Review of Applied Science and Technology

Volume: 1; Issue: 4
Pages: 283– 322

ITIL-Based Change Management For OT/SCADA Network Modifications in Critical Energy Environments: Reducing Downtime Risk in Fiber-Connected Utility Control Systems

Abu Naser Md Golam Mosharraf[1]; Amir Razaq[2];

[1]. *IT & Digital service NOC operational lead, Grameenphone Ltd, Dhaka, Bangladesh;*
Email: anmmosharraf@gmail.com

[2]. *Projects Engineer, NAFFCO Group, Doha, Qatar;*
Email: amirleghari75@gmail.com

Doi: 10.63125/e2gqtp57
Received: *11 September 2022;* ***Revised:*** *18 October 2022;* ***Accepted:*** *13 November 2022;* ***Published:*** *04 December 2022*

Abstract

This study investigates the critical problem of downtime risk during OT/SCADA network modifications in fiber-connected utility control systems, where poorly governed changes can disrupt real-time monitoring, control visibility, and operational continuity in energy infrastructure. The purpose of the research is to quantitatively assess how ITIL-based change management practices contribute to reducing downtime risk and improving system resilience in critical energy environments. A quantitative, cross-sectional, case-based research design was adopted, using a structured Likert-scale survey administered to a purposive sample of 214 professionals drawn from cloud-integrated enterprise and utility control system environments, including OT engineers, SCADA operators, network engineers, and ITIL practitioners. The study examined key independent variables such as change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review and documentation, with downtime risk reduction as the dependent variable. Data were analyzed using descriptive statistics, reliability testing, Pearson correlation, and multiple regression modeling. The findings reveal strong statistical relationships, with the regression model explaining 67.5% of the variance in downtime risk reduction ($R^2 = 0.675$, $p < 0.001$). Change risk assessment emerged as the strongest predictor ($\beta = 0.31$), followed by rollback and recovery planning ($\beta = 0.27$) and change planning ($\beta = 0.22$). Correlation results further confirm significant positive associations, particularly between change risk assessment and downtime reduction ($r = 0.72$, $p < 0.001$). The overall downtime risk reduction score was high ($M = 4.20$), while system resilience was also strong ($M = 4.12$), although moderate risk exposure remained ($M = 3.96$). These findings indicate that structured ITIL-based governance significantly enhances operational continuity. The study implies that integrating risk-aware planning, recovery readiness, and formal authorization into change processes can reduce failures and improve resilience in critical infrastructure systems.

Keywords

ITIL Change Management, OT/SCADA Systems, Downtime Risk Reduction, Critical Energy Infrastructure, Operational Resilience;

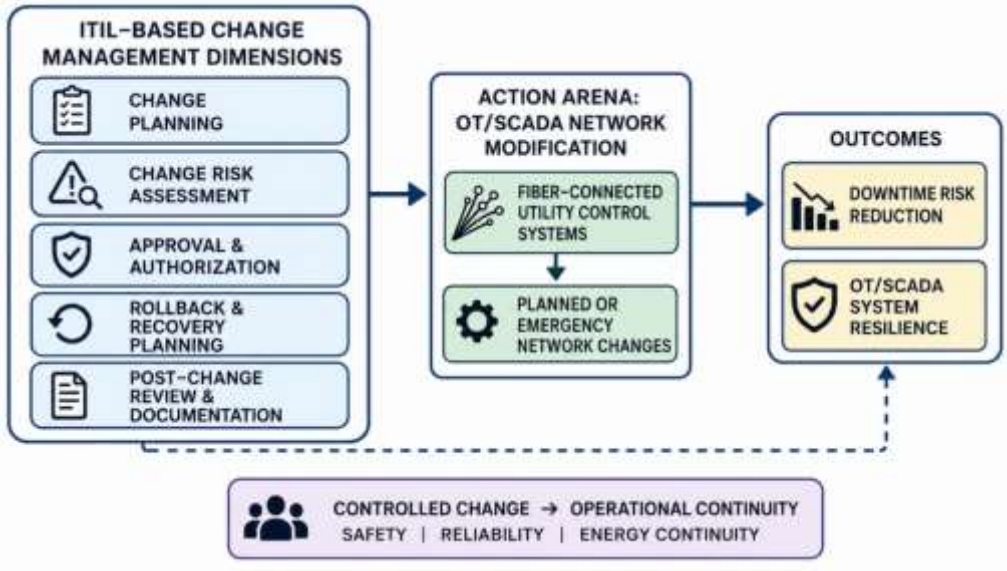
INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are industrial control arrangements used to monitor, collect, communicate, and supervise operational data from geographically distributed field assets, while Operational Technology (OT) refers to the hardware, software, control logic, sensors, actuators, communication devices, and engineering processes that directly monitor or control physical equipment (Blumberg et al., 2019). In critical energy environments, OT/SCADA systems support electricity generation, transmission, distribution, substation automation, load balancing, protection coordination, remote switching, alarm handling, and control-center visibility. Industrial Control Systems (ICS) include SCADA, distributed control systems, programmable logic controllers, human–machine interfaces, communication networks, and field devices; these systems are widely used in power generation, distribution, water treatment, nuclear plants, and other critical infrastructures. In this study, fiber-connected utility control systems refer to OT/SCADA communication architectures in which fiber-optic networks connect substations, control centers, field equipment, protection systems, and utility communication nodes (Farhangi, 2010). Fiber connectivity is important because modern energy operations require high availability, low latency, predictable communication, electromagnetic interference resistance, and long-distance data transmission. Internationally, SCADA and smart-grid communication research has emphasized that electric power infrastructure is no longer only an electrical system; it is also a cyber-physical system where computation, communication, automation, and physical energy flows are tightly integrated (Iden & Eikebrokk, 2013). This integration increases the operational significance of controlled change because a network modification can affect not only information flow but also real-time physical control, system visibility, protection coordination, and restoration capability (Knowles et al., 2015). Earlier SCADA security research identified interconnectivity, protocol exposure, remote access, and dependency on communication networks as major sources of control-system vulnerability. Later studies extended this concern to smart-grid and cyber-physical energy systems, showing that communication architectures, security requirements, and control-loop dependencies make energy networks internationally significant from economic, safety, and national-infrastructure perspectives. Therefore, the present research defines OT/SCADA network modification as any planned or emergency change to the communication, configuration, routing, segmentation, switching, security, monitoring, or recovery components that support real-time utility control (Podsakoff et al., 2012).

