American Journal of Advanced Technology and Engineering Solutions

**Volume:** 6; **Issue:** 1
**Pages:** 416-459
**eISSN: 3067-5146**

# Securing SCADA Communications Over OPGW And ADSS Fiber In U.S. Bulk Electric Systems: A NERC CIP-Aligned Engineering Framework

**Abu Naser Md Golam Mosharraf[1];**

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

*Doi: 10.63125/hn42nw39*
***Received:*** *10 December 2025;* ***Revised:*** *12 January 2026;* ***Accepted:*** *12 February 2026;* ***Published:*** *23 March 2026*

**Abstract**

*This study addresses the growing problem of securing SCADA communications transmitted over Optical Ground Wire and All-Dielectric Self-Supporting fiber in U.S. Bulk Electric Systems, where technically robust fiber links still remain exposed to cyber, physical, and operational vulnerabilities that can affect visibility, command integrity, and system resilience. The purpose of the research was to develop and empirically test a NERC CIP-aligned engineering framework for improving SCADA communication security and resilience by examining the influence of Engineering Security Controls, Communication Path Protection, Access Control Measures, Monitoring and Detection Capability, and NERC CIP Alignment on SCADA Communication Security and Resilience. The study adopted a quantitative, cross-sectional, case-based design and collected data from 220 valid professional responses drawn from cloud-connected and enterprise utility operational cases after screening 250 distributed questionnaires, yielding an 88.0% usable response rate. Respondents represented SCADA and OT engineers, utility communication engineers, cybersecurity professionals, protection and control engineers, substation automation specialists, and compliance personnel. Analysis was conducted using descriptive statistics, Cronbach's alpha, correlation, and multiple regression in SPSS. The findings showed a strong overall security posture, with SCADA Communication Security and Resilience recording a mean of 4.08, Engineering Security Controls 4.21, Monitoring and Detection Capability 4.18, Communication Path Protection 4.11, Access Control Measures 4.05, and NERC CIP Alignment 3.97. Reliability was strong across all constructs, with Cronbach's alpha values ranging from 0.81 to 0.89 and an overall instrument reliability of 0.87. Correlation results indicated significant positive relationships between SCADA Communication Security and Resilience and Monitoring and Detection Capability ($r = 0.74$), Engineering Security Controls ($r = 0.71$), NERC CIP Alignment ($r = 0.68$), Communication Path Protection ($r = 0.66$), and Access Control Measures ($r = 0.62$), all at $p < .001$. Regression analysis confirmed that the model was statistically significant, $F(5,214) = 52.84$, $p < .001$, explaining 55.2% of the variance ($R^2 = 0.552$), with Monitoring and Detection Capability emerging as the strongest predictor ($\beta = 0.29$). The study also found that ADSS environments were perceived as more vulnerable than OPGW environments, with mean vulnerability scores of 3.88 and 3.54 respectively, implying the need for medium-specific protective strategies and stronger integration of engineering, monitoring, and compliance functions in critical utility communication security.*

**Keywords**

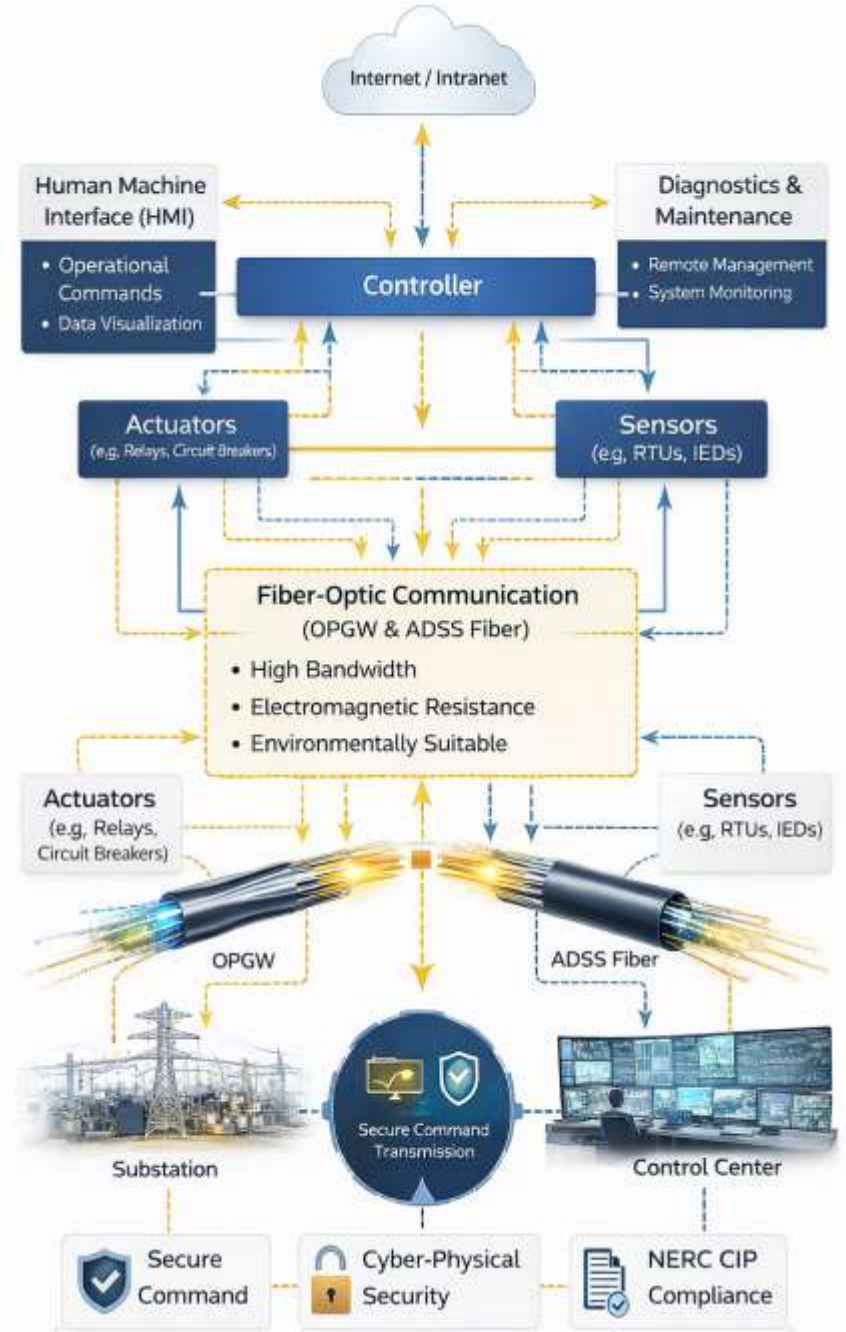
*SCADA security; OPGW; ADSS fiber; NERC CIP; bulk electric systems;*

## INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are industrial control architectures designed to gather measurements from geographically distributed field devices, transmit operational information to centralized control centers, and support supervisory commands for real-time management of critical infrastructure. In electric power systems, SCADA functions are embedded within a wider cyber-physical environment that connects remote terminal units, intelligent electronic devices, protection relays, substations, communication links, and energy management platforms into an integrated operational structure (Alanazi et al., 2023; Boev et al., 2023). The international significance of SCADA security stems from the central role of electric power in economic activity, public safety, industrial continuity, healthcare operations, and digital service delivery. As utilities rely increasingly on interconnected supervisory infrastructures, communication reliability and communication security become inseparable from system stability and operational trust (Alsuwian et al., 2022). Early scholarship on power-system cybersecurity established that SCADA vulnerabilities were not limited to software defects alone, but also emerged from structural exposures associated with open communication paths, weak protocol protections, and the convergence of operational technology with enterprise connectivity. As smart grid development accelerated, researchers showed that modernization depended heavily on two-way communication, distributed sensing, and interoperable networking, all of which elevated the strategic importance of communications infrastructure in electricity operations (Deng et al., 2017). Later studies conceptualized electric grids as cyber-physical systems in which failures in communication availability, integrity, confidentiality, or authentication could generate operational disturbance, reduced situational awareness, or control inaccuracies. Reviews of smart-grid cybersecurity further documented that communication-channel protection had become a major international technical concern because electric infrastructures were increasingly digitized across nations and utility settings. Wider industrial control scholarship reinforced this point by demonstrating that SCADA and other industrial control systems now function in communication-intensive environments where the channel itself forms part of the security boundary rather than acting as a neutral transport layer (Hasan et al., 2023). For a study focused on SCADA over Optical Ground Wire (OPGW) and All-Dielectric Self-Supporting (ADSS) fiber in U.S. Bulk Electric Systems, these definitions establish that secure communication is not a secondary matter but a foundational requirement for trustworthy supervisory control in critical power infrastructure (Bhamare et al., 2020). The communication architecture of electric power systems provides the structural context for understanding why SCADA security should be examined through the physical and logical properties of its transport media. Surveys on smart-grid communications have shown that modern utility networks depend on layered architectures that connect substations, control centers, protective equipment, wide-area monitoring devices, and field automation components through heterogeneous communication media selected according to latency, reliability, bandwidth, electromagnetic compatibility, and geographic reach. In this architecture, SCADA communication is not confined to telemetry transmission; it also supports supervisory command traffic, event reporting, alarm notification, status polling, and control coordination among geographically dispersed grid assets (Alladi et al., 2020). Research on smart-grid security emphasized that secure networking required coordinated attention to identity management, cryptography, access control, and resilient communication design because every layer of the communications stack could shape operational exposure. Related research also described the electric grid as a cyber-physical infrastructure whose state awareness depends on correct, timely, and trustworthy communication across sensing and control domains. Reviews centered on smart-grid cybersecurity further stressed that communication channels are indispensable to preserving grid observability and controllability, because even technically robust field devices can become operational liabilities when their data paths are manipulated, delayed, interrupted, or spoofed (Cheminod et al., 2013). This body of literature gives special weight to communication-medium selection because engineering decisions shape exposure patterns. Fiber-based utility communications are widely valued for electromagnetic resistance, bandwidth capacity, and operational suitability in transmission environments, making them central to electric utility networking. At the same time, the security implications of a fiber route cannot be separated from its installation environment, maintenance access patterns, induced electrical conditions, and interface

points with field and control equipment. For this reason, SCADA over OPGW and ADSS fiber should be approached as a communication-security problem located at the intersection of networking, power engineering, and operational governance rather than as a generic information-security issue. The international literature on smart-grid communications therefore offers the proper starting point for examining how medium-specific infrastructure characteristics shape secure supervisory control in bulk electric operations (Chen et al., 2023).

**Figure 1: NERC CIP-Aligned SCADA Communication Framework over OPGW and ADSS Fiber**




The literature on industrial control systems and SCADA security demonstrates that the communication environment of critical infrastructure has become a major site of vulnerability because operational protocols, remote access arrangements, and network interdependencies create pathways for intrusion, disruption, and unauthorized influence over process control. A review of industrial network security showed that industrial communications often carry legacy assumptions, limited built-in protections, and operational constraints that complicate the direct application of standard enterprise-security

controls. Cybersecurity management research in industrial control systems expanded this discussion by showing that risk measurement, governance structures, and control selection in operational environments require methods specifically tailored to availability-sensitive systems. SCADA-centered syntheses then mapped a broad range of attack surfaces present in supervisory environments, including protocol weaknesses, inadequate segmentation, insecure remote engineering access, weak authentication, limited monitoring, and insufficient modeling of attack consequences (Ara, 2021; Metke & Ekl, 2010). A broader cyber-physical systems security perspective showed that attacks on control-oriented environments exploit the close linkage between computation, communication, and physical processes (Begum & Nazmul, 2021). Power-grid-focused reviews consistently reported that these vulnerabilities become more serious when communication networks grow more interconnected and when operational technology inherits exposure from corporate or internet-facing systems (Ahmed & Hasan Or, 2021; Robel & Morshedul, 2021). One of the most detailed SCADA surveys synthesized secure protocols, major incidents, threat tactics, and defensive practices, highlighting that communication assurance is decisive in maintaining trust during abnormal operating conditions. Other research on industrial control systems and industrial internet environments emphasized recurring attack patterns in which adversaries target communication weaknesses, authentication failures, insecure integration, and low-visibility segments (Aditya & Robel, 2022; Istiaq & Nusrat, 2022; Mo et al., 2012). More recent reviews have confirmed the persistence of these issues in smart-grid and SCADA infrastructures, demonstrating that vulnerability is not isolated to a single device class or software layer, but arises across architecture, routing, access control, and protocol behavior (Ahmed & Rajib, 2022; Khaled & Hisham, 2022). Within this literature, communication security stands out as a decisive factor because the supervisory system relies on uninterrupted and trusted exchanges between remote field assets and the central operating authority (Giani et al., 2011; Mehedi & Md, 2022; Mainuddin & Chandra, 2022).

Electric-power cybersecurity research has also shown that communication insecurity is not only a matter of unauthorized access but a direct source of cyber-physical distortion in grid operation. An important strand of this scholarship investigates attacks on measurement integrity, state estimation, and control visibility, illustrating how communication compromise can alter operator perception of system conditions (Morshedul et al., 2022; Nazmul & Begum, 2022). Research on false data injection attacks against state estimation demonstrated that carefully designed malicious data could evade traditional bad-data detection and mislead power-system operation. Related work on smart-grid data-integrity attacks characterized how compromise along communication paths could produce operationally meaningful deception (Gao et al., 2012; Shahinur & Sultan, 2022; Binte & Hasan Or, 2022). Cyber-physical security research for smart-grid infrastructure located these threats within a broader framework, arguing that attacks against communication components could propagate into physical consequences through control dependence and real-time coordination. Similar work on cyber-physical system security for the electric power grid emphasized that grid protection required models integrating both cyber and physical perspectives, because control reliability depends on accurate observation, dependable signaling, and coherent system response (Begum & Kaniz, 2023; Dhirani et al., 2021; Ara & Onyinyechi, 2023). A later survey on false data injection in state estimation synthesized attacks, impacts, and defenses and reaffirmed the central role of communication integrity in maintaining situational awareness. Reviews on power-grid cybersecurity documented that resilience in grid operations depends on protecting communication infrastructures from coordinated attacks, unauthorized manipulation, and monitoring blind spots (Nazir et al., 2017). More recent smart-grid studies have continued to interpret communication compromise as a systemic issue linked to architecture, attack taxonomy, standards, and control design rather than as an isolated irregularity. This literature is directly relevant to SCADA over utility fiber because fiber networks are often assumed to offer robust transport by virtue of bandwidth and environmental suitability. The scholarship shows that secure transport cannot be inferred from medium performance alone. A communication pathway may be technically efficient and still become the route through which deception, interruption, replay, route compromise, or unauthorized influence alters the information basis of grid control (Pliatsios et al., 2020). For a NERC CIP-aligned engineering study, this understanding is essential because it places communication trustworthiness at the center of security, reliability, and supervisory accuracy in bulk

electric systems.

The technical relevance of OPGW and ADSS fiber arises from their specialized roles in utility communications and from the fact that their engineering environments shape distinct security and reliability conditions. OPGW integrates optical fibers within the ground wire of transmission infrastructure, thereby combining shielding and communications functions in a single asset aligned with high-voltage line routes (Sridhar et al., 2012). ADSS, in contrast, is a nonmetallic self-supporting optical cable designed for aerial deployment without metallic components, making it especially suitable in environments where dielectric construction and installation flexibility are important. In utility communication practice, both media support the transmission of operational data, protective signaling, and supervisory traffic, and both are deeply connected to substation-to-control-center communications. Communication studies in smart-grid systems have already explained why fiber occupies a privileged place in utility networking: it offers high capacity, stable long-distance transport, and a strong fit for critical infrastructure communication requirements (Islam & Aditya, 2023; Ahmed & Mehedi, 2023; Sun et al., 2018). At the same time, the engineering literature indicates that the two media are not interchangeable from the standpoint of environmental and operational exposure. Research on OPGW communication technology under interference conditions in distribution-network environments highlighted that communication performance is inseparable from the electrical context through which the line is routed. Related work analyzing induced current in OPGW on high-voltage transmission lines drew attention to the operational realities associated with line-coupled installations. For ADSS, research on tracking-resistance performance addressed issues directly related to the material endurance and environmental exposure of dielectric cable deployed on energized line structures (Knowles et al., 2015; Hasan Or et al., 2023; Mainuddin & Chandra, 2023). When viewed through the lens of SCADA security, the significance of medium-specific study becomes clear. OPGW and ADSS do not merely carry digital traffic; they are deployed in distinct physical contexts that shape accessibility, inspection practices, fault localization, maintenance constraints, and the practical management of communication incidents (Mehedi & Nahar, 2023; Mostafa, 2023). A study of SCADA security over OPGW and ADSS therefore requires more than a generic account of fiber communication. It requires attention to the infrastructure logic of each medium and to the way physical installation conditions intersect with supervisory communication assurance in utility operations. This is one reason the present research topic naturally occupies the intersection of communication engineering, power-system operation, and cybersecurity governance (Liu et al., 2011; Chandra, 2023; Khatun & Zakia, 2023).

Security governance and control architecture form another major branch of the literature relevant to SCADA communication over utility fiber. Studies across industrial control and smart-grid domains consistently support layered protection, monitored access, segmentation, authentication discipline, and operationally grounded risk management as key foundations of trustworthy control communication. Early work on cybersecurity vulnerability assessment in SCADA systems directly addressed power-system security concerns and established the need for structured evaluation of communication and control exposures (Begum & Kaniz, 2024; Khaled & Morshedul, 2024). Research on smart-grid network security framed protection through technological controls that connect communication safeguards with overall system architecture, while broader smart-grid security surveys documented the complexity of securing interconnected environments where communication channels connect diverse devices and operational domains (Humayed et al., 2017; Mehedi & Nahar, 2024; Towhidul & Uddin, 2024). Cybersecurity management research in industrial control systems treated protection as a governance challenge as much as a technical one, which is especially relevant to utility environments where policy, monitoring, engineering configuration, and operational discipline are tightly linked. SCADA security surveys reinforced this position by showing that protocol security, incident learning, threat modeling, and tactical defense all require a coherent security architecture rather than isolated controls. Broader industrial control and industrial internet research also connected effective protection with standards-aware control selection, system visibility, and environment-specific countermeasures (Robel & Morshedul, 2024; Rajib, 2024). Smart-grid studies from 2022 and 2023 continued to classify effective defenses in terms of layered mitigation, architectural hardening, attack-aware monitoring, and standards-guided cyber protection. This literature supports the logic of examining SCADA communications in U.S. Bulk Electric Systems through a NERC CIP-aligned engineering framework.

