Innovation*, *3*(01), 117–152. https://doi.org/10.63125/fa50dw13

[51]. Md Mehedi, H., & Md, F. (2022). Advanced Computing–Enabled Secure Financial Information Systems for Real-Time Fraud Detection in U.S. Digital Payments: A Quantitative Analysis. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 97-133. https://doi.org/10.63125/9mv2qd37

[52]. Md. Ashfaq, S., & Ashraful, I. (2025). Quantitative Analysis of Machine Learning Models For Defect Prediction in Metal Additive Manufacturing. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1810–1847. https://doi.org/10.63125/3fkkwg05

[53]. Md. Hasan Or, R., Tanjina Binte, S., & Rajib, S. (2023). Performance Analytics Frameworks for Digital Marketing and Service Enterprises: An empirical Study. *American Journal of Data Science and Analytics*, *4*(03), 01-35. https://doi.org/10.63125/aq7y1792

[54]. Md. Mainuddin, F., & Palash Chandra, D. (2022). Fabrication-Driven Structural Optimization Techniques for Cost-Efficient Steel Construction Using CNC-Based Design Workflows. *American Journal of Interdisciplinary Studies*, *3*(04), 464-499. https://doi.org/10.63125/n08g1x15

[55]. Md. Mainuddin, F., & Palash Chandra, D. (2023). Advanced Computing–Based Modeling of Steel Connection Behavior and Stability Performance using ETABS And STAAD Pro. *American Journal of Advanced Technology and Engineering Solutions*, *3*(04), 42-86. https://doi.org/10.63125/xfkzrg56

[56]. Md. Mehedi, H., & Khairum Nahar, P. (2023). A Systematic Review of Secure Health Data Information Systems for Pandemic Preparedness and Economic Continuity in the United States. *Review of Applied Science and Technology*, *2*(01), 227–258. https://doi.org/10.63125/77h2m531

[57]. Md. Mehedi, H., & Khairum Nahar, P. (2024). Advanced Computing and AI-Driven National Information Systems for Predictive Disaster Risk Management and Economic Loss Mitigation. *American Journal of Scholarly Research and Innovation*, *3*(02), 296–336. https://doi.org/10.63125/4sbz5j45

[58]. Md. Morshedul, I., Rukaiya Khatun, M., & Khairum Nahar, P. (2022). Machine Learning–Driven Forecasting Pipelines for Financial Volatility Detection in Integrated Enterprise ERP Environments. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 134-173. https://doi.org/10.63125/y42nk811

[59]. Md. Nazmul, H., & Amena Begum, S. (2022). AI-Based Psychodiagnostics' Models to Support Early Intervention and Reduce Suicide Risk in Adolescents and Youth: Development and Clinical Validation. *American Journal of Data Science and Analytics*, *3*(06), 40-79. https://doi.org/10.63125/vb5f7e98

[60]. Md. Shahinur, I., & Md. Sultan, M. (2022). Digital-Twin-Based Quantitative Frameworks for Modeling, Monitoring, and Optimization of Electrical Power Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 365-393. https://doi.org/10.63125/dvmj1y93

[61]. Md. Towhidul, I., & Uddin, M. D. S. (2024). Simulation-Based Forecasting and Inventory Control Models For Consumer Goods Networks: A Quantitative Study Using Monte Carlo Simulation and Time-Series Methods. *Review of Applied Science and Technology*, *3*(04), 165–197. https://doi.org/10.63125/a3047d06

[62]. Mohammad Robel, M. (2025). Advanced Computing Frameworks for Distributed Training, Deployment, and Monitoring of Artificial Intelligence and Machine Learning Models. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1922–1957. https://doi.org/10.63125/rxb2cb66

[63]. Mohammad Robel, M., & Md. Morshedul, I. (2021). Foundational Approaches to Secure Data Collection and Processing in Networked and Distributed Computing Environments. *International Journal of Business and Economics Insights*, *1*(4), 32–69. https://doi.org/10.63125/thrtkw71

[64]. Mohammad Robel, M., & Md. Morshedul, I. (2024). Data Preprocessing and Feature Engineering Strategies for Large-Scale Predictive Modeling Applications. *Review of Applied Science and Technology*, *3*(01), 263–302. https://doi.org/10.63125/tqqqed47

[65]. Moreira, N., Molina, E., Lázaro, J., Jacob, E., & Astarloa, A. (2016). Cyber-security in substation automation systems. *Renewable and Sustainable Energy Reviews*, *54*, 1552–1562. https://doi.org/10.1016/j.rser.2015.10.124

[66]. Mostafa, K. (2023). An Empirical Evaluation of Machine Learning Techniques for Financial Fraud Detection in Transaction-Level Data. *American Journal of Interdisciplinary Studies*, *4*(04), 210-249. https://doi.org/10.63125/60amyk26

[67]. Murad, M. D. H. R. (2025). Machine Learning–Based Consumer Behavior Prediction Models for E-Commerce Platforms: Enhancing Digital Financial Inclusion and Market Accessibility. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2078–2118. https://doi.org/10.63125/pnz32s94

[68]. Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

[69]. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, *31*(4), 418–436. https://doi.org/10.1016/j.cose.2012.02.009

[70]. Palash Chandra, D. (2023). Machine Learning–Driven Optimization of Water Distribution Networks: Demand Forecasting, and Energy Efficiency Analysis. *Journal of Sustainable Development and Policy*, *2*(04), 257-296. https://doi.org/10.63125/jdxq0819

[71]. Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R., & Misurec, J. (2021). Application perspective on cybersecurity testbed for industrial control systems. *Sensors*, *21*(23), 8119. https://doi.org/10.3390/s21238119

[72]. Rajib, S. (2024). Quantitative Assessment of Data-Driven Pricing Optimization Strategies for E-Commerce Platforms in Developing Economies. *Review of Applied Science and Technology*, *3*(02), 01–40. https://doi.org/10.63125/g5va6e03

[73]. Rukaiya Khatun, M., & Zakia, A. (2023). Quantitative Assessment of Data Privacy and Access Control Effectiveness in SAP/ERP Analytics Systems. *Review of Applied Science and Technology*, *2*(01), 259–300. https://doi.org/10.63125/vb03b363

[74]. Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224. https://doi.org/10.1109/jproc.2011.2165269

[75]. Tanjina Binte, S., & Md. Hasan Or, R. (2022). Advanced Computing, IT Strategy, and Network-Optimized Frameworks for Retail Business Intelligence. *American Journal of Interdisciplinary Studies*, *3*(04), 429-463. https://doi.org/10.63125/dgyg3762

[76]. Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, *10*(8), 76. https://doi.org/10.3390/fi10080076

[77]. Ten, C.-W., Manimaran, G., & Liu, C.-C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, *40*(4), 853–865. https://doi.org/10.1109/tsmca.2010.2048028

[78]. Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371. https://doi.org/10.1016/j.comnet.2012.12.017

[79]. Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, *14*(4), 998–1010. https://doi.org/10.1109/surv.2012.010912.00035

[80]. Zakia, A., & Rukaiya Khatun, M. (2024). Quantitative Assessment of CRM-Based Business Intelligence on Customer Satisfaction and Retention: Evidence from Multi-Channel Service Operations. *Journal of Sustainable Development and Policy*, *3*(02), 01-42. https://doi.org/10.63125/hjd22x72

[81]. Zhu, K., Zhang, J., & Mukherjee, B. (2005). Ethernet-over-SONET (EoS) over WDM in optical wide-area networks (WANs): Benefits and challenges. *Photonic Network Communications*, *10*(1), 107–118. https://doi.org/10.1007/s11107-005-1698-7