ITIL-based change management refers to a structured service-management approach for controlling changes through planning, assessment, authorization, implementation coordination, documentation, and review. In the context of this research, ITIL-based change management is not treated as a general administrative process; it is treated as a disciplined risk-control mechanism for OT/SCADA network modifications where downtime can disrupt the visibility, controllability, and reliability of energy infrastructure. IT service management research has shown that ITIL adoption is associated with process standardization, service-quality improvement, governance discipline, clearer responsibilities, and more consistent operational practices (Pollard & Cater-Steel, 2009). Successful ITIL implementation depends on strategy, organizational commitment, and critical success factors, while ITIL implementation research is also connected to service reliability and managerial control. In energy environments, change management has a narrower tolerance for error than conventional enterprise IT because change failure can produce communication loss, delayed switching, outage escalation, relay miscoordination, operator blind spots, alarm floods, or recovery delays (Sridhar et al., 2012). The international significance of this issue is linked to the global modernization of electricity infrastructure, where older power grids have increasingly adopted digital control, automation, wide-area communication, and intelligent monitoring to improve reliability and efficiency. Smart-grid communication studies show that energy reliability increasingly depends on secure and reliable information exchange among control centers, substations, distributed devices, and grid applications (Ten et al., 2010). In this context, an ITIL-based change process can support OT/SCADA governance by requiring formal change requests, risk classification, dependency review, stakeholder coordination, approval checkpoints, implementation scheduling, backout planning, and post-change evaluation. These activities are important because OT/SCADA modifications often involve a chain of interdependent components, including routers, switches, firewalls, remote terminal units,

communication processors, protocol gateways, historian servers, engineering workstations, network monitoring systems, and fiber transport equipment (Vogus & Sutcliffe, 2007).

Figure 1: ITIL-Based Change Management Framework for Reducing Downtime Risk in OT/SCADA Utility Control Systems



Downtime risk in fiber-connected utility control systems can be defined as the likelihood and potential operational effect of service interruption, communication instability, delayed control response, loss of telemetry, failed failover, degraded monitoring, or extended restoration caused by planned or unplanned network changes (McLaughlin et al., 2016). This definition is important because downtime in OT/SCADA environments has a different meaning from downtime in office information systems. In enterprise IT, downtime may affect productivity, customer access, or data availability; in OT/SCADA energy systems, downtime may reduce control-center awareness, interrupt operational commands, delay fault isolation, weaken protection visibility, or increase restoration time (Cheminod et al., 2013). Research on SCADA and industrial networks has repeatedly shown that these systems have unique availability, timing, safety, and reliability requirements that separate them from traditional IT environments. Industrial-network security studies have also highlighted the special characteristics of industrial communications, while industrial control system research has shown that these systems have moved from legacy electromechanical arrangements toward ICT-based cyber-physical systems with close links between cyber and physical components. This close coupling makes change control internationally significant because a technical modification in a utility network may produce direct operational consequences. Cyber-physical system security literature also shows that industrial and energy systems combine computation, communication, and physical processes, creating risks that must be evaluated across both digital and operational domains (Cárdenas et al., 2008). For example, a change to a firewall rule, VLAN, routing table, fiber path, substation switch configuration, remote-access rule, or SCADA polling route can alter how field devices communicate with control centers. If the change is not planned, tested, authorized, and recoverable, operational continuity may be weakened. Risk assessment is therefore central to this study because OT/SCADA network modification is not only a technical activity but also a risk event involving service availability, energy continuity, safety, cybersecurity, and organizational coordination (Bhamare et al., 2020).