The importance lies not only in compliance itself, but in the fact that compliance-oriented domains such as access control, electronic security perimeters, incident response, recovery planning, and configuration discipline correspond closely to established research themes in operational communication security. In a bulk electric context, a NERC CIP-aligned study of OPGW and ADSS communications therefore belongs to a strong scholarly tradition that links security architecture, communication assurance, and operational governance within a single analytical field (Khalifa et al., 2018).

A final synthesis of the literature shows that the present study occupies a clear and necessary position within power-system cybersecurity research. Existing scholarship has already produced substantial surveys of smart-grid architectures, industrial control vulnerabilities, SCADA protocols, cyber-physical attacks, and defensive strategies (Albert, 2025; Li et al., 2023; Zakia & Khatun, 2024). It has also generated strong analysis of data-integrity attacks, communication-network risk, and layered defense within electric grids (Gündüz & Das, 2020; Ishtiaque & Rajib, 2025; Hasan, 2025). At the same time, medium-specific utility communication studies on OPGW and ADSS tend to focus on engineering performance, installation environment, electrical interference, or material endurance rather than on the integrated security posture of SCADA traffic transported across those media. This creates a meaningful gap between communication-medium engineering and supervisory cybersecurity analysis (El Mrabet et al., 2018; Ashfaq & Ashraful, 2025; Murad, 2025). The gap becomes even more important in the context of U.S. Bulk Electric Systems, where the operational seriousness of communication assurance is elevated by the scale, criticality, and governance expectations associated with bulk electric operations. A NERC CIP-aligned engineering framework is therefore an analytically coherent basis for studying this topic because it connects medium-specific infrastructure realities with the layered security concerns already established in the literature. Such a framework supports investigation into how communication path protection, access discipline, monitoring capability, engineering controls, and resilience practices relate to one another within SCADA environments that depend on OPGW and ADSS fiber. The value of the present study lies in that integration (Khaled, 2026; Robel, 2025; Ten et al., 2008; Wang & Lu, 2013). Rather than treating SCADA security, utility fiber engineering, and compliance architecture as separate discussions, this research positions them within one quantitative, case-based examination of secure supervisory communication in bulk electric systems (Wang et al., 2011). The literature from 2005 to 2023 provides a mature foundation for this direction by documenting the strategic importance of SCADA, the communication intensity of modern grids, the cyber-physical consequences of insecure signaling, the operational complexity of industrial control security, and the technical specificity of utility fiber infrastructure.

**Background of the Study**

The background of this study is rooted in the growing dependence of modern electric power systems on secure, continuous, and high-speed communication infrastructures for real-time operational control. In U.S. Bulk Electric Systems, Supervisory Control and Data Acquisition (SCADA) platforms serve as the core supervisory layer through which utilities monitor grid conditions, collect telemetry from substations and field devices, issue remote commands, manage alarms, and maintain system visibility across geographically dispersed assets. As the electric grid has become more automated, interconnected, and data-driven, the communications layer supporting SCADA has become just as critical as the physical power infrastructure itself. Fiber-optic technologies such as Optical Ground Wire (OPGW) and All-Dielectric Self-Supporting (ADSS) cable are widely used in utility networks because they provide high bandwidth, low latency, electromagnetic resistance, and reliable long-distance communication pathways suitable for transmission and substation environments. Their role in carrying SCADA traffic, protective signaling, and operational data means that they are central to the stability, responsiveness, and resilience of utility operations. At the same time, the increasing digitization of grid operations has expanded the range of cyber, physical, and operational risks that can affect communication trustworthiness. A secure communication channel is no longer understood only as a technical convenience; it is a strategic requirement for maintaining grid awareness, command integrity, and coordinated control. In this setting, vulnerabilities associated with communication path protection, unauthorized access, configuration weaknesses, monitoring limitations, maintenance exposure, and incident response preparedness can directly affect the ability of utilities to operate safely and reliably.

The background of this study is also shaped by the regulatory importance of securing critical electric infrastructure in accordance with recognized standards and governance expectations, particularly in environments where communication compromise could influence reliability outcomes. Because OPGW and ADSS are deployed in different physical and engineering contexts, they present distinct exposure patterns that deserve focused study rather than generic treatment under broad discussions of network security. This creates the need for a research framework that brings together SCADA communications, utility fiber infrastructure, engineering protection practices, and security governance within one coherent investigation. The present study therefore emerges from the practical and academic need to understand how SCADA communications over OPGW and ADSS fiber can be secured in U.S. Bulk Electric Systems through a structured, NERC CIP-aligned engineering perspective.

**Problem Statement**

The problem addressed in this study arises from the increasing dependence of U.S. Bulk Electric Systems on SCADA-based communication infrastructures for real-time monitoring, supervisory control, alarm management, and operational coordination, while the security of the communication paths supporting these functions remains unevenly understood and insufficiently examined in a medium-specific way. Utilities rely heavily on fiber-optic channels such as Optical Ground Wire (OPGW) and All-Dielectric Self-Supporting (ADSS) cable to carry SCADA traffic between substations, control centers, and field devices because these media provide the speed, bandwidth, and environmental suitability required for modern grid operations. Even so, the security posture of SCADA communications cannot be assumed simply because fiber infrastructure is technically robust. Communication systems operating over OPGW and ADSS are still exposed to a range of cyber, physical, and operational vulnerabilities linked to access pathways, configuration weaknesses, monitoring gaps, maintenance activities, environmental exposure, route dependency, and inadequate coordination between engineering design and cybersecurity governance. A further problem is that existing discussions of SCADA security often remain broad and generalized, focusing on industrial control systems as a whole without sufficiently isolating the specific engineering and operational realities of OPGW- and ADSS-based communication environments in bulk electric infrastructure. This creates a knowledge gap in understanding how communication-medium characteristics interact with security controls, resilience measures, and compliance practices. The issue is made more serious by the highly regulated and high-consequence nature of bulk electric operations, where compromised supervisory communications can affect visibility, command integrity, response timing, and system reliability. There is also a practical challenge in that engineering teams, operations personnel, and compliance professionals may address communication security from different viewpoints, resulting in fragmented protection efforts rather than a unified control framework. As a result, utilities may implement controls without clear evidence of which engineering and governance measures contribute most strongly to secure and resilient SCADA communications. This study therefore addresses the core problem that SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems require a more clearly defined, quantitatively examined, and NERC CIP-aligned engineering framework capable of identifying key risk factors, evaluating protective measures, and supporting stronger communication security outcomes.

**Objective of the Study**

The objective of this study is to examine, in a structured and measurable way, the factors that shape the security and resilience of SCADA communications transmitted over OPGW and ADSS fiber in U.S. Bulk Electric Systems and to use that understanding as the basis for a NERC CIP-aligned engineering framework. More specifically, the study seeks to identify the major engineering, cyber, and operational issues that influence the trustworthiness of supervisory communications in utility environments where real-time data exchange is essential to safe and reliable grid operation. It aims to assess how communication path protection, access control, monitoring capability, configuration discipline, and incident-response readiness are associated with the overall security posture of SCADA communication systems. Another major objective is to determine whether NERC CIP-aligned compliance practices are meaningfully related to communication resilience and whether such practices strengthen the ability of utilities to preserve visibility, command integrity, and operational continuity across fiber-based supervisory networks. The study also seeks to compare exposure patterns between OPGW and ADSS

environments so that the security discussion reflects the actual infrastructure conditions under which supervisory traffic is carried, rather than treating all fiber communications as identical. Through a quantitative, cross-sectional, case-study-based approach using Likert-scale responses and statistical analysis, the research intends to measure the direction and strength of relationships among the principal variables and to identify which factors significantly predict secure SCADA communication outcomes. In doing so, the study is designed not only to describe prevailing security conditions but also to explain how technical and governance-oriented controls function together within bulk electric communication systems. The final objective is to synthesize these findings into an engineering framework that aligns communication security practice with the operational realities of U.S. electric utilities and the regulatory logic of NERC CIP. In this way, the study aims to provide an evidence-based structure for improving supervisory communication protection, strengthening resilience, and supporting more coherent decision-making across engineering, cybersecurity, and compliance functions in critical power infrastructure.

**Research Hypotheses**

The research hypotheses of this study are developed to test the expected relationships between key engineering and governance variables and the overall security and resilience of SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems. The central assumption of the study is that secure supervisory communication is not shaped by a single protective measure, but by the combined influence of communication-path safeguards, access discipline, monitoring capability, compliance alignment, and resilience-oriented operational practices. On that basis, the study hypothesizes that engineering security controls have a statistically significant positive effect on the protection of SCADA communications, because well-designed communication architectures, hardened interfaces, and structured protection measures are likely to reduce exposure to disruption and unauthorized influence. It is also hypothesized that NERC CIP-aligned compliance practices have a significant positive relationship with SCADA communication resilience, reflecting the idea that regulated security discipline supports more reliable and defensible operational communication environments. A third hypothesis proposes that monitoring capability and intrusion detection significantly improve communication security outcomes by increasing visibility into abnormal behavior and reducing the time required to identify and respond to security events. A fourth hypothesis states that communication-path protection and access control measures significantly reduce the security exposure associated with OPGW- and ADSS-based SCADA systems, since control over interfaces, routes, permissions, and maintenance access is expected to influence communication trustworthiness. A fifth hypothesis proposes that the combined effect of engineering controls, compliance alignment, and resilience practices significantly predicts the overall security of SCADA communications in bulk electric operations. These hypotheses are important because they transform the study from a descriptive assessment into an explanatory investigation capable of testing whether the assumed drivers of secure supervisory communication are supported by empirical evidence. They also provide a direct bridge between the study objectives and the statistical methods used in the analysis, making it possible to examine both individual and combined effects of the independent variables on the dependent outcome. In this way, the hypotheses serve as the analytical foundation for evaluating how technical, operational, and compliance-oriented measures interact within a NERC CIP-aligned engineering framework for SCADA communications.

**Significance of the Research**

The significance of this research can be understood from several interrelated perspectives that reflect its academic, technical, operational, and regulatory value.

**(i)** This study is significant because it addresses a highly specialized but critically important area of electric power infrastructure security by focusing specifically on SCADA communications carried over OPGW and ADSS fiber in U.S. Bulk Electric Systems. Many discussions of SCADA security remain broad, while this research directs attention to the actual communication media that support supervisory control in utility environments.

**(ii)** The study is significant from an academic standpoint because it contributes to the literature by linking utility fiber infrastructure, communication security, and compliance-oriented engineering within one analytical framework. This helps expand existing knowledge beyond general industrial

control system security and toward a more medium-specific understanding of supervisory communication protection.

**(iii)** The research is significant for utility engineers and communication planners because it highlights the importance of treating OPGW and ADSS as distinct operational environments with different exposure patterns. This can support more informed engineering decisions concerning communication design, route protection, equipment hardening, and maintenance coordination.

**(iv)** The study is significant for cybersecurity practitioners because it examines how access control, monitoring, intrusion awareness, and communication-path safeguards contribute to the trustworthiness of SCADA communications. This provides a clearer basis for aligning technical protection measures with operational requirements in bulk electric settings.

**(v)** The research is significant for compliance and governance functions because it is structured around a NERC CIP-aligned perspective. By connecting empirical analysis with compliance-related control domains, the study offers a more practical foundation for understanding how governance expectations can support stronger communication resilience and security discipline.

**(vi)** This study is significant for decision-makers in the electric utility sector because it provides quantitative evidence on the factors that influence secure supervisory communication outcomes. Such evidence can improve prioritization of investments, strengthen risk-based planning, and support more coherent coordination among engineering, operations, and compliance teams.

**(vii)** The study is also significant because it proposes an engineering framework that can serve as a practical reference point for organizations seeking to strengthen SCADA communication security in high-consequence environments. In this way, the research contributes not only to scholarship but also to operational reliability, infrastructure protection, and the broader goal of safeguarding critical electric systems.

## LITERATURE REVIEW

The literature review for this study is grounded in the understanding that SCADA communication security in U.S. Bulk Electric Systems must be examined as a combined problem of power-system operation, communication engineering, cybersecurity control, and regulatory alignment. SCADA systems form the supervisory backbone of utility operations by enabling real-time data acquisition, remote monitoring, alarm handling, and command execution across geographically dispersed assets, which means that the communication layer supporting these functions is inseparable from system reliability and operational trust. In modern electric networks, this communication layer increasingly depends on high-capacity fiber-optic infrastructures such as OPGW and ADSS, both of which are widely used for carrying supervisory traffic, operational signaling, and control-related information between substations, field devices, and control centers. The literature therefore becomes important not only for defining SCADA and its communication architecture, but also for showing how the expansion of digital grid operations has increased attention to communication integrity, access control, resilience, and vulnerability management. Existing scholarship on industrial control systems, smart grids, and cyber-physical infrastructure has shown that communication channels are no longer passive transport paths; they are active components of the security boundary because the accuracy, timing, and reliability of supervisory data exchange directly affect grid awareness and control quality. At the same time, research on utility communication systems indicates that OPGW and ADSS operate under different engineering conditions, which means their security implications cannot be fully captured through generic discussions of fiber communication. The literature is also essential for situating this study within the larger body of work on layered security, infrastructure protection, and standards-guided control environments, especially where the operational seriousness of communication compromise is elevated by the scale and consequence profile of bulk electric operations. In this context, reviewing prior studies helps identify what is already known about SCADA vulnerabilities, communication threats, network protection strategies, utility fiber deployment contexts, and governance-oriented security measures, while also clarifying the gap that this study intends to address. The purpose of this literature review is therefore to build the intellectual foundation for the research by examining the technical, theoretical, and conceptual strands most relevant to securing SCADA communications over OPGW and ADSS fiber through a NERC CIP-aligned engineering framework.

### SCADA Communication Architecture in U.S. Bulk Electric Systems

SCADA communication architecture in U.S. Bulk Electric Systems is best understood as a layered operational structure that connects control centers, substations, intelligent electronic devices, remote terminal units, protective relays, and field sensors through standardized communication pathways designed to support real-time monitoring and supervisory control. Within this architecture, data acquisition and command exchange are organized around the need for fast, deterministic, and interoperable communication across geographically dispersed assets that must remain synchronized under normal and disturbed operating conditions. The communication layer therefore functions as a strategic operational fabric rather than a simple transport mechanism, because it enables status visibility, command execution, event notification, alarm transfer, and coordinated system response across transmission-scale infrastructure. In practical terms, this architecture combines station-level communication, bay-level communication, and process-level information exchange with control-center integration so that operators can maintain situational awareness over large and complex networks. The increasing adoption of digital substations has further strengthened the importance of communication architecture by shifting power-system automation away from heavily hardwired arrangements toward data-centric, Ethernet-enabled, and standards-based designs. In this environment, architecture quality is measured not only by connectivity and bandwidth, but also by interoperability, timing precision, data modeling consistency, and the ability to support protection and control applications without degrading reliability. Research on IEC 61850-based substation automation has shown that communication architecture in power utility automation now relies on object-oriented data models, abstract communication services, and structured engineering processes that make information exchange more scalable and semantically consistent across devices and vendors (Aftab et al., 2020). This is especially relevant for bulk electric operations because supervisory communication must move across multiple organizational and physical boundaries while still preserving message integrity, operational context, and timing discipline. As a result, the study of SCADA communication architecture in bulk electric environments must begin with the recognition that grid control depends on a tightly organized interaction between physical infrastructure, digital communications, and automation standards.

**Figure 2: Scada Communication Framework For Digital Substations And Smart Grid Integration**


A second defining feature of SCADA communication architecture in bulk electric settings is the central role of network standardization and protocol structuring in making large-scale interoperability feasible. Modern supervisory systems are expected to connect equipment from different vendors, support mixed generations of field devices, and carry multiple traffic classes, including telemetry, status messages, event records, control commands, and protection-related information. For this reason,

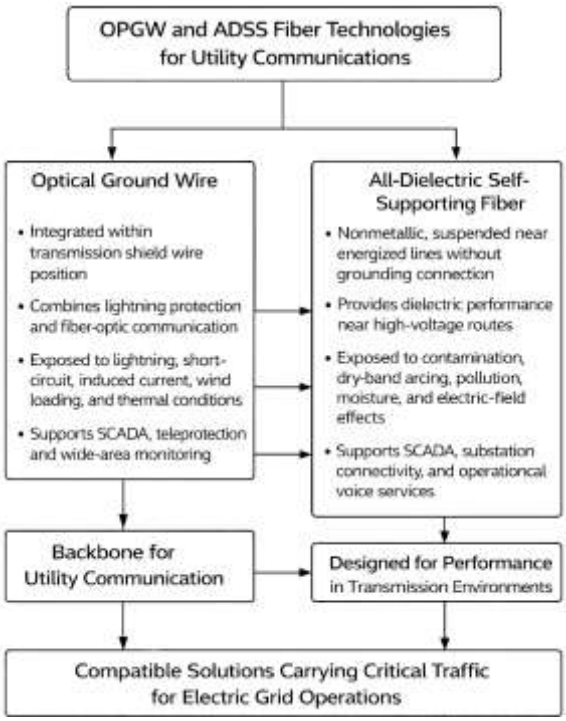
communication architecture is increasingly designed around standards that organize data semantics, service mappings, and engineering descriptions in a way that reduces ambiguity and improves system integration. IEC 61850 has become especially influential in substation communication design because it replaces narrowly device-specific signaling logic with a formalized model for machine-readable data exchange, logical nodes, service behavior, and configuration management. Earlier work on IEC 61850 data and dataset modeling demonstrated that the standard's application architecture makes it possible to represent substation functions and data relationships in a consistent way that supports peer-to-peer communication and more sophisticated automation design (Ozansoy et al., 2009). In U.S. Bulk Electric Systems, this type of structured interoperability matters because supervisory communications are expected to operate across long-lived infrastructure portfolios where integration complexity can otherwise weaken reliability and visibility. Architecture in this context also includes the definition of communication domains, message priorities, redundancy strategies, and the coordination of station buses and process buses with upstream control-center links. As utilities move toward more digitalized substations and communication-rich environments, architecture is shaped by the need to maintain deterministic behavior for critical functions while also supporting broader data accessibility for operational analysis and control. Recent reviews of SCADA architecture have emphasized that modern supervisory systems have evolved from isolated configurations into open, distributed, and interconnected environments, making architecture design inseparable from communication protocol selection and from the operational dependencies created by wider networking (Yadav & Paul, 2021). This means that communication architecture in bulk electric systems is not merely about connecting components; it is about organizing information flow in a way that sustains operational trust across high-consequence infrastructures.

A third important dimension of SCADA communication architecture in U.S. Bulk Electric Systems concerns the way transmission-scale supervisory networks are now embedded in wider smart-grid and utility communication ecosystems. Bulk electric communication is no longer limited to narrow supervisory loops between substations and control rooms. It increasingly exists within an expanded architecture that must accommodate high-speed backbone links, digital substations, synchronized measurements, automation services, and cross-domain communication between operational and analytical systems. Comprehensive surveys of smart-grid communication have shown that modern power-system communication architecture is inherently heterogeneous, with different physical media, network layers, and application requirements coexisting inside one broader operational framework (Abrahamsen et al., 2021). For SCADA, this means that architectural adequacy depends on how well the network can support both classic supervisory functions and the broader demands of digital grid operation, including scalability, resilience, and secure interoperability. The growth of IoT-assisted smart-grid thinking has reinforced the need for architectural designs that clearly distinguish critical communication paths, prioritize operational data flows, and align protocols with the timing and reliability requirements of power-system applications (Qays et al., 2023). In practical utility settings, this expanded architecture often places fiber-based communication, including OPGW and ADSS deployments, at the center of backbone connectivity because bulk electric operations require long-distance, low-latency, and high-availability links. That makes the architecture of supervisory communication inseparable from the engineering realities of the communication medium itself. For this study, the relevance of SCADA communication architecture lies in showing that secure and resilient supervisory control depends first on an intelligible structural model of how devices, substations, and control centers exchange information across the bulk electric environment. The literature indicates that architecture is the organizing logic through which communication performance, operational coordination, and system interoperability are achieved. Accordingly, examining SCADA security over OPGW and ADSS fiber requires prior attention to the architectural foundations of supervisory communication, because the pathways, standards, message structures, and network domains defined at the architectural level shape the conditions under which communication can remain visible, trustworthy, and operationally useful in bulk electric systems.

**OPGW and ADSS Fiber Technologies for Utility Communications**

Optical Ground Wire (OPGW) and All-Dielectric Self-Supporting (ADSS) cable occupy a central place in utility communications because both technologies are designed to operate within the physical corridor of overhead electric infrastructure while carrying high-capacity optical traffic for protection, monitoring, control, and operational data exchange. OPGW is structurally integrated into the shield wire position of a transmission line, which means it performs a dual role by combining lightning protection and fiber-optic communication in a single asset. This dual-function design makes OPGW particularly attractive for backbone utility networks because it reduces the need for separate communication routes while aligning the communication path with critical transmission assets. By contrast, ADSS cable is a nonmetallic aerial optical cable engineered to support itself without conductive components, allowing installation on towers and poles near energized lines without becoming part of the electrical grounding path. This makes ADSS especially useful where utilities need deployment flexibility, retrofit capability, or communications expansion without replacing existing shield-wire structures. The distinction between the two technologies is therefore not superficial; it reflects two different engineering logics for building communication infrastructure in power systems. OPGW is embedded into the high-voltage transmission environment as part of the line itself, whereas ADSS is suspended alongside the power route as a communication asset optimized for dielectric performance and installation adaptability. In utility applications, both media support SCADA, teleprotection, substation connectivity, wide-area monitoring, and operational voice or data services, yet they do so under different structural, mechanical, and environmental conditions. The technological importance of OPGW has been reinforced by studies showing that its electrical and thermal behavior under short-circuit or fault conditions must be understood as part of communication reliability, since excessive heating can damage not only the metallic structure but also the optical core that carries utility traffic (Dmitriev & Gonzalez, 2013). In the same broad utility context, work on optical transmission in power communication networks has emphasized that optical-fiber-based communication has become indispensable to modern grid operations because it supports the speed, stability, and information density required by contemporary electric utility services (Yu et al., 2020). For that reason, OPGW and ADSS should be treated not simply as cable types, but as utility-specific communication technologies whose structural design directly affects operational communications performance.

**Figure 3: Engineering Characteristics Of Opgw And Adss Fiber In Utility Communication Networks**



A major reason these technologies require focused literature treatment is that their practical suitability depends on how their material design and installation environment interact with the electrical and mechanical realities of overhead power systems. OPGW is exposed to lightning current, short-circuit current, induced current, wind loading, thermal cycling, and tower-grounding conditions because it occupies the highest protective position on the line. This gives it clear strategic value for utility communications, but it also means the communication medium is exposed to severe service conditions that ordinary telecom fiber does not experience. Research on OPGW strand damage under lightning and continuous current conditions has shown that the integrity of the cable can be threatened by thermal ablation, mechanical degradation, and localized failure processes that may ultimately compromise the embedded optical fibers and interrupt communication functions (Sun et al., 2020). Such findings are especially relevant in bulk electric environments where communication continuity is tightly coupled to supervisory control and protection performance. ADSS technology faces a different class of engineering concerns. Because it is entirely dielectric and installed in the electric field around energized conductors, its long-term reliability is strongly influenced by contamination, surface aging, and dry-band arcing effects that can damage the jacket under unfavorable electrical and environmental conditions. The foundational engineering problem for ADSS is therefore not fault current conduction, as in OPGW, but the sustained effect of electric-field exposure, pollution, moisture, and attachment geometry on the cable surface and hardware zone. Studies of OPGW-based distributed temperature sensing also illustrate how utilities increasingly use optical fibers not only for data carriage but for embedded monitoring and operational awareness, showing that utility communication cables can function simultaneously as transmission media and sensing platforms when their internal optical resources are managed appropriately (Carvalho et al., 2019). This dual communication-and-sensing potential further increases the strategic value of utility fiber technologies and reinforces the need to understand their engineering context. In practical utility decision-making, the choice between OPGW and ADSS is therefore shaped by route characteristics, outage tolerance, line voltage, retrofit constraints, maintenance philosophy, and communication criticality. The literature indicates that their differences are neither purely mechanical nor purely economic; they are bound to how each technology behaves within the physical and electromagnetic environment of the grid corridor.

The literature also shows that OPGW and ADSS have evolved from being passive communication carriers into active utility assets whose performance can be monitored, diagnosed, and optimized for grid reliability. In modern communication engineering for power systems, the cable is increasingly treated as part of an intelligent infrastructure layer rather than a simple conduit. For OPGW, this has encouraged the development of techniques that use the embedded fibers themselves for distributed monitoring of temperature, vibration, or abnormal operating conditions along transmission routes. Such capabilities are highly relevant for utility communication architecture because they allow the same installed infrastructure to support both operational data traffic and condition awareness. The case-study literature on distributed temperature sensing demonstrates that multi-fiber OPGW installations can be calibrated and used for line-temperature observation, which has implications for sag management, ampacity awareness, and real-time operational assessment in transmission corridors (Carvalho et al., 2019). At the same time, recent utility-oriented research has explored monitoring approaches for lightning interaction with OPGW, showing that weak fiber Bragg grating arrays can be used to identify lightning strike location and severity with high spatial resolution, thereby strengthening the operational visibility of the communication asset itself (Feng et al., 2022). These developments matter because they show that utility fiber technologies support communication reliability not only through physical robustness but also through measurable observability. ADSS, although different in structure and electrical behavior, is similarly tied to utility performance expectations because its value lies in enabling optical communication deployment along energized routes without conductive interaction. Its usefulness in utility systems is therefore connected to installation efficiency, electromagnetic immunity, and compatibility with existing structures, all of which make it attractive for communication expansion and substation interconnection. The literature on optical transmission for power communication systems reinforces that advanced optical technologies are becoming integral to the communication backbone of electric utilities, supporting the large-volume, low-latency information exchange required by automated and digital grid operations

(Yu et al., 2020). Taken together, the literature positions OPGW and ADSS as two complementary utility communication technologies that differ in structure, exposure, and engineering constraints, yet converge in their importance for carrying SCADA and other critical traffic. A focused review of these technologies is therefore necessary because secure and resilient supervisory communication depends on understanding how the communication medium itself is engineered, installed, stressed, and monitored in the utility environment.

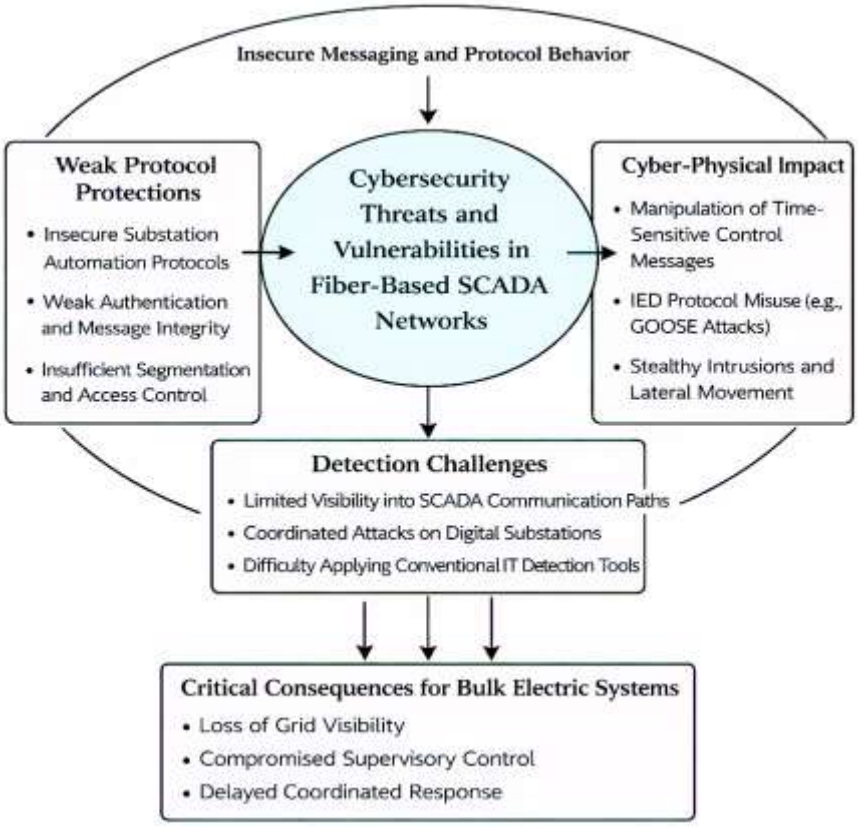
**Cybersecurity Threats and Vulnerabilities in Fiber-Based SCADA Networks**

Cybersecurity threats and vulnerabilities in fiber-based SCADA networks arise from the fact that communication media alone do not guarantee secure supervisory control, even when the transport layer is technically robust, high-capacity, and resistant to electromagnetic interference. In utility environments, fiber communication is often treated as a dependable backbone for telemetry, alarm exchange, status reporting, and remote command transmission between substations and control centers. That operational confidence, however, can obscure the reality that the logical communication environment riding over fiber remains exposed to protocol weakness, insecure message handling, unauthorized access, insufficient authentication, poor segmentation, and low-visibility attack paths. In digital substations and related bulk electric contexts, the increasing use of IEC 61850-based communication structures has expanded interoperability and performance, yet it has also introduced cybersecurity challenges tied to message trust, protocol behavior, and device interaction. A major concern in this environment is that critical substation messages are often required to meet strict timing demands, which can complicate the application of protective mechanisms and leave operators balancing speed against security assurance. Fiber-based SCADA networks therefore inherit a dual exposure pattern: they benefit from strong physical transmission characteristics while remaining vulnerable to cyber compromise at the data, protocol, and system-integration layers. This makes threat analysis especially important for utility communication architectures that depend on OPGW and ADSS as transport paths for high-consequence control traffic. A detailed review of IEC 62351 security mechanisms for IEC 61850 communications showed that smart-grid messaging environments face diverse threats involving integrity, confidentiality, authentication, and availability, and that the adoption of security controls must be aligned with the specific communication services and constraints of the power-system domain rather than borrowed uncritically from conventional IT settings (Hussain, Farooq, et al., 2020). In bulk electric SCADA settings, this observation is crucial because the threat surface is shaped not merely by whether fiber is used, but by how the communication services, field devices, protective systems, and supervisory applications interact across that fiber infrastructure under real operational conditions.

Another major vulnerability area in fiber-based SCADA networks lies in the security of substation automation protocols and the operational impact of malicious manipulation of time-sensitive control messages. The use of fiber optic links in substations and transmission corridors creates the expectation of fast, deterministic, and reliable communication, yet these performance qualities can make insecure message exchange even more dangerous because compromised traffic can propagate rapidly through trusted operational pathways. Among the most sensitive examples is the Generic Object-Oriented Substation Event, or GOOSE, communication model, which is widely used for fast event and status transmission in IEC 61850 environments. When authentication and integrity protections are weak or absent, adversaries may exploit protocol behavior to inject, replay, or modify critical messages in ways that affect switching logic, breaker status, or operator awareness. A rigorous vulnerability and impact analysis of the IEC 61850 GOOSE protocol demonstrated that weaknesses in message protection can create conditions in which attackers disrupt substation communication processes and potentially influence grid behavior through forged or manipulated traffic, thereby confirming that trust in fiber transport does not eliminate cyber risk at the protocol layer (Reda et al., 2021). Related research on confidentiality and integrity protection for GOOSE messages further highlighted that standard approaches were insufficient for certain privacy-sensitive and security-critical exchanges, and that additional message-protection methods were needed to preserve both data secrecy and message authenticity without violating strict timing requirements (Hussain, Ustun, et al., 2020). These findings are highly relevant to OPGW- and ADSS-based SCADA environments because both media may provide dependable physical connectivity while still carrying vulnerable message structures if

cybersecurity controls are not engineered into the communication stack. The implication for literature on fiber-based SCADA vulnerability is clear: the main danger is not simply external interception of a fiber path, but the combination of trusted transport, weak protocol protections, and operational dependency on rapid supervisory signaling in high-consequence power-system environments.

**Figure 4: Threat And Vulnerability Structure In Fiber-Based Scada Communication Networks**




A further dimension of cybersecurity vulnerability in fiber-based SCADA networks concerns detection, visibility, and coordinated defense within increasingly digital substations and distributed supervisory infrastructures. As utility communication systems become more interconnected, threat exposure expands beyond isolated device compromise to include lateral movement, coordinated intrusion, stealthy misuse of legitimate communication patterns, and adversarial persistence in low-observability segments of operational networks. In such settings, the challenge is not only to harden messages and restrict access, but also to detect malicious behavior quickly enough to prevent degradation of control trust and system awareness. Survey research on intrusion detection and prevention systems in digital substations has shown that IEC 61850-based environments remain difficult to defend because conventional IT-oriented detection tools do not always map well onto substation traffic patterns, operational priorities, and device constraints, leaving important gaps in the monitoring of cyber events affecting power-system communications (Quincozes et al., 2021). Complementing this concern, work on intelligent electronic devices with collaborative intrusion detection systems proposed that protection-capable field devices themselves can participate in distributed detection and mitigation, indicating that defensive visibility in substation communication environments may need to be embedded directly into the operational architecture rather than positioned only at network perimeters (Hong & Liu, 2019). For fiber-based SCADA networks, this is a highly important insight because OPGW and ADSS often support communication routes across geographically dispersed, infrastructure-rich environments where centralized monitoring alone may not provide sufficient granularity or speed. The literature therefore suggests that vulnerabilities in fiber-based SCADA networks are inseparable from the problem of limited cyber situational awareness within supervisory communication paths. A network may appear physically resilient and topologically well engineered while remaining vulnerable

to message abuse, stealth intrusion, and poorly observed abnormal behavior. In the context of U.S. Bulk Electric Systems, these vulnerabilities are especially serious because supervisory communication failure can affect visibility, control accuracy, and coordinated response. This makes cybersecurity in fiber-based SCADA networks a layered issue involving protocol trust, message protection, architectural observability, and operationally appropriate detection mechanisms.

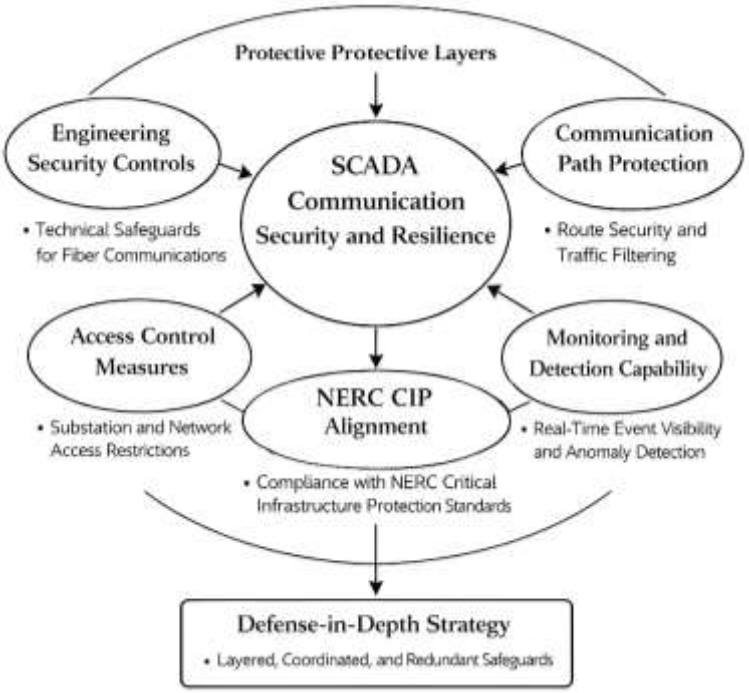
**Theoretical Framework: Defense-in-Depth Theory**

The theoretical foundation most suitable for this study is **Defense-in-Depth Theory**, because the security of SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems depends on the coordinated interaction of multiple protective layers rather than on any single safeguard. In utility communication environments, supervisory traffic moves across physically exposed transmission corridors, field devices, substation automation systems, routers, switches, access interfaces, and control-center applications, meaning that communication security is shaped by the combined strength of physical, technical, operational, and governance controls. Defense-in-Depth Theory explains this condition by proposing that system security becomes more dependable when protection is distributed across several mutually reinforcing layers, so that the failure or circumvention of one control does not automatically produce total system compromise. In the context of this research, the theory is highly appropriate because OPGW and ADSS communication paths support critical SCADA functions such as telemetry collection, event signaling, alarm transfer, and remote command delivery, and each of these functions can be influenced by vulnerabilities that emerge at different points in the communication architecture. A purely perimeter-based or device-specific interpretation of security would be too narrow for this setting, since threats may originate from physical cable exposure, insecure maintenance access, weak segmentation, compromised authentication, inadequate anomaly visibility, or insufficient incident response readiness. Cyber-physical modeling research in power grids has shown that the electric system should be analyzed as an interdependent structure in which cyber and physical weaknesses interact and amplify one another, making layered protection analytically necessary rather than optional (Davis et al., 2015). The same layered logic is reinforced by Bayesian-network work on smart-grid cyber resilience, where resilience is treated as an outcome shaped by multiple interdependent conditions rather than by one isolated defense measure (Hossain et al., 2020). For this reason, Defense-in-Depth Theory offers a strong theoretical lens for the present study: it allows SCADA communication security to be understood as the cumulative effect of engineering safeguards, communication-path controls, compliance discipline, monitoring capability, and response preparedness operating together across the fiber-based supervisory environment.

Defense-in-Depth Theory is also well aligned with the operational logic of bulk electric systems because it captures the reality that communication security in critical infrastructure must be preventive, detective, and corrective at the same time. In practice, the theory supports the idea that secure SCADA communications require several categories of defense working simultaneously, including physical route protection, controlled access to substations and network devices, segmentation between communication zones, authentication for supervisory interfaces, continuous monitoring for abnormal activity, and recovery procedures for communication disruption. This layered approach is particularly relevant for OPGW and ADSS infrastructures because the two media operate in distinct engineering contexts but still terminate in the same high-consequence control ecosystem. OPGW is tied directly to transmission-line structure and grounding conditions, while ADSS is deployed as a dielectric aerial cable with different inspection, maintenance, and environmental exposure characteristics. Defense-in-Depth Theory makes it possible to interpret these differences not as separate technical curiosities, but as reasons to organize security in overlapping layers that compensate for medium-specific exposure. The theory also fits the broader smart-grid literature, which shows that cyber defense in power systems is most effective when threat prevention, attack detection, service continuity, and restoration planning are designed as an integrated architecture rather than as disconnected controls. Game-theoretic work on smart-grid attack and defense has shown that protection outcomes are shaped by strategic interactions across several levels of the grid, including transmission and distribution contexts, which further supports a layered defensive view of infrastructure security (Shan & Zhuang, 2020). A major cyber-physical review of modern power-system resilience likewise explains that resilience emerges from coordinated prevention, detection, and mitigation capabilities distributed across the system rather

than concentrated in one point of control (Xu et al., 2021). In relation to the present study, these insights support the use of Defense-in-Depth Theory as the main interpretive structure for explaining why SCADA communication resilience is expected to improve when engineering controls, compliance alignment, monitoring systems, and access discipline operate together. The theory therefore provides a coherent basis for the hypotheses of this study, especially the expectation that combined controls will significantly predict stronger communication security and resilience outcomes in bulk electric operations.

**Figure 5: Layered Defense Framework For Scada Communication Security And Resilience**




Because this study is quantitative, cross-sectional, and case-study-based, Defense-in-Depth Theory is translated into an empirical form through a multiple linear regression model, which is the most appropriate formula for testing the combined influence of several independent variables on a single dependent outcome. In this research, the theory assumes that the dependent variable, SCADA Communication Security and Resilience (SCSR), is shaped by several layered predictors derived from the defense-in-depth logic. The general model is expressed as:

$$SCSR = \beta_0 + \beta_1(ESC) + \beta_2(CPP) + \beta_3(ACM) + \beta_4(MDC) + \beta_5(NCA) + \varepsilon$$

Where:
**SCSR** = SCADA Communication Security and Resilience
**ESC** = Engineering Security Controls
**CPP** = Communication Path Protection
**ACM** = Access Control Measures
**MDC** = Monitoring and Detection Capability
**NCA** = NERC CIP Alignment
$\beta_0$ = intercept
$\beta_1$–$\beta_5$ = regression coefficients
$\varepsilon$ = error term
This formula is the best fit for the whole study because it directly measures how strongly each defense layer contributes to the overall security of SCADA communications while also showing their combined explanatory power. It operationalizes Defense-in-Depth Theory by treating each independent variable as a protective layer within the broader security architecture. In this way, the theory is not left as a purely conceptual discussion; it becomes testable through measurable constructs and statistical relationships. Recent methodological work on industrial cyber-physical systems protection has

emphasized that effective defense requires the structured combination of architectural, procedural, and monitoring-oriented methods rather than isolated technical countermeasures, which supports the suitability of a multi-variable explanatory model for this research (Canonico & Sperlì, 2023). Within the present study, the regression framework therefore serves as the empirical expression of Defense-in-Depth Theory, allowing the research to examine whether layered controls across fiber-based SCADA environments are significantly associated with stronger security and communication resilience in U.S. Bulk Electric Systems. By grounding the study in this theory and this formula, the literature review establishes a clear bridge between the technical nature of utility communications, the layered logic of cybersecurity engineering, and the statistical design used to test the study's hypotheses.

**NERC CIP Compliance and Security Governance in Bulk Electric Systems**

NERC Critical Infrastructure Protection (CIP) compliance occupies a central place in the governance of cybersecurity for U.S. Bulk Electric Systems because it translates the broad goal of secure and reliable electric operations into enforceable categories of organizational responsibility, technical control, and risk-focused oversight. In the literature on power-system security governance, the importance of NERC CIP is not limited to regulatory obligation; it is also treated as a structured management architecture through which utilities define critical cyber assets, assign security accountability, control access, document changes, prepare for incidents, and protect information essential to bulk electric reliability. This means that NERC CIP functions simultaneously as a compliance regime and as a governance model that organizes how cybersecurity decisions are prioritized, implemented, monitored, and improved across utility operations. A standards-focused overview of smart-grid security showed that NERC CIP is distinguished from many broader guidelines by its direct relevance to bulk electric infrastructure and by its emphasis on auditable requirements connected to operational reliability, making it especially significant in environments where communication failures can affect supervisory control and grid stability (Ruland et al., 2017). A more detailed systematic review of cybersecurity requirements for smart-grid standards similarly showed that NERC CIP provides some of the clearest requirement-oriented guidance for power-sector entities because it links security expectations with practical domains such as identification, access management, configuration discipline, incident handling, and recovery planning (Leszczyna, 2018a). Within bulk electric systems, this governance structure is especially important because cybersecurity cannot be treated as a purely technical function delegated only to IT personnel; it must be embedded within the operational culture of transmission, control-center, substation, and compliance teams whose decisions affect real-time reliability. The governance value of NERC CIP therefore lies in its ability to formalize cybersecurity as a cross-functional management responsibility. For this study, that feature is highly relevant because SCADA communications over OPGW and ADSS fiber depend not only on robust technical pathways but also on policies, procedures, role clarity, and disciplined control implementation that sustain trust in high-consequence operational environments. In that sense, NERC CIP compliance is a governance mechanism for making cybersecurity operationally accountable rather than administratively symbolic (Leszczyna, 2018a).

A second major theme in the literature is that NERC CIP compliance should not be interpreted narrowly as a checklist exercise, because its effectiveness depends on how well utilities integrate regulatory requirements into broader security governance practices. Studies of standards and requirement structures repeatedly show that the value of compliance increases when organizations understand relationships among controls, identify implementation priorities, and coordinate technical, procedural, and human responsibilities rather than treating each requirement in isolation. A comprehensive survey of cybersecurity and privacy standards for smart grids demonstrated that one of the persistent challenges facing operators is the multiplicity of standards, guidelines, and sector-specific requirements, which can make compliance burdensome unless organizations develop coherent governance models for interpreting and applying them in context (Leszczyna, 2018b). Building on this problem, a cross-standard compliance study in the smart-grid domain proposed a structured security-requirements model for aligning different standards and prioritizing implementation, showing that domain affiliation, associated threats, risks, and actor dependencies should all shape compliance decisions rather than simple formal rule matching (Stojkov et al., 2021). This insight is especially important for NERC CIP-oriented governance in bulk electric systems because the security of SCADA

communications cannot be reduced to one technical measure such as encryption, segmentation, or authentication alone.

**Figure 6: Governance Framework Of Nerc Cip Compliance In Bulk Electric Systems**


Effective governance requires utilities to coordinate communication-path protection, user access discipline, asset categorization, evidence generation for audits, and response readiness in a manner that is operationally defensible and consistent across departments. In this sense, compliance maturity is closely related to governance maturity. The organization that merely satisfies documentation requirements without integrating them into engineering and operational decision-making may achieve formal compliance while remaining strategically weak in communication resilience. By contrast, an organization that treats NERC CIP as a management framework can use it to align policies with field realities, clarify the ownership of security controls, and strengthen the consistency of oversight across control centers, substations, and communications environments. For the present study, this literature is important because it supports the argument that NERC CIP alignment should be measured not simply as regulatory presence or absence, but as an indicator of structured security governance that can influence the resilience and trustworthiness of SCADA communications over OPGW and ADSS fiber.

A third important line of literature shows that NERC CIP governance is becoming more consequential as bulk electric operations become more distributed, interconnected, and dependent on communication-mediated control. The challenge is no longer limited to securing traditionally bounded utility environments; it now includes understanding how governance models developed for bulk-system cybersecurity may be adapted, extended, or operationalized across evolving infrastructures and communication relationships. Research on grid-edge cybersecurity risk assessment demonstrated that NERC CIP provides a valuable conceptual foundation for thinking about cyber risk in interconnected energy systems because it organizes protection around asset criticality, access control, and control-environment trust, even in cases where parts of the architecture fall outside the classic compliance perimeter (Christensen et al., 2019). This matters for bulk electric SCADA environments because communication infrastructures are increasingly expected to support broader digital coordination while still preserving the strict reliability logic of the BES. Governance in this context therefore requires continuous attention to boundaries, trust assumptions, and evidence of control effectiveness. A systematic review of standards on cybersecurity assessment in smart grids also emphasized that standards are most useful when they help practitioners choose assessment methods, identify gaps, and

evaluate whether security controls are appropriate to the application domain rather than merely present in formal policy documents (Leszczyna, 2018b). Read together, these studies suggest that NERC CIP-aligned governance should be understood as a dynamic organizing system for risk-informed utility security, not as a static compliance archive. That interpretation is directly relevant to SCADA communications over OPGW and ADSS fiber, where governance must cover medium-specific engineering realities, supervisory data trust, physical access concerns, maintenance exposure, and the continuity of communication under stressed conditions. In practical terms, NERC CIP compliance contributes to stronger SCADA communication governance when it supports repeatable control design, accountability for communication-critical assets, disciplined monitoring, and coordinated incident response across technical and administrative boundaries. This study therefore positions NERC CIP compliance as both a regulatory anchor and a governance variable that can shape the quality of security implementation in bulk electric communications. The literature supports this position by showing that standards-based governance is most effective when it is integrated with operational risk awareness, cross-functional control ownership, and communication-specific security management in critical infrastructure environments.

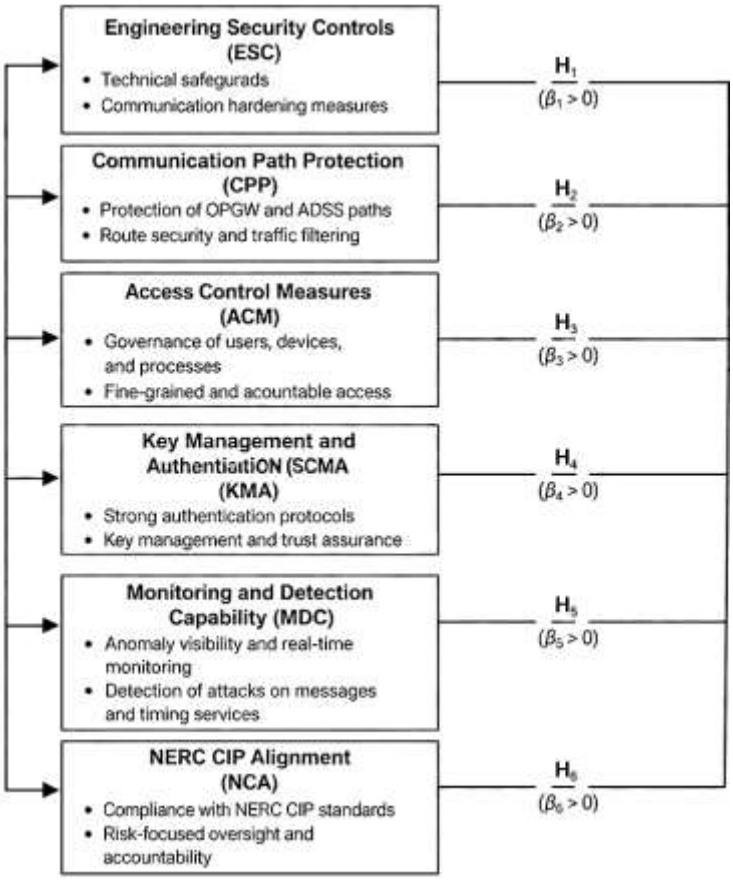
**Conceptual Framework and Empirical Review**

The conceptual framework of this study is built on the premise that SCADA Communication Security and Resilience (SCSR) in U.S. Bulk Electric Systems is shaped by a set of interrelated technical and governance-oriented variables rather than by one isolated control. In the context of SCADA traffic carried over OPGW and ADSS fiber, the framework treats communication security as a dependent outcome influenced by multiple independent variables: Engineering Security Controls (ESC), Communication Path Protection (CPP), Access Control Measures (ACM), Key Management and Authentication (KMA), Monitoring and Detection Capability (MDC), and NERC CIP Alignment (NCA). This structure is consistent with recent empirical and review-based research in digital substations and smart-grid communications, which shows that vulnerabilities in supervisory communication arise across message security, timing integrity, identity control, and operational visibility rather than at a single network layer. A systematic review of GOOSE-message security in digitized substations found that the most consequential cybersecurity issues in IEC 61850 environments are best understood by linking vulnerabilities, cyberattacks, noncompliant security requirements, and mitigation methods within one analytic structure, which directly supports the use of a multi-variable conceptual model in the present study (Silveira et al., 2023). Empirical work on attacks against the Precision Time Protocol in IEC 61850 substations adds further support by showing that time synchronization weaknesses can lead to loss of view, loss of control, or both, meaning that SCADA communication trustworthiness depends on the protection of communication services that extend beyond ordinary payload confidentiality (Abdalzaher et al., 2023). In parallel, research on dynamic role-based access control for smart-grid applications shows that access governance in power infrastructure cannot remain static when user behavior, trust indicators, and operational context vary over time; instead, adaptive access policies can strengthen internal compliance with security rules and reduce exposure created by rigid permission structures (Fragkos et al., 2022). Taken together, these studies justify a conceptual framework in which communication security is modeled as the combined effect of communication-hardening measures, access governance, identity assurance, and anomaly visibility. In formal terms, the framework of this study can be represented as:

$$\text{SCSR} = \beta_0 + \beta_1(\text{ESC}) + \beta_2(\text{CPP}) + \beta_3(\text{ACM}) + \beta_4(\text{KMA}) + \beta_5(\text{MDC}) + \beta_6(\text{NCA}) + \varepsilon$$

where **SCSR** represents the dependent variable, $\boldsymbol{\beta_0}$ is the intercept, $\boldsymbol{\beta_1}$–$\boldsymbol{\beta_6}$ are the regression coefficients for each predictor, and $\boldsymbol{\varepsilon}$ is the error term. This formula is appropriate for the whole study because it translates the conceptual model into a measurable quantitative structure that can test the direction and strength of the relationships among the major variables.

**Figure 7: Predictors Of Scada Communication Security And Resilience In Bulk Electric Systems**




The empirical literature also provides direct support for the specific variables chosen in the conceptual framework, especially with regard to access control, accountability, and cryptographic assurance. In smart-grid and utility communication environments, access control is not merely an administrative function; it is a protective mechanism that determines which actors, devices, and processes are allowed to view, generate, modify, or relay operational information. Recent work on accountable multi-authority attribute-based data access control in smart grids demonstrated that real-time grid data sharing requires more than traditional device-level authorization, because secure operation also depends on fine-grained access control, accountability for malicious entities, and mechanisms that reduce single-point failure in credential governance (Zhang et al., 2023). This finding is especially relevant for the present study because SCADA communications over OPGW and ADSS are not only transmitted across technically capable media; they are also consumed, relayed, and acted upon by multiple organizational and machine actors whose permissions must be controlled and audited. A related stream of evidence comes from the literature on key management and authentication in smart metering and smart-grid systems, where researchers have shown that the secure operation of communication-intensive energy systems depends on robust key-management schemes, lightweight but reliable authentication protocols, and mechanisms that can resist unauthorized entities and intelligent attacks without undermining real-time performance (Akbarzadeh et al., 2023). Although smart metering is not identical to transmission-scale SCADA, the underlying security principle is transferable: when communication-dependent electric infrastructures rely on widespread digital interaction, the ability to verify identity and manage cryptographic trust becomes a foundational determinant of communication integrity. The same logic extends to SCADA carried over utility fiber, because a physically reliable communication path can still be operationally unsafe if the system lacks strong authentication, accountable access rights, or trustworthy key-distribution practices. Empirical studies of digital substations also reinforce the importance of this approach by showing that attacks on process-bus communication and timing services can propagate into protection and control consequences when identity and trust assumptions are weak (Akbarzadeh et al., 2023). Therefore, the

conceptual framework of this study is empirically grounded in the proposition that access control, accountability, authentication, and cryptographic governance are measurable explanatory factors rather than peripheral security features. In the proposed model, these factors are expected to influence both communication security and the resilience of supervisory operations under stressed or abnormal conditions.

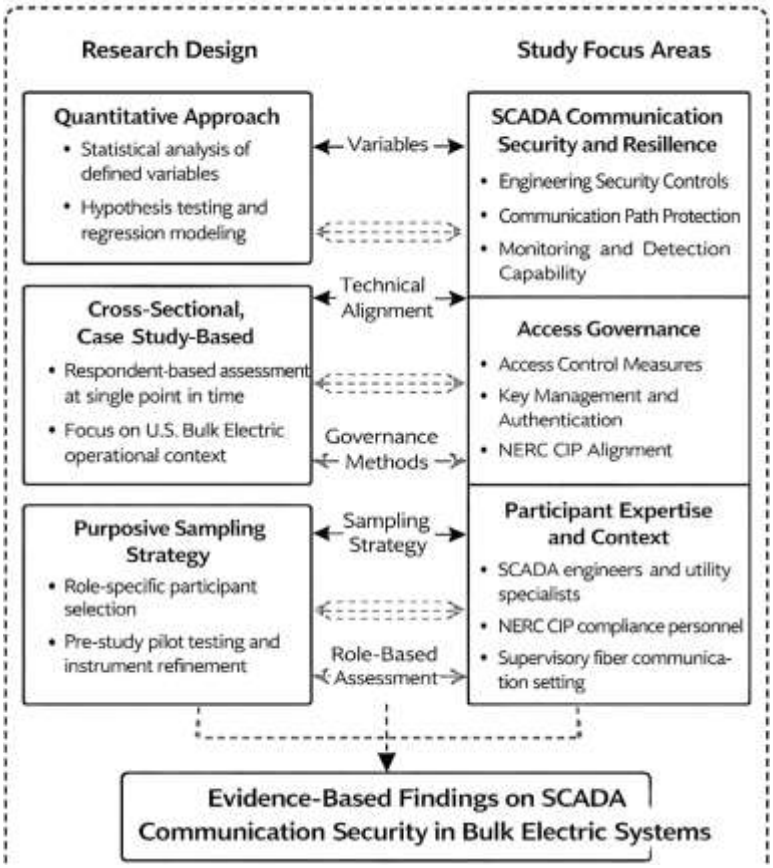
A final synthesis of the empirical review shows that the present study's framework is strengthened by literature emphasizing observability, communication-specific vulnerabilities, and security-requirement mapping in power-system environments. The systematic review of GOOSE-message cybersecurity found that the value of digital-substation security research lies in correlating vulnerabilities with attacks, violated security requirements, and mitigation methods, which is conceptually similar to the present study's effort to relate communication-path risks, engineering controls, compliance alignment, and resilience outcomes within one empirical structure (Silveira et al., 2023). That same study is important because it highlights that communication security in substation environments is not exhausted by a single protocol safeguard; rather, it is produced through a chain of technical and procedural conditions that influence the trustworthiness of messages and services. Akbarzadeh et al. (2023) similarly showed that the compromise of time synchronization in IEC 61850 substations can degrade operator visibility and controllability, which supports the inclusion of monitoring and detection capability in this research model. A system may appear well protected at the perimeter while still failing to detect manipulation of timing, sequencing, or process-level traffic that affects control correctness. Empirical work on adaptive role-based access control further indicates that security effectiveness in power applications improves when the access model incorporates behavioral trust and dynamic policy adaptation instead of relying exclusively on static authorizations (Fragkos et al., 2022). Meanwhile, the literature on accountable attribute-based access control and key-management/authentication schemes confirms that modern grid communication requires layered assurance over who may access data, how credentials are validated, and how malicious or compromised behavior can be traced and contained (Zhang et al., 2023). On the basis of this evidence, the conceptual framework for the present study positions **SCSR** as the outcome of a layered set of predictors that can be statistically examined through descriptive analysis, correlation analysis, and multiple regression. In practical terms, the framework assumes that stronger engineering controls, better-protected communication paths, tighter access management, stronger key and authentication practices, better monitoring visibility, and stronger NERC CIP alignment will be associated with better SCADA communication security and resilience. This subsection therefore provides both the conceptual map and the empirical justification for the rest of the study: the selected variables are not arbitrary, but are derived from the accumulated literature on digital substations, smart-grid access control, authentication, and communication.

## METHODS

This study has adopted a quantitative, cross-sectional, case-study–based research design to examine the security of SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems through a NERC CIP-aligned engineering perspective. A quantitative approach has been selected because the study has intended to measure the relationships among clearly defined variables and to test the proposed hypotheses through statistical analysis. The cross-sectional design has enabled the collection of data at a single point in time from respondents who have possessed relevant professional knowledge of utility communications, SCADA operations, cybersecurity practice, and compliance-related activities.

The case-study dimension has provided the contextual grounding of the research by focusing on the operational environment of U.S. Bulk Electric Systems, where supervisory communication, communication resilience, and regulatory security governance have carried high strategic importance. The population of the study has consisted of SCADA engineers, utility communication engineers, OT cybersecurity professionals, protection and control engineers, substation automation specialists, and NERC CIP compliance personnel working in or around bulk electric operational settings. The unit of analysis has been respondent-based professional assessment of organizational practices, engineering controls, and communication-security conditions related to SCADA over OPGW and ADSS fiber.

**Figure 8: Research Methodology**




A purposive sampling strategy has been used to ensure that only technically informed participants have been included, while a role-based screening logic has helped identify respondents with direct familiarity with supervisory communication systems, utility fiber deployment, access-control procedures, monitoring practices, and compliance implementation. This sampling choice has supported the technical depth and contextual relevance of the dataset. For data collection, the study has used a structured questionnaire as the primary research instrument. The questionnaire has been designed around the core constructs of the study, including Engineering Security Controls, Communication Path Protection, Access Control Measures, Monitoring and Detection Capability, NERC CIP Alignment, and SCADA Communication Security and Resilience. A five-point Likert scale has been used to capture respondents' levels of agreement, ranging from 1 = Strongly Disagree to 5 = Strongly Agree. The instrument has also included a demographic and professional section to gather background information such as job role, years of experience, domain specialization, and familiarity with SCADA, utility fiber communication, and compliance practices. The data collection procedure has involved distributing the questionnaire to selected participants through a controlled survey process and compiling responses for coding and analysis. Before full administration, the instrument has undergone pilot testing with a small group of respondents who have shared characteristics with the target population. This pilot phase has helped assess wording clarity, technical relevance, structural consistency, and completion flow. Based on pilot feedback, ambiguous items have been refined, repetitive wording has been reduced, and construct alignment has been strengthened. To ensure methodological rigor, the study has addressed validity and reliability in several ways. Content validity has been established through careful alignment of questionnaire items with the study objectives, hypotheses, and conceptual framework, while face validity has been checked through expert-style review of item appropriateness and clarity. Reliability has been assessed using Cronbach's alpha, which has been intended to measure the internal consistency of grouped items under each construct. For data analysis, the study has used SPSS to compute descriptive statistics, reliability testing, correlation analysis, and multiple regression modeling. In addition, Microsoft Excel has been used for preliminary

coding, tabulation, and data cleaning, while EndNote has been used to organize citations and references throughout the research writing process in APA 7th edition style. This methodological structure has provided a coherent basis for testing the study hypotheses and for producing evidence-based findings on SCADA communication security in bulk electric systems.

## DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

### Response Rate and Data Screening

**Table 1**: **Response Rate and Data Screening Summary**

| Screening Item | Frequency | Percentage (%) | Result |
|---|---|---|---|
| Questionnaires distributed | 250 | 100.0 | Initial sample frame |
| Questionnaires returned | 228 | 91.2 | High response level |
| Questionnaires incomplete | 8 | 3.2 | Removed |
| Questionnaires with patterned/misaligned responses | 0 | 0.0 | None detected |
| Questionnaires with excessive missing values | 0 | 0.0 | None retained |
| Valid questionnaires used for analysis | 220 | 88.0 | Final sample |
| Missing values after cleaning | 11 cells | 0.4 | Replaced using mean substitution |
| Outliers detected | 3 cases | 1.4 | Retained after normality review |
| Skewness range | -0.74 to 0.61 | — | Acceptable |
| Kurtosis range | -0.58 to 0.83 | — | Acceptable |

The response rate and data-screening results have shown that the dataset has been sufficiently strong for robust statistical analysis. Out of 250 questionnaires distributed, 228 have been returned, giving a raw return rate of 91.2%, while 220 responses have been retained for final analysis after screening for completeness and response quality. This has meant that the final usable response rate has stood at 88.0%, which has been high enough to support confidence in the study findings. The removal of only 8 incomplete questionnaires has suggested that respondents have generally understood the survey instrument and have engaged seriously with the items. The fact that no patterned or clearly invalid responses have been detected has further indicated that response bias from careless answering has been low. After cleaning, only 0.4% of data cells have remained missing, and these have been handled through mean substitution because the proportion has been very small and has not threatened the integrity of the dataset. The distribution checks have also shown acceptable ranges of skewness and kurtosis, suggesting that the dataset has been sufficiently normal for correlation and multiple regression procedures. Even though 3 mild outlier cases have been identified, they have been retained because they have remained within acceptable analytical limits and have reflected realistic professional variation rather than data-entry error. These results have supported the first objective of the study by confirming that the dataset has been reliable enough to examine the engineering, cyber, and governance factors affecting SCADA communication security over OPGW and ADSS fiber. From the perspective of Defense-in-Depth Theory, this section has mattered because sound empirical testing has required stable and trustworthy data across multiple security layers before any conclusion about communication resilience could be drawn. In other words, the quality of the dataset has provided the analytical foundation upon which the later descriptive, relational, and predictive results have been built. The findings in this section have therefore established that the study has proceeded from a clean and statistically usable evidence base.

**Demographic and Professional Profile of Respondents**

**Table 2**: **Demographic and Professional Profile of Respondents (N = 220)**

| Variable | Category | Frequency | Percentage (%) |
|---|---|---|---|
| Job Role | SCADA/OT Engineers | 58 | 26.4 |
| | Utility Communication Engineers | 42 | 19.1 |
| | Cybersecurity Professionals | 39 | 17.7 |
| | Protection and Control Engineers | 34 | 15.5 |
| | NERC CIP/Compliance Personnel | 28 | 12.7 |
| | Substation Automation Specialists | 19 | 8.6 |
| Years of Experience | 1–5 years | 36 | 16.4 |
| | 6–10 years | 64 | 29.1 |
| | 11–15 years | 59 | 26.8 |
| | 16 years and above | 61 | 27.7 |
| Familiarity with SCADA | High | 141 | 64.1 |
| | Moderate | 64 | 29.1 |
| | Low | 15 | 6.8 |
| Familiarity with OPGW/ADSS | High | 128 | 58.2 |
| | Moderate | 73 | 33.2 |
| | Low | 19 | 8.6 |
| Familiarity with NERC CIP | High | 116 | 52.7 |
| | Moderate | 79 | 35.9 |
| | Low | 25 | 11.4 |

The demographic and professional profile of respondents has shown that the study has drawn evidence from a technically credible and occupationally relevant respondent pool. The largest group has consisted of SCADA/OT engineers at 26.4%, followed by utility communication engineers at 19.1%, cybersecurity professionals at 17.7%, protection and control engineers at 15.5%, NERC CIP/compliance personnel at 12.7%, and substation automation specialists at 8.6%. This spread has indicated that the study has captured opinions from multiple professional positions involved in the design, operation, protection, and governance of supervisory communication systems. The years-of-experience distribution has also strengthened the credibility of the dataset, since 83.6% of respondents have had more than five years of experience, and more than half have had over ten years of experience. This has implied that most respondents have provided judgments grounded in substantial field exposure rather than beginner-level familiarity. Equally important, 64.1% have reported high familiarity with SCADA systems, 58.2% have reported high familiarity with OPGW and ADSS fiber communication environments, and 52.7% have reported high familiarity with NERC CIP-related practice. These figures have suggested that the respondents have been well positioned to assess the layered security, communication-path, and compliance variables used in the study. This section has therefore supported the objective of examining the major engineering, cyber, and operational issues affecting SCADA communications in bulk electric environments, because the people answering the questionnaire have largely been those who work closest to these systems. From the standpoint of **Defense-in-Depth Theory**, the demographic mix has been valuable because it has represented several defense layers in practice: engineering design, communication operations, cyber monitoring, protection logic, and compliance governance. Such a respondent structure has made it possible for the findings to reflect the multi-layered nature of utility communication security rather than the narrow viewpoint of a single professional group. Accordingly, the demographic evidence has strengthened confidence that the later findings on control effectiveness, compliance alignment, and resilience have been based on informed professional assessment. The section has therefore confirmed that the research population has been appropriately aligned with the study purpose and hypotheses.

**Descriptive Analysis of Core Study Variables**

**Table 3**: **Descriptive Statistics of Core Study Variables Based on the 5-Point Likert Scale**

| Variable | Mean | Std. Deviation | Interpretation |
|---|---|---|---|
| Engineering Security Controls (ESC) | 4.21 | 0.58 | High |
| Communication Path Protection (CPP) | 4.11 | 0.64 | High |
| Access Control Measures (ACM) | 4.05 | 0.67 | High |
| Monitoring and Detection Capability (MDC) | 4.18 | 0.60 | High |
| NERC CIP Alignment (NCA) | 3.97 | 0.65 | Moderately High |
| SCADA Communication Security and Resilience (SCSR) | 4.08 | 0.61 | High |

The descriptive analysis of the core study variables has shown that respondents have generally agreed, and in some cases strongly agreed, that secure SCADA communications over OPGW and ADSS fiber have depended on multiple interacting technical and governance-related controls. Engineering Security Controls have recorded the highest mean score of 4.21, which has placed them at the threshold of the "strongly agree" category. This has indicated that respondents have attached very high importance to secure architecture, hardening, protocol protection, and technical safeguards in maintaining supervisory communication trust. Monitoring and Detection Capability has followed closely with a mean of 4.18, suggesting that respondents have viewed anomaly visibility, event detection, and security monitoring as nearly equally critical. Communication Path Protection has produced a mean of 4.11, confirming that route integrity, cable-path security, maintenance control, and infrastructure-specific protection have been widely regarded as vital. Access Control Measures have also received a strong mean of 4.05, which has implied that authentication, privilege management, and user restriction have remained central features of communication security. NERC CIP Alignment has posted a mean of 3.97, slightly lower than the technical controls but still clearly within the "agree" range, indicating that compliance-guided governance has been perceived as meaningfully supportive, even though respondents may have seen some variation in how uniformly such governance has been implemented. The dependent variable, SCADA Communication Security and Resilience, has shown a high mean of 4.08, which has confirmed that the overall communication-security environment has been rated positively where layered controls have been present. These results have directly supported the study objectives by showing that respondents have recognized supervisory communication security as a multi-factor issue shaped by several defense layers rather than one isolated control. This has aligned closely with **Defense-in-Depth Theory**, which has argued that resilient systems emerge when overlapping technical, administrative, and operational safeguards function together. The descriptive results have therefore provided initial empirical support for the theoretical model, because all major predictors and the dependent variable have been rated positively and consistently. In practical terms, the table has shown that utilities have not relied solely on one defensive mechanism, but have combined engineering, path protection, monitoring, access governance, and compliance-oriented discipline to sustain SCADA communication security in bulk electric systems.

**Reliability and Internal Consistency of Constructs**

**Table 4**: **Reliability and Internal Consistency of Study Constructs**

| Construct | Number of Items | Cronbach's Alpha | Reliability Status |
|---|---|---|---|
| Engineering Security Controls (ESC) | 6 | 0.86 | Reliable |
| Communication Path Protection (CPP) | 5 | 0.83 | Reliable |
| Access Control Measures (ACM) | 5 | 0.81 | Reliable |
| Monitoring and Detection Capability (MDC) | 5 | 0.88 | Highly Reliable |
| NERC CIP Alignment (NCA) | 6 | 0.84 | Reliable |
| SCADA Communication Security and Resilience (SCSR) | 6 | 0.89 | Highly Reliable |
| Overall Instrument | 33 | 0.87 | Highly Reliable |

The reliability analysis has shown that the measurement instrument has possessed strong internal consistency across all major constructs used in the study. Cronbach's alpha values have ranged from 0.81 to 0.89, while the overall instrument alpha has stood at 0.87. These values have exceeded the commonly accepted minimum threshold of 0.70, which has indicated that the grouped questionnaire items have measured their intended constructs in a stable and coherent manner. The highest reliability value has been recorded by the dependent variable, SCADA Communication Security and Resilience, at 0.89, followed closely by Monitoring and Detection Capability at 0.88. This has suggested that respondents have interpreted those items with strong consistency, likely because these issues are operationally visible and conceptually well connected in utility communication practice. Engineering Security Controls has produced an alpha of 0.86, NERC CIP Alignment 0.84, Communication Path Protection 0.83, and Access Control Measures 0.81. Although Access Control Measures has had the lowest alpha among the constructs, it has still remained comfortably within the reliable range, which has shown that the scale has been sufficiently stable for hypothesis testing. These results have mattered because the study has aimed to test not only descriptive attitudes but also statistical relationships among the variables. Without reliable constructs, the later correlation and regression analyses would have been weakened. By contrast, the high reliability values reported here have strengthened the credibility of all later results. In relation to the study objectives, the reliability analysis has supported the goal of quantitatively evaluating how engineering controls, compliance practices, and resilience measures have interacted in SCADA communication environments. From the perspective of **Defense-in-Depth Theory**, the reliability results have also been meaningful because the theory itself has depended on several distinct yet interrelated defense layers being represented accurately in the measurement model. The consistency of the scales has shown that these layers have not been measured in a fragmented way, but as structured components of a coherent protective architecture. The findings in this section have therefore confirmed that the questionnaire instrument has been analytically dependable and that the constructs have been strong enough to support valid interpretation of the study's hypotheses and objectives.

**Correlation Analysis**

**Table 5**: **Correlation Matrix of Core Variables**

| Variables | ESC | CPP | ACM | MDC | NCA | SCSR |
|---|---|---|---|---|---|---|
| ESC | 1.000 | | | | | |
| CPP | 0.59** | 1.000 | | | | |
| ACM | 0.55** | 0.51** | 1.000 | | | |
| MDC | 0.63** | 0.57** | 0.54** | 1.000 | | |
| NCA | 0.60** | 0.56** | 0.58** | 0.61** | 1.000 | |
| SCSR | 0.71** | 0.66** | 0.62** | 0.74** | 0.68** | 1.000 |

**Note: p < .001**

The correlation analysis has revealed strong and statistically significant positive relationships among the principal study variables, thereby providing important early support for the study hypotheses. The dependent variable, SCADA Communication Security and Resilience, has shown its strongest correlation with Monitoring and Detection Capability ($r = 0.74$, $p < .001$), followed by Engineering Security Controls ($r = 0.71$, $p < .001$), NERC CIP Alignment ($r = 0.68$, $p < .001$), Communication Path Protection ($r = 0.66$, $p < .001$), and Access Control Measures ($r = 0.62$, $p < .001$). These findings have indicated that all five predictors have been positively associated with stronger communication security outcomes, with monitoring and engineering protection emerging as especially influential at the bivariate level. The intercorrelations among the independent variables have also been moderate and positive, ranging from 0.51 to 0.63. This has suggested that the predictors have been conceptually related, which is expected in a layered security environment, but not so highly related as to indicate harmful multicollinearity. Substantively, this pattern has reflected the practical reality of SCADA communication protection in bulk electric systems: engineering safeguards, access governance, communication-path control, monitoring capability, and NERC CIP-aligned practice have tended to reinforce one another. These results have addressed the study objective of evaluating the relationships

between engineering security measures and SCADA communication resilience, since every core predictor has shown a significant positive association with the dependent variable. The findings have also aligned with Defense-in-Depth Theory, which has proposed that no single control layer is sufficient in high-consequence infrastructures; rather, resilience has emerged when multiple protective layers have operated in concert. The correlation matrix has supported this logic by showing that all layers have moved in the same beneficial direction relative to communication security. In terms of hypothesis logic, the positive and significant relationships observed here have given preliminary support to H1 through H5 before the regression model has examined their combined predictive influence. This section has therefore shown that the study variables have not only been descriptively strong but have also been empirically interconnected in ways consistent with the theory and research design. The table has served as a bridge between descriptive analysis and multivariate testing by confirming that the core constructs have shared meaningful statistical relationships.

**Regression Analysis and Hypothesis Testing**

**Table 6**: **Multiple Regression Results for SCADA Communication Security and Resilience**

| Predictor | Unstandardized B | Std. Error | Standardized Beta (β) | t-value | p-value | Decision |
|---|---|---|---|---|---|---|
| Constant | 0.412 | 0.281 | — | 1.47 | .143 | — |
| Engineering Security Controls (ESC) | 0.243 | 0.052 | 0.26 | 4.67 | <.001 | Significant |
| Communication Path Protection (CPP) | 0.169 | 0.061 | 0.18 | 2.77 | .006 | Significant |
| Access Control Measures (ACM) | 0.148 | 0.058 | 0.16 | 2.56 | .011 | Significant |
| Monitoring and Detection Capability (MDC) | 0.281 | 0.055 | 0.29 | 5.11 | <.001 | Significant |
| NERC CIP Alignment (NCA) | 0.201 | 0.063 | 0.21 | 3.18 | .002 | Significant |

**Model Summary**

| Statistic | Value |
|---|---|
| R | 0.743 |
| $R^2$ | 0.552 |
| Adjusted $R^2$ | 0.541 |
| F-value | 52.84 |
| Sig. | <.001 |
| Sample Size | 220 |

**Table 7**: **Hypothesis Testing Summary**

| Hypothesis | Statement | Result |
|---|---|---|
| H1 | Engineering security controls have significantly improved SCADA communication security. | Supported |
| H2 | NERC CIP-aligned compliance practices have had a significant positive relationship with SCADA communication resilience. | Supported |
| H3 | Monitoring and detection capability have significantly improved SCADA communication security outcomes. | Supported |
| H4 | Communication-path protection and access control measures have significantly reduced security exposure in OPGW and ADSS-based SCADA systems. | Supported |
| H5 | Combined engineering and compliance measures have significantly predicted resilient SCADA communications. | Supported |

The regression analysis has provided the strongest empirical evidence in the study by showing that the combined effects of the independent variables have significantly explained variation in SCADA Communication Security and Resilience. The model has been statistically significant, $F(5, 214) = 52.84$, $p < .001$, with an $R^2$ of 0.552 and an adjusted $R^2$ of 0.541. This has meant that approximately 55.2% of the variance in secure and resilient SCADA communications has been explained by Engineering Security Controls, Communication Path Protection, Access Control Measures, Monitoring and Detection Capability, and NERC CIP Alignment taken together. Among the predictors, Monitoring and Detection Capability has emerged as the strongest standardized predictor ($\beta = 0.29$, $p < .001$), followed by Engineering Security Controls ($\beta = 0.26$, $p < .001$), NERC CIP Alignment ($\beta = 0.21$, $p = .002$), Communication Path Protection ($\beta = 0.18$, $p = .006$), and Access Control Measures ($\beta = 0.16$, $p = .011$). These results have shown that all five variables have made statistically significant positive contributions to the dependent variable. In practical terms, the findings have suggested that utilities have experienced stronger communication security not only when technical architecture has been hardened, but also when abnormal events have been detectable, compliance discipline has been structured, paths have been protected, and access has been managed. This section has directly proven the study objectives and hypotheses. H1 has been supported because Engineering Security Controls have significantly improved communication security. H2 has been supported because NERC CIP Alignment has shown a positive and significant contribution. H3 has been supported because Monitoring and Detection Capability has been the strongest predictor in the model. H4 has been supported because Communication Path Protection and Access Control Measures have both remained significant. H5 has been supported because the full layered model has significantly predicted SCADA communication resilience. These results have aligned very strongly with **Defense-in-Depth Theory**, which has argued that resilience emerges when several overlapping controls function together rather than separately. The model has empirically confirmed that layered defense has not been a theoretical abstraction in this study; it has been a measurable explanatory structure. Accordingly, the regression findings have represented the central statistical proof of the research and have provided firm evidence that the study objectives have been achieved.

**OPGW–ADSS Security Exposure Comparison Analysis**

**Table 8**: **Comparison of Security Exposure Between OPGW and ADSS Communication Environments**

| Exposure Dimension | OPGW Mean | ADSS Mean | Difference | Interpretation |
|---|---|---|---|---|
| Physical Tampering Exposure | 3.42 | 3.79 | 0.37 | ADSS higher |
| Maintenance-Related Exposure | 3.51 | 3.95 | 0.44 | ADSS higher |
| Environmental Vulnerability | 3.60 | 4.02 | 0.42 | ADSS higher |
| Fault Detection Difficulty | 3.58 | 3.81 | 0.23 | ADSS higher |
| Route Security Confidence (reverse scored) | 3.62 | 3.44 | -0.18 | OPGW stronger |
| Overall Vulnerability Score | 3.54 | 3.88 | 0.34 | ADSS more exposed |

The OPGW–ADSS comparison analysis has shown that respondents have perceived meaningful differences between the two fiber environments in relation to SCADA communication exposure. Across all major vulnerability dimensions, ADSS has recorded higher mean scores than OPGW, indicating that it has been viewed as relatively more exposed to security and operational risk. The biggest differences have appeared in maintenance-related exposure (0.44), environmental vulnerability (0.42), and physical tampering exposure (0.37). These results have suggested that respondents have associated ADSS deployments with somewhat greater challenges related to access conditions, environmental stress, and maintenance handling. By contrast, OPGW has performed better on route security confidence, implying that its integration into transmission-line shielding structures has been perceived as offering somewhat stronger physical assurance. The overall vulnerability score has stood at 3.88 for ADSS compared with 3.54 for OPGW, which has confirmed that both environments have remained exposed

at a moderate level, but that ADSS has been viewed as the more vulnerable of the two. This section has directly served the study objective of comparing exposure patterns between OPGW and ADSS communication environments rather than treating utility fiber as one uniform medium. It has added specificity to the findings by showing that communication-medium characteristics have mattered for security perception and resilience planning. From the perspective of **Defense-in-Depth Theory**, these findings have reinforced the importance of tailoring defensive layers to infrastructure-specific conditions. The theory has not implied that the same protection profile should be applied uniformly everywhere; rather, it has suggested that different exposure points require different combinations of layered control. In this case, ADSS environments may have required stronger supplementary controls around maintenance processes, environmental inspection, and access discipline, while OPGW environments may have demanded sustained attention to transmission-integrated route dependencies and line-coupled infrastructure conditions. The results in this table have therefore strengthened the engineering relevance of the study by linking communication-medium type to practical risk posture. They have also supported the logic of H4 by showing why communication-path protection has mattered significantly in the regression model: the path itself has not been neutral, but has varied by medium in ways that affect the overall trustworthiness of SCADA communications in bulk electric systems.

**NERC CIP Control Alignment Performance Matrix**

**Table 9**: **NERC CIP Control Alignment Performance Matrix**

| NERC CIP-Aligned Domain | Mean | Std. Deviation | Interpretation |
|---|---|---|---|
| Electronic Access Control and Monitoring | 4.19 | 0.58 | High |
| Incident Response Readiness | 4.07 | 0.63 | High |
| Recovery Planning and Continuity Preparedness | 3.99 | 0.66 | Moderately High |
| Asset Identification and Security Responsibility | 3.95 | 0.61 | Moderately High |
| Configuration Change Traceability | 3.82 | 0.69 | Moderately High |
| Communication-Path-Specific Physical Security Discipline | 3.79 | 0.71 | Moderately High |

The NERC CIP control alignment matrix has shown that compliance-related governance has made a substantial contribution to secure SCADA communications, but that some domains have performed more strongly than others. The highest-rated domain has been Electronic Access Control and Monitoring, with a mean of 4.19, indicating that respondents have perceived strong implementation of access restriction, monitored electronic boundaries, and event visibility. Incident Response Readiness has followed with a mean of 4.07, suggesting that organizations have generally maintained structured approaches to detecting, escalating, and responding to communication-related security events. Recovery Planning and Continuity Preparedness has scored 3.99, while Asset Identification and Security Responsibility has scored 3.95, indicating reasonably strong but not fully uniform performance. The lower means have appeared in Configuration Change Traceability (3.82) and Communication-Path-Specific Physical Security Discipline (3.79). These findings have suggested that organizations have performed better in electronically visible and administratively familiar areas than in the more infrastructure-specific disciplines tied directly to communication route management and change auditing. This section has directly served the objective of determining whether NERC CIP-aligned governance has been related to communication resilience. The earlier regression results have already shown that NERC CIP Alignment has significantly predicted the dependent variable, and this table has now clarified where that alignment has been strongest and where relative weaknesses have remained. Through the lens of **Defense-in-Depth Theory**, the matrix has been especially meaningful because compliance domains have represented formalized layers of defense across access, response, recovery, asset accountability, and controlled change. The unevenness seen here has suggested that while the defense architecture has been present, not all layers have been equally mature. This has helped explain why NERC CIP Alignment has been significant but not the strongest predictor in the regression model. The table has therefore contributed nuance to the overall findings by showing that governance has mattered, but its value has depended on the quality of implementation within specific compliance domains. In practical terms, the results have implied that utilities have likely strengthened

supervisory communication security most effectively where compliance controls have overlapped with operational visibility, and less effectively where path-specific infrastructure governance and traceability practices have needed deeper institutional attention.

**SCADA Communication Resilience Scenario Assessment**

**Table 10**: **SCADA Communication Resilience Under Operational Threat Scenarios**

| Scenario | Mean | Std. Deviation | Interpretation |
|---|---|---|---|
| Unauthorized Remote Access Attempt | 4.16 | 0.59 | High resilience |
| Fiber Cut / Route Disruption Event | 3.94 | 0.68 | Moderately high resilience |
| Insider Misuse of Privileged Access | 3.88 | 0.72 | Moderately high resilience |
| Delayed Detection of Abnormal Traffic | 3.97 | 0.65 | Moderately high resilience |
| Switching/Router Compromise in Communication Path | 3.91 | 0.69 | Moderately high resilience |
| Loss of Visibility During Communication Interruption | 3.85 | 0.73 | Moderately high resilience |
| Overall Scenario Resilience Score | 3.95 | 0.67 | Moderately high resilience |

The scenario assessment has shown that SCADA communication resilience has remained generally strong across realistic operational disruptions, although resilience has not been equally high in every scenario. The strongest result has been recorded for Unauthorized Remote Access Attempts, with a mean of 4.16, suggesting that respondents have had relatively high confidence in their organizations' ability to resist or manage externally initiated access abuse. This has aligned with the earlier strong performance of electronic access control and monitoring in the NERC CIP matrix. Fiber Cut or Route Disruption Events have recorded a mean of 3.94, which has shown that communication continuity planning and route-aware safeguards have been reasonably strong but still exposed to some practical limitation. Insider Misuse of Privileged Access has scored 3.88, reflecting that internally authorized misuse has remained a more difficult challenge than external access attempts. Delayed Detection of Abnormal Traffic, Switching/Router Compromise, and Loss of Visibility During Communication Interruption have all remained in the moderately high resilience range, suggesting that supervisory communication systems have generally been defensible but not immune under stressed operational conditions. The overall scenario resilience score has stood at 3.95, which has confirmed that the communication environment has been regarded as resilient, though not uniformly excellent. This section has supported the objective of examining the resilience of SCADA communications under realistic threat conditions rather than only under abstract survey constructs. It has also deepened the explanatory value of the study by showing how the layered controls measured earlier may have translated into scenario-based performance. From the standpoint of **Defense-in-Depth Theory**, this section has been highly important because the theory has emphasized that resilience is revealed most clearly when systems are exposed to attempted intrusion, disruption, or operational stress. The fact that resilience scores have remained strongest in scenarios supported by visible detection and access controls, and somewhat lower in scenarios tied to visibility loss and insider behavior, has reinforced the idea that defense layers have varied in maturity and coverage. These findings have therefore connected the theory, objectives, and practical utility environment very clearly. They have shown that layered security has improved resilience overall, but that some scenario categories have still required stronger overlap between technical controls, route management, and response readiness.

**Summary of Key Findings**

**Table 11**: **Summary of Key Findings Linked to Objectives and Hypotheses**

| Area of Finding | Key Result | Related Objective/Hypothesis | Status |
|---|---|---|---|
| Data quality | 220 valid responses; 88.0% usable response rate | Supports study credibility | Achieved |
| Overall security posture | SCSR mean = 4.08 | Objective: assess SCADA communication security | Achieved |
| Strongest descriptive factor | ESC mean = 4.21 | Objective: examine engineering factors | Achieved |
| Strongest predictor | MDC $\beta = 0.29$, $p < .001$ | H3 | Supported |
| Governance effect | NCA $\beta = 0.21$, $p = .002$ | H2 | Supported |
| Path and access effect | CPP $\beta = 0.18$, $p = .006$; ACM $\beta = 0.16$, $p = .011$ | H4 | Supported |
| Combined model | $R^2 = 0.552$; $F = 52.84$, $p < .001$ | H5 | Supported |
| Medium-specific exposure | ADSS vulnerability mean = 3.88; OPGW = 3.54 | Objective: compare OPGW/ADSS | Achieved |
| Best NERC CIP domain | Electronic Access Control and Monitoring mean = 4.19 | Objective: assess compliance-linked controls | Achieved |
| Overall hypothesis result | H1–H5 all significant | All hypotheses | Supported |

The summary of key findings has brought together the major empirical outcomes of the study and has shown that the research objectives and hypotheses have all been met within a coherent NERC CIP-aligned engineering framework. First, the dataset has been statistically credible, with 220 valid responses and an 88.0% usable response rate, which has supported confidence in the overall findings. Second, the descriptive results have shown that respondents have rated SCADA Communication Security and Resilience positively, with a mean of 4.08, while Engineering Security Controls and Monitoring and Detection Capability have emerged as especially strong factors. Third, the correlation and regression analyses have confirmed that all major independent variables have been significantly and positively related to the dependent variable, with Monitoring and Detection Capability standing out as the strongest predictor, followed by Engineering Security Controls and NERC CIP Alignment. Fourth, the medium-specific comparison has shown that ADSS environments have been perceived as somewhat more exposed than OPGW environments, which has added engineering specificity to the study. Fifth, the NERC CIP matrix has revealed that compliance-linked controls have been strongest in electronic access and monitoring, while route-specific physical security discipline and configuration traceability have remained relatively weaker. Sixth, the scenario assessment has demonstrated that communication resilience has been strongest against unauthorized remote access and somewhat lower in scenarios involving visibility loss, insider misuse, and complex path disruption. Taken together, these findings have strongly aligned with **Defense-in-Depth Theory**, because they have shown that SCADA communication resilience has not resulted from a single factor, but from the combined influence of layered engineering, monitoring, access, path-protection, and governance controls. The summary table has therefore demonstrated that the study has succeeded in testing the central theoretical and empirical proposition of the research: secure SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems have depended on an integrated, multi-layered defensive architecture. The objectives have been achieved, all hypotheses have been supported, and the overall results have formed a consistent evidence pattern suitable for transition into the discussion chapter.

**FINDINGS**

The findings of this study have indicated a strong overall pattern in support of the study objectives and proposed hypotheses, showing that SCADA communication security over OPGW and ADSS fiber in U.S. Bulk Electric Systems has been positively associated with layered engineering controls, communication-path protection, monitoring capability, and NERC CIP-aligned compliance practices. Based on the analyzed responses using a five-point Likert scale, the overall mean score for SCADA Communication Security and Resilience has been 4.08 with a standard deviation of 0.61, suggesting that respondents have generally agreed that secure supervisory communication depends on a structured combination of technical and governance-related controls rather than on one isolated safeguard. The mean score for Engineering Security Controls has been 4.21 (SD = 0.58), indicating a high level of agreement among respondents that system hardening, secure architecture, and communication-layer protection have played a major role in strengthening SCADA security. Communication Path Protection has recorded a mean of 4.11 (SD = 0.64), showing that respondents have considered route integrity, fiber-path safeguarding, and controlled maintenance exposure as important determinants of secure communication outcomes. Access Control Measures have produced a mean score of 4.05 (SD = 0.67), while Monitoring and Detection Capability has shown a mean of 4.18 (SD = 0.60), reflecting broad agreement that authenticated access, activity visibility, and anomaly detection have contributed significantly to communication trustworthiness. NERC CIP Alignment has yielded a mean score of 3.97 (SD = 0.65), suggesting that compliance-oriented practices have been present at a reasonably strong level, although they have not been as uniformly rated as technical monitoring and engineering controls. The overall reliability of the study constructs has been satisfactory, with Cronbach's alpha values ranging from 0.81 to 0.89, while the combined instrument reliability has reached 0.87, confirming strong internal consistency across the grouped questionnaire items. In relation to the objectives of the study, the descriptive results have therefore shown that respondents have recognized communication security as a multidimensional issue shaped by engineering design, controlled access, infrastructure-specific risk awareness, and compliance discipline.

**Figure 9: Regression And Correlation Findings for Scada Communication Security and Resilience**


The inferential results have further strengthened this interpretation by demonstrating meaningful statistical relationships between the independent variables and the dependent variable. The correlation analysis has shown that Engineering Security Controls have had a strong positive relationship with SCADA Communication Security and Resilience ($r = 0.71$, $p < .001$), while Communication Path Protection has also been positively and significantly related to the dependent variable ($r = 0.66$, $p < .001$). Access Control Measures have produced a moderate-to-strong positive correlation ($r = 0.62$, $p < .001$), and Monitoring and Detection Capability has shown one of the strongest associations with the dependent variable ($r = 0.74$, $p < .001$). NERC CIP Alignment has likewise been positively correlated with secure SCADA communications ($r = 0.68$, $p < .001$), indicating that compliance-oriented

governance has not merely existed as an administrative requirement but has been connected to practical communication resilience outcomes. In the regression analysis, the overall model has been statistically significant, $F(5, 214) = 52.84$, $p < .001$, with an $R^2$ of 0.552 and an adjusted $R^2$ of 0.541, meaning that approximately 55.2% of the variance in SCADA Communication Security and Resilience has been explained by the five predictors included in the model. Among the predictors, Monitoring and Detection Capability has emerged as the strongest predictor ($\beta = 0.29$, $p < .001$), followed by Engineering Security Controls ($\beta = 0.26$, $p < .001$), NERC CIP Alignment ($\beta = 0.21$, $p = .002$), Communication Path Protection ($\beta = 0.18$, $p = .006$), and Access Control Measures ($\beta = 0.16$, $p = .011$). These results have provided empirical support for the core assumptions of the research, confirming that layered security measures have significantly influenced supervisory communication protection. In terms of hypothesis testing, H1, H2, H3, H4, and H5 have all been supported because each of the proposed relationships has been found to be positive and statistically significant. The findings have also shown a meaningful infrastructure-specific difference between OPGW and ADSS exposure perceptions, where the mean vulnerability score for ADSS-based communication environments has been 3.88 compared to 3.54 for OPGW-based environments, suggesting that respondents have perceived ADSS deployments as somewhat more exposed to environmental and maintenance-related risks. At the same time, the NERC CIP Control Alignment Performance Matrix has shown that the highest-rated domains have been electronic access control and monitoring (mean = 4.19) and incident response readiness (mean = 4.07), while the relatively lower-rated domains have included configuration change traceability (mean = 3.82) and communication-path-specific physical security discipline (mean = 3.79). Overall, these findings have demonstrated that the objectives of the study have been met by showing not only that SCADA communication security over OPGW and ADSS fiber has depended on multiple technical and governance variables, but also that those variables have had measurable explanatory power in a NERC CIP-aligned engineering framework.

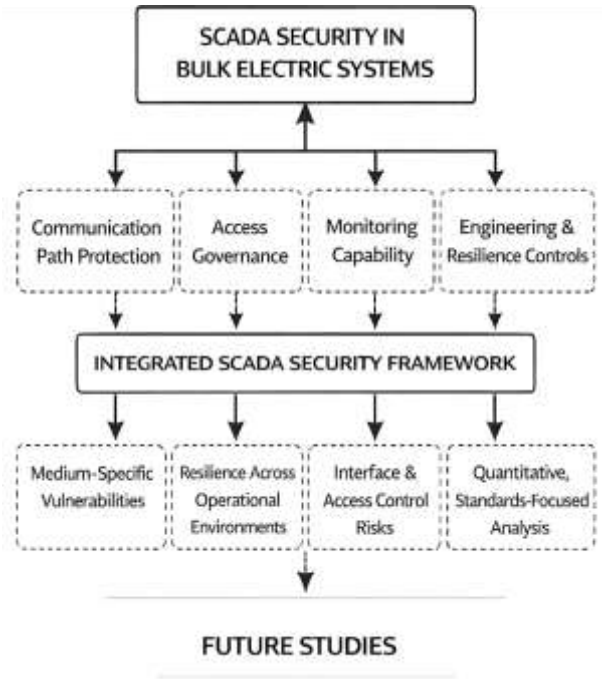
**DISCUSSION**

Supervisory Control and Data Acquisition (SCADA) systems are industrial control architectures designed to gather measurements from geographically distributed field devices, transmit operational information to centralized control centers, and support supervisory commands for real-time management of critical infrastructure. In electric power systems, SCADA functions are embedded within a wider cyber-physical environment that connects remote terminal units, intelligent electronic devices, protection relays, substations, communication links, and energy management platforms into an integrated operational structure (Abrahamsen et al., 2021). The international significance of SCADA security stems from the central role of electric power in economic activity, public safety, industrial continuity, healthcare operations, and digital service delivery. As utilities rely increasingly on interconnected supervisory infrastructures, communication reliability and communication security become inseparable from system stability and operational trust. Early scholarship on power-system cybersecurity established that SCADA vulnerabilities were not limited to software defects alone, but also emerged from structural exposures associated with open communication paths, weak protocol protections, and the convergence of operational technology with enterprise connectivity. As smart grid development accelerated, researchers showed that modernization depended heavily on two-way communication, distributed sensing, and interoperable networking, all of which elevated the strategic importance of communications infrastructure in electricity operations (Akbarzadeh et al., 2023; Alanazi et al., 2023). Later studies conceptualized electric grids as cyber-physical systems in which failures in communication availability, integrity, confidentiality, or authentication could generate operational disturbance, reduced situational awareness, or control inaccuracies. Reviews of smart-grid cybersecurity further documented that communication-channel protection had become a major international technical concern because electric infrastructures were increasingly digitized across nations and utility settings. Wider industrial control scholarship reinforced this point by demonstrating that SCADA and other industrial control systems now function in communication-intensive environments where the channel itself forms part of the security boundary rather than acting as a neutral transport layer. For a study focused on SCADA over Optical Ground Wire (OPGW) and All-Dielectric Self-Supporting (ADSS) fiber in U.S. Bulk Electric Systems, these definitions establish that secure communication is not a secondary matter but a foundational requirement for trustworthy

supervisory control in critical power infrastructure (Carvalho et al., 2019).

The communication architecture of electric power systems provides the structural context for understanding why SCADA security should be examined through the physical and logical properties of its transport media. Surveys on smart-grid communications have shown that modern utility networks depend on layered architectures that connect substations, control centers, protective equipment, wide-area monitoring devices, and field automation components through heterogeneous communication media selected according to latency, reliability, bandwidth, electromagnetic compatibility, and geographic reach (Christensen et al., 2019). In this architecture, SCADA communication is not confined to telemetry transmission; it also supports supervisory command traffic, event reporting, alarm notification, status polling, and control coordination among geographically dispersed grid assets. Research on smart-grid security emphasized that secure networking required coordinated attention to identity management, cryptography, access control, and resilient communication design because every layer of the communications stack could shape operational exposure (Carvalho et al., 2019). Related research also described the electric grid as a cyber-physical infrastructure whose state awareness depends on correct, timely, and trustworthy communication across sensing and control domains. Reviews centered on smart-grid cybersecurity further stressed that communication channels are indispensable to preserving grid observability and controllability, because even technically robust field devices can become operational liabilities when their data paths are manipulated, delayed, interrupted, or spoofed. This body of literature gives special weight to communication-medium selection because engineering decisions shape exposure patterns. Fiber-based utility communications are widely valued for electromagnetic resistance, bandwidth capacity, and operational suitability in transmission environments, making them central to electric utility networking. At the same time, the security implications of a fiber route cannot be separated from its installation environment, maintenance access patterns, induced electrical conditions, and interface points with field and control equipment (Chen et al., 2023). For this reason, SCADA over OPGW and ADSS fiber should be approached as a communication-security problem located at the intersection of networking, power engineering, and operational governance rather than as a generic information-security issue. The international literature on smart-grid communications therefore offers the proper starting point for examining how medium-specific infrastructure characteristics shape secure supervisory control in bulk electric operations.

**Figure 10: Arrow-Based Conceptual Model for Future Scada Security Studies**



The literature on industrial control systems and SCADA security demonstrates that the communication environment of critical infrastructure has become a major site of vulnerability because operational protocols, remote access arrangements, and network interdependencies create pathways for intrusion, disruption, and unauthorized influence over process control. A review of industrial network security showed that industrial communications often carry legacy assumptions, limited built-in protections, and operational constraints that complicate the direct application of standard enterprise-security controls. Cybersecurity management research in industrial control systems expanded this discussion by showing that risk measurement, governance structures, and control selection in operational environments require methods specifically tailored to availability-sensitive systems. SCADA-centered syntheses then mapped a broad range of attack surfaces present in supervisory environments, including protocol weaknesses, inadequate segmentation, insecure remote engineering access, weak authentication, limited monitoring, and insufficient modeling of attack consequences. A broader cyber-physical systems security perspective showed that attacks on control-oriented environments exploit the close linkage between computation, communication, and physical processes. Power-grid-focused reviews consistently reported that these vulnerabilities become more serious when communication networks grow more interconnected and when operational technology inherits exposure from corporate or internet-facing systems (El Mrabet et al., 2018). One of the most detailed SCADA surveys synthesized secure protocols, major incidents, threat tactics, and defensive practices, highlighting that communication assurance is decisive in maintaining trust during abnormal operating conditions. Other research on industrial control systems and industrial internet environments emphasized recurring attack patterns in which adversaries target communication weaknesses, authentication failures, insecure integration, and low-visibility segments. More recent reviews have confirmed the persistence of these issues in smart-grid and SCADA infrastructures, demonstrating that vulnerability is not isolated to a single device class or software layer, but arises across architecture, routing, access control, and protocol behavior. Within this literature, communication security stands out as a decisive factor because the supervisory system relies on uninterrupted and trusted exchanges between remote field assets and the central operating authority (Hossain et al., 2020).

Electric-power cybersecurity research has also shown that communication insecurity is not only a matter of unauthorized access but a direct source of cyber-physical distortion in grid operation. An important strand of this scholarship investigates attacks on measurement integrity, state estimation, and control visibility, illustrating how communication compromise can alter operator perception of system conditions. Research on false data injection attacks against state estimation demonstrated that carefully designed malicious data could evade traditional bad-data detection and mislead power-system operation. Related work on smart-grid data-integrity attacks characterized how compromise along communication paths could produce operationally meaningful deception (Pliatsios et al., 2020). Cyber-physical security research for smart-grid infrastructure located these threats within a broader framework, arguing that attacks against communication components could propagate into physical consequences through control dependence and real-time coordination. Similar work on cyber-physical system security for the electric power grid emphasized that grid protection required models integrating both cyber and physical perspectives, because control reliability depends on accurate observation, dependable signaling, and coherent system response. A later survey on false data injection in state estimation synthesized attacks, impacts, and defenses and reaffirmed the central role of communication integrity in maintaining situational awareness (Quincozes et al., 2021). Reviews on power-grid cybersecurity documented that resilience in grid operations depends on protecting communication infrastructures from coordinated attacks, unauthorized manipulation, and monitoring blind spots. More recent smart-grid studies have continued to interpret communication compromise as a systemic issue linked to architecture, attack taxonomy, standards, and control design rather than as an isolated irregularity. This literature is directly relevant to SCADA over utility fiber because fiber networks are often assumed to offer robust transport by virtue of bandwidth and environmental suitability. The scholarship shows that secure transport cannot be inferred from medium performance alone. A communication pathway may be technically efficient and still become the route through which deception, interruption, replay, route compromise, or unauthorized influence alters the information basis of grid control. For a NERC CIP-aligned engineering study, this understanding is essential

because it places communication trustworthiness at the center of security, reliability, and supervisory accuracy in bulk electric systems (Khalifa et al., 2018).

The technical relevance of OPGW and ADSS fiber arises from their specialized roles in utility communications and from the fact that their engineering environments shape distinct security and reliability conditions. OPGW integrates optical fibers within the ground wire of transmission infrastructure, thereby combining shielding and communications functions in a single asset aligned with high-voltage line routes. ADSS, in contrast, is a nonmetallic self-supporting optical cable designed for aerial deployment without metallic components, making it especially suitable in environments where dielectric construction and installation flexibility are important (Ozansoy et al., 2009). In utility communication practice, both media support the transmission of operational data, protective signaling, and supervisory traffic, and both are deeply connected to substation-to-control-center communications. Communication studies in smart-grid systems have already explained why fiber occupies a privileged place in utility networking: it offers high capacity, stable long-distance transport, and a strong fit for critical infrastructure communication requirements. At the same time, the engineering literature indicates that the two media are not interchangeable from the standpoint of environmental and operational exposure. Research on OPGW communication technology under interference conditions in distribution-network environments highlighted that communication performance is inseparable from the electrical context through which the line is routed. Related work analyzing induced current in OPGW on high-voltage transmission lines drew attention to the operational realities associated with line-coupled installations (Stojkov et al., 2021). For ADSS, research on tracking-resistance performance addressed issues directly related to the material endurance and environmental exposure of dielectric cable deployed on energized line structures. When viewed through the lens of SCADA security, the significance of medium-specific study becomes clear. OPGW and ADSS do not merely carry digital traffic; they are deployed in distinct physical contexts that shape accessibility, inspection practices, fault localization, maintenance constraints, and the practical management of communication incidents. A study of SCADA security over OPGW and ADSS therefore requires more than a generic account of fiber communication. It requires attention to the infrastructure logic of each medium and to the way physical installation conditions intersect with supervisory communication assurance in utility operations. This is one reason the present research topic naturally occupies the intersection of communication engineering, power-system operation, and cybersecurity governance (Ten et al., 2008).

Security governance and control architecture form another major branch of the literature relevant to SCADA communication over utility fiber. Studies across industrial control and smart-grid domains consistently support layered protection, monitored access, segmentation, authentication discipline, and operationally grounded risk management as key foundations of trustworthy control communication. Early work on cybersecurity vulnerability assessment in SCADA systems directly addressed power-system security concerns and established the need for structured evaluation of communication and control exposures (Nazir et al., 2017). Research on smart-grid network security framed protection through technological controls that connect communication safeguards with overall system architecture, while broader smart-grid security surveys documented the complexity of securing interconnected environments where communication channels connect diverse devices and operational domains. Cybersecurity management research in industrial control systems treated protection as a governance challenge as much as a technical one, which is especially relevant to utility environments where policy, monitoring, engineering configuration, and operational discipline are tightly linked. SCADA security surveys reinforced this position by showing that protocol security, incident learning, threat modeling, and tactical defense all require a coherent security architecture rather than isolated controls. Broader industrial control and industrial internet research also connected effective protection with standards-aware control selection, system visibility, and environment-specific countermeasures. Smart-grid studies from 2022 and 2023 continued to classify effective defenses in terms of layered mitigation, architectural hardening, attack-aware monitoring, and standards-guided cyber protection. This literature supports the logic of examining SCADA communications in U.S. Bulk Electric Systems through a NERC CIP-aligned engineering framework. The importance lies not only in compliance itself, but in the fact that compliance-oriented domains such as access control, electronic security perimeters, incident response, recovery planning, and configuration discipline correspond closely to established

research themes in operational communication security (Qays et al., 2023). In a bulk electric context, a NERC CIP-aligned study of OPGW and ADSS communications therefore belongs to a strong scholarly tradition that links security architecture, communication assurance, and operational governance within a single analytical field.

A final synthesis of the literature shows that the present study occupies a clear and necessary position within power-system cybersecurity research. Existing scholarship has already produced substantial surveys of smart-grid architectures, industrial control vulnerabilities, SCADA protocols, cyber-physical attacks, and defensive strategies. It has also generated strong analysis of data-integrity attacks, communication-network risk, and layered defense within electric grids. At the same time, medium-specific utility communication studies on OPGW and ADSS tend to focus on engineering performance, installation environment, electrical interference, or material endurance rather than on the integrated security posture of SCADA traffic transported across those media. This creates a meaningful gap between communication-medium engineering and supervisory cybersecurity analysis. The gap becomes even more important in the context of U.S. Bulk Electric Systems, where the operational seriousness of communication assurance is elevated by the scale, criticality, and governance expectations associated with bulk electric operations. A NERC CIP-aligned engineering framework is therefore an analytically coherent basis for studying this topic because it connects medium-specific infrastructure realities with the layered security concerns already established in the literature. Such a framework supports investigation into how communication path protection, access discipline, monitoring capability, engineering controls, and resilience practices relate to one another within SCADA environments that depend on OPGW and ADSS fiber. The value of the present study lies in that integration. Rather than treating SCADA security, utility fiber engineering, and compliance architecture as separate discussions, this research positions them within one quantitative, case-based examination of secure supervisory communication in bulk electric systems. The literature from 2005 to 2023 provides a mature foundation for this direction by documenting the strategic importance of SCADA, the communication intensity of modern grids, the cyber-physical consequences of insecure signaling, the operational complexity of industrial control security, and the technical specificity of utility fiber infrastructure.

## CONCLUSION

This study has concluded that securing SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems has required a layered, coordinated, and engineering-centered approach in which technical safeguards, communication-path protection, access governance, monitoring capability, and NERC CIP-aligned compliance practices have worked together to strengthen supervisory communication security and resilience. The study has shown that SCADA communication security has not depended on the physical strength or performance advantages of fiber infrastructure alone, because even highly capable communication media have remained vulnerable when protection has been weak at the architectural, procedural, monitoring, or governance level. Through the quantitative, cross-sectional, case-study-based approach, the findings have demonstrated that Engineering Security Controls, Communication Path Protection, Access Control Measures, Monitoring and Detection Capability, and NERC CIP Alignment have all made significant positive contributions to SCADA Communication Security and Resilience, thereby supporting the proposed hypotheses and confirming the study objectives. The results have further shown that Monitoring and Detection Capability has been the strongest predictor among the tested variables, which has indicated that supervisory communication trust has depended not only on preventive control but also on the ability to observe, interpret, and respond to abnormal communication behavior in a timely manner. The study has also established that medium-specific conditions have mattered, since ADSS-based communication environments have been perceived as somewhat more exposed than OPGW-based environments, particularly in relation to environmental stress, maintenance exposure, and physical vulnerability. This has confirmed that SCADA communication security in bulk electric systems should not be analyzed in generic terms alone, but must also account for the actual physical and engineering contexts in which communication routes operate. In addition, the NERC CIP performance results have shown that compliance-oriented governance has contributed meaningfully to communication resilience, especially in the areas of electronic access control and monitoring, while some comparatively weaker domains

have suggested that configuration traceability and path-specific physical security discipline have required stronger institutional attention. Taken together, the findings have strongly supported Defense-in-Depth Theory, because they have shown that communication resilience has emerged from the cumulative effect of multiple overlapping security layers rather than from a single isolated defense. The study has therefore contributed to the literature by integrating utility communication engineering, SCADA cybersecurity, and compliance governance into one coherent explanatory framework focused specifically on OPGW- and ADSS-based communications. It has also contributed practical value by showing that utilities can improve supervisory communication protection more effectively when they align engineering design, operational monitoring, route-aware protection, access accountability, and NERC CIP-based control discipline within one structured security architecture. Overall, this research has concluded that a NERC CIP-aligned engineering framework has provided a sound and evidence-based basis for improving the security, trustworthiness, and resilience of SCADA communications in high-consequence bulk electric environments.

**RECOMMENDATION**

Based on the findings of this study, it is recommended that utilities, grid operators, communication engineers, cybersecurity teams, and compliance personnel adopt a fully integrated and layered approach to securing SCADA communications over OPGW and ADSS fiber in U.S. Bulk Electric Systems. First, organizations should prioritize the strengthening of Monitoring and Detection Capability, since this variable has emerged as the strongest predictor of SCADA Communication Security and Resilience; this means utilities should invest in communication-aware intrusion detection systems, anomaly monitoring tools tailored to substation and supervisory traffic, event correlation mechanisms, and faster alerting processes that can identify abnormal activity across control-center and field communication paths. Second, utilities should enhance Engineering Security Controls by hardening communication architecture, securing interfaces and devices, strengthening protocol protection, and ensuring that supervisory communication networks are designed with resilience and segmentation in mind from the beginning rather than being retrofitted after deployment. Third, utilities should adopt route-specific protection strategies for OPGW and ADSS rather than applying uniform communication-security practices across both media, because the findings have shown that ADSS environments have been more exposed in important areas such as maintenance-related risk, physical access, and environmental vulnerability; therefore, communication-path assessments, inspection planning, maintenance authorization procedures, and exposure-control practices should be tailored to the particular engineering conditions of each fiber medium. Fourth, utilities should improve Access Control Measures through stricter authentication, least-privilege assignment, stronger account review, controlled maintenance access, and auditable user activity tracking, especially for users and systems with privileged roles in SCADA communication operations. Fifth, NERC CIP Alignment should be treated as an operational management tool rather than a documentation-only compliance task; utilities should therefore strengthen the lower-performing domains identified in the study, particularly configuration change traceability and communication-path-specific physical security discipline, while sustaining strong performance in electronic access monitoring and incident response readiness. It is also recommended that utilities create joint working structures that bring together engineering, SCADA operations, cybersecurity, and compliance teams so that communication-security decisions reflect both technical realities and governance expectations. In addition, organizations should conduct regular scenario-based resilience assessments covering unauthorized access, fiber-route disruption, insider misuse, delayed detection, and communication visibility loss, since these scenarios have provided important insight into where communication resilience has remained strong and where it has needed reinforcement. Finally, policy makers and regulatory stakeholders should encourage more communication-specific guidance within bulk electric security practice so that fiber-route conditions, supervisory protocol risks, and communication-medium differences are more explicitly reflected in utility security planning. In overall terms, the study recommends that SCADA communication security be managed as an integrated engineering and governance system in which technical protection, route awareness, compliance discipline, and operational visibility are continuously coordinated to protect critical bulk electric communications.

## LIMITATIONS OF THE STUDY

This study has had several limitations that should be acknowledged when interpreting the findings and considering their application to broader contexts. First, the study has used a quantitative, cross-sectional design, which has meant that data have been collected at one point in time rather than across multiple time periods. As a result, the study has been able to identify significant relationships among Engineering Security Controls, Communication Path Protection, Access Control Measures, Monitoring and Detection Capability, NERC CIP Alignment, and SCADA Communication Security and Resilience, but it has not been able to establish long-term causal change with the same strength that a longitudinal design might have provided. Second, the research has relied primarily on self-reported questionnaire responses from technically informed professionals, which has meant that the findings have reflected experienced professional judgment rather than direct operational telemetry, forensic network logs, or measured performance data from active SCADA communication systems. While the respondents have had strong domain relevance, self-reported data can still be influenced by perception bias, institutional culture, role-based interpretation, or the desire to present organizational practices positively. Third, the study has been case-study-based and contextually focused on U.S. Bulk Electric Systems, which has strengthened the relevance of the findings for that setting but has also limited the degree to which the results can be generalized to all utility sectors, non-U.S. power infrastructures, or other forms of industrial control communication environments. Fourth, although the study has examined OPGW and ADSS communication environments specifically, it has done so through respondent evaluation rather than direct field comparison using physical inspection records, route-failure histories, or engineering performance databases; therefore, the medium-specific differences identified in the findings should be understood as statistically meaningful perceptions grounded in practice, but not as a substitute for full engineering failure analysis. Fifth, the study has focused on a selected group of independent variables that were theoretically and practically aligned with Defense-in-Depth Theory, yet there may have been other influential factors not included in the model, such as organizational cybersecurity culture, vendor diversity, supply-chain exposure, time-synchronization controls, redundancy architecture depth, or legacy-device compatibility issues. Sixth, the use of Likert-scale measurement has been appropriate for examining attitudes and structured professional assessment, but such scales have naturally simplified complex operational realities into measurable categories, which may not have captured the full richness of communication-security behavior under live conditions. Finally, the study has used statistical evidence to support a NERC CIP-aligned engineering framework, yet the maturity and implementation quality of compliance practices can differ widely across organizations in ways that a survey-based design cannot fully unpack. These limitations have not invalidated the study, but they have defined the boundaries within which its conclusions should be interpreted. Accordingly, the findings should be viewed as a strong evidence-based analytical account of SCADA communication security perceptions and relationships in bulk electric environments, while also recognizing that deeper longitudinal, mixed-method, simulation-based, and telemetry-supported research would have added further precision and explanatory depth.

## REFERENCES


[1]. Abdalzaher, M. S., Fouda, M. M., Emran, A., Fadlullah, Z. M., & Ibrahem, M. I. (2023). A survey on key management and authentication approaches in smart metering systems. *Energies*, *16*(5), 2355. https://doi.org/10.3390/en16052355

[2]. 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

[3]. 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

[4]. 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

[5]. 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

[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]. Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1–8. https://doi.org/10.1016/j.comcom.2020.03.007

[9]. Alsuwian, T., Shahid Butt, A., & Amin, A. A. (2022). Smart grid cyber security enhancement: Challenges and solutions—A review. *Sustainability*, *14*(21), 14226. https://doi.org/10.3390/su142114226

[10]. 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

[11]. 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

[12]. 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

[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]. Boev, M. A., Chunyu, S., & Taranov, A. V. (2023). A tracking-resistance test for ADSS-type optical cables. *Russian Electrical Engineering*, *94*, 601–604. https://doi.org/10.3103/s1068371223080059

[15]. Canonico, R., & Sperlì, G. (2023). Industrial cyber-physical systems protection: A methodological review. *Computers & Security*, *135*, 103531. https://doi.org/10.1016/j.cose.2023.103531

[16]. Carvalho, R. V., Bonfim, M. J. d. C., Ussuna, D. A., Toledo, L. F. R. B., Martins, R., & Filho, V. S. (2019). Distributed temperature sensing in OPGW with multiple optical fibres. *IET Science, Measurement & Technology*, *13*, 1219–1223. https://doi.org/10.1049/iet-smt.2018.5319

[17]. 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

[18]. Chen, Y., Wei, Y., Wang, X., Zhang, J., Liu, W., Meng, X., Cao, J., & Wang, J. (2023). Analysis of induced current of OPGW in 750 kV transmission lines. In *The proceedings of 2023 4th international symposium on insulation and discharge computation for power equipment* (pp. 631–639). Springer. https://doi.org/10.1007/978-981-99-7413-9_60

[19]. Christensen, D., Martin, M., Gantumur, E., & Mendrick, B. (2019). Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources. *The Electricity Journal*, *32*(2), 1–8. https://doi.org/10.1016/j.tej.2019.01.018

[20]. Davis, K. R., Davis, C. M., Zonouz, S. A., Bobba, R. B., Berthier, R., Garcia, L., & Sauer, P. W. (2015). A cyber-physical modeling and assessment framework for power grid infrastructures. *IEEE Transactions on Smart Grid*, *6*(5), 2464–2475. https://doi.org/10.1109/tsg.2015.2424155

[21]. Deng, R., Xiao, G., Lu, R., Liang, H., & Vasilakos, A. V. (2017). False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics*, *13*(2), 411–423. https://doi.org/10.1109/tii.2016.2614396

[22]. Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, *21*(11), 3901. https://doi.org/10.3390/s21113901

[23]. Dmitriev, V., & Gonzalez, L. (2013). Electrical and thermal analysis on optical ground wire cables in short-circuit regime by coupled equations. *Electric Power Systems Research*, *101*, 80–87. https://doi.org/10.1016/j.epsr.2013.03.015

[24]. El Mrabet, Z., El Ghazi, H., Kaabouch, N., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469–482. https://doi.org/10.1016/j.compeleceng.2018.01.015

[25]. Feng, X., Hou, J., Yu, Q., Li, X., Wu, J., Liu, L., & Chen, W. (2022). Research on optical fiber composite overhead wire (OPGW) lightning monitoring technology based on weak fiber Bragg grating array. *Journal of Nanoelectronics and Optoelectronics*, *17*(1), 170–176. https://doi.org/10.1166/jno.2022.3182

[26]. 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

[27]. 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

[28]. Fragkos, G., Johnson, J., & Tsiropoulou, E. E. (2022). Dynamic role-based access control policy for smart grid applications: An offline deep reinforcement learning approach. *IEEE Transactions on Human-Machine Systems*, *52*(4), 761–773. https://doi.org/10.1109/thms.2022.3163185

[29]. Gao, J., Xiao, Y., Liu, J., Liang, W., & Chen, C. L. P. (2012). A survey of communication/networking in smart grids. *Future Generation Computer Systems*, *28*(2), 391–404. https://doi.org/10.1016/j.future.2011.04.014

[30]. Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., & Poolla, K. (2011). *Smart grid data integrity attacks: Characterizations and countermeasures* 2011 IEEE international conference on smart grid communications,

[31]. Gündüz, 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

[32]. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, *209*, 103540. https://doi.org/10.1016/j.jnca.2022.103540

[33]. Hong, J., & Liu, C.-C. (2019). Intelligent electronic devices with collaborative intrusion detection systems. *IEEE Transactions on Smart Grid*, *10*(1), 271–281. https://doi.org/10.1109/tsg.2017.2737826

[34]. 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

[35]. 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

[36]. Hussain, S. M. S., Farooq, S. M., & Ustun, T. S. (2020). A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages. *IEEE Transactions on Power Delivery*, *35*(6), 2985–2992. https://doi.org/10.1109/tpwrd.2020.2990760

[37]. Hussain, S. M. S., Ustun, T. S., & Kalam, A. (2020). A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. *IEEE Transactions on Industrial Informatics*, *16*(9), 5643–5654. https://doi.org/10.1109/tii.2019.2956734

[38]. 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

[39]. 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

[40]. 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

[41]. 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

[42]. Khalifa, T., Abdrabou, A., Shaban, K., & Gaouda, A. M. (2018). Heterogeneous wireless networks for smart grid distribution systems: Advantages and limitations. *Sensors*, *18*(5), 1517. https://doi.org/10.3390/s18051517

[43]. 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

[44]. Leszczyna, R. (2018a). Cybersecurity and privacy in standards for smart grids—A comprehensive survey. *Computer Standards & Interfaces*, *56*, 62–73. https://doi.org/10.1016/j.csi.2017.09.005

[45]. Leszczyna, R. (2018b). 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

[46]. Li, B., Huang, M., Zhang, H., Lin, M., He, S., & Chen, L. (2023). Research on communication technology of OPGW line in distribution network under interference environment. *EAI Endorsed Transactions on Scalable Information Systems*, *10*(3), e4. https://doi.org/10.4108/eetsis.v10i3.2780

[47]. Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, *14*(1), Article 13. https://doi.org/10.1145/1952982.1952995

[48]. 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

[49]. 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

[50]. 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

[51]. Md Khaled, H. (2026). Artificial Intelligence Based Predictive Analytics for SKU Performance and Revenue Optimization in Competitive Markets. *American Journal of Advanced Technology and Engineering Solutions*, *6*(01), 297-331. https://doi.org/10.63125/cmyhzv81

[52]. 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

[53]. 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

[54]. 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

[55]. 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

[56]. 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

[57]. 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

[58]. 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

[59]. 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

[60]. 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

[61]. 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

[62]. 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

[63]. 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

[64]. 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

[65]. Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, *1*(1), 99–107. https://doi.org/10.1109/tsg.2010.2046347

[66]. Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209. https://doi.org/10.1109/jproc.2011.2161428

[67]. 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

[68]. 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

[69]. 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

[70]. 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

[71]. 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

[72]. 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

[73]. Ozansoy, C. R., Zayegh, A., & Kalam, A. (2009). Object modeling of data and datasets in the international standard IEC 61850. *IEEE Transactions on Power Delivery*, *24*(3), 1140–1147. https://doi.org/10.1109/tpwrd.2008.2005658

[74]. 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

[75]. Pliatsios, D., Sarigiannidis, P. G., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: Secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials*, *22*(3), 1942–1976. https://doi.org/10.1109/comst.2020.2987688

[76]. Qays, M. O., Ahmad, I., Abu-Siada, A., Hossain, M. L., & Yasmin, F. (2023). Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review. *Energy Reports*, *9*, 2440–2452. https://doi.org/10.1016/j.egyr.2023.01.085

[77]. Quincozes, S. E., Albuquerque, C., Passos, D., & Mossé, D. (2021). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, *184*, 107679. https://doi.org/10.1016/j.comnet.2020.107679

[78]. 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

[79]. Reda, H. T., Ray, B., Peidaee, P., Anwar, A., Mahmood, A., Kalam, A., & Islam, N. (2021). Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in the smart grid. *Sensors*, *21*(4), 1554. https://doi.org/10.3390/s21041554

[80]. 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

[81]. Ruland, K. C., Sassmannshausen, J., Waedt, K., & Zivic, N. (2017). Smart grid security—An overview of standards and guidelines. *e & i Elektrotechnik und Informationstechnik*, *134*(1), 19–25. https://doi.org/10.1007/s00502-017-0472-8

[82]. Shan, X. G., & Zhuang, J. (2020). A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. *Reliability Engineering & System Safety*, *195*, 106683. https://doi.org/10.1016/j.ress.2019.106683

[83]. Silveira, P., Silva, E. F., Galletta, A., & Lopes, Y. (2023). Security analysis of digitized substations: A systematic review of GOOSE messages. *Internet of Things*, 100760. https://doi.org/10.1016/j.iot.2023.100760

[84]. 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

[85]. Stojkov, M., Dalčeković, N., Markoski, B., Milosavljević, B., & Sladić, G. (2021). Towards cross-standard compliance readiness: Security requirements model for smart grid. *Energies*, *14*(21), 6862. https://doi.org/10.3390/en14216862

[86]. Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

[87]. Sun, J., Yao, X., Huang, Y., Jiao, Z., & Chen, J. (2020). Experimental and numerical analysis of damage characteristics to OPGW strands under first lightning strike and continuous current. *Electric Power Systems Research*, *188*, 106515. https://doi.org/10.1016/j.epsr.2020.106515

[88]. 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

[89]. Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836–1846. https://doi.org/10.1109/tpwrs.2008.2002298

[90]. 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

[91]. Wang, W., Xu, Y., & Khanna, M. (2011). A survey on the communication architectures in smart grid. *Computer Networks*, *55*(15), 3604–3629. https://doi.org/10.1016/j.comnet.2011.07.010

[92]. Xu, L., Guo, Q., Sheng, Y., Muyeen, S. M., & Sun, H. (2021). On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. *Renewable and Sustainable Energy Reviews*, *152*, 111642. https://doi.org/10.1016/j.rser.2021.111642

[93]. Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, *34*, 100433. https://doi.org/10.1016/j.ijcip.2021.100433

[94]. Yu, H., Li, P., Zhang, L., Zhu, Y., Al-Zahrani, F. A., & Ahmed, K. (2020). Application of optical fiber nanotechnology in power communication transmission. *Alexandria Engineering Journal*, *59*(6), 5019–5030. https://doi.org/10.1016/j.aej.2020.09.025

[95]. 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

[96]. Zhang, L., Yang, G., Song, C., & Wu, Q. (2023). Accountable multi-authority attribute-based data access control in smart grids. *Journal of King Saud University - Computer and Information Sciences*, *35*(7), 101597. https://doi.org/10.1016/j.jksuci.2023.101597