The international importance of ITIL-based change management for OT/SCADA environments is strengthened by the global shift from isolated industrial networks toward interconnected, remotely managed, and data-driven energy systems (McJunkin & Rieger, 2019). Industrial control systems were historically designed for functionality, determinism, and availability, with less emphasis on exposure to enterprise networks and external communication pathways; contemporary ICS environments

increasingly interact with corporate systems, remote support platforms, analytics environments, cloud services, and cybersecurity monitoring tools. Industrial control systems no longer operate in isolation, and increased connection to corporate networks and internet-facing environments has raised cyber-risk management challenges, including the need for ICS-specific security metrics. The same structural issue applies to change management because the more interconnected an OT/SCADA system becomes, the more likely a network change in one layer may affect another layer (Metke & Ekl, 2010). Fiber-connected utility control systems often include layered dependencies among optical transport, Ethernet switching, IP routing, serial-to-IP conversion, SCADA protocols, remote engineering access, network segmentation, security appliances, and control-center applications. Studies on smart-grid communications and cybersecurity describe electric grids as communication-intensive systems where reliability, security, privacy, resilience, and control performance depend on the quality of information exchange. Therefore, a poorly governed change may not remain a localized configuration issue; it may create service degradation across operational domains (Yan et al., 2012). ITIL-based change management is relevant because it offers a repeatable mechanism to classify change types, distinguish standard, normal, and emergency changes, document approvals, evaluate impact, schedule work, and manage rollback. ITSM research supports the value of structured service-management practices in improving operational discipline, cross-functional coordination, service quality, and adoption of process maturity. For OT/SCADA utility networks, the value of such discipline lies in reducing unplanned disruption during modifications to communication links, security boundaries, redundancy paths, and control-system access (Wang & Lu, 2013).

This research is motivated by a practical and measurable problem: critical energy organizations must modify OT/SCADA networks to maintain reliability, security, capacity, compliance, and operational performance, while each modification introduces the possibility of downtime or degraded control-system service. The study focuses on five ITIL-based change management dimensions: change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review/documentation. These dimensions are selected because they represent the operational path through which change management can influence downtime risk. Planning defines the scope, timing, stakeholders, technical steps, resources, and expected service effect of a modification. Risk assessment identifies dependencies, communication-path sensitivity, cybersecurity exposure, safety relevance, service criticality, and possible failure modes (Zhu et al., 2011). Approval and authorization create accountability by ensuring that high-risk OT/SCADA changes are reviewed by appropriate technical and managerial decision makers. Rollback and recovery planning provide a controlled method for restoring previous configurations, alternate communication paths, or operational visibility when implementation errors occur. Post-change review and documentation convert completed changes into organizational learning by recording results, problems, restoration steps, and lessons for later modifications (Humayed et al., 2017). ITIL implementation studies show that process success is linked to management support, process ownership, staff involvement, organizational change, and sustained improvement mechanisms. Quantitative ITSM studies further show that service-management frameworks can influence organizational benefits, process performance, and cross-national adoption patterns. In OT/SCADA environments, these ITIL dimensions also align with resilience-oriented thinking. Organizational resilience research highlights the ability of organizations to continue functioning under strain through awareness, adaptation, coordination, and recovery capacity, while resilient control-system work emphasizes state awareness and operational normalcy during disturbances in critical infrastructure systems (Henseler et al., 2015). The present study uses these ideas to frame downtime reduction as both a process-management and operational-resilience concern.

A quantitative, cross-sectional, case-study–based approach is appropriate for this research because the core problem concerns measurable relationships among ITIL-based change management practices and perceived downtime risk reduction in OT/SCADA network modifications. The study will use Likert-scale survey items to measure respondents' perceptions of change planning, risk assessment, approval and authorization, rollback and recovery planning, post-change review/documentation, downtime risk reduction, OT/SCADA change risk exposure, and fiber-connected utility control system resilience (Gungor et al., 2011). This design allows statistical examination of whether stronger change-

management practices are associated with lower downtime risk and higher system resilience. Correlation analysis can measure the direction and strength of relationships among the study variables, while multiple regression can estimate the predictive contribution of each ITIL-based factor to downtime risk reduction. Methodological literature supports the use of carefully designed survey instruments, validity checks, and reliability assessment when constructs are measured through respondent perceptions. The importance of controlling common method bias in behavioral and organizational survey research has been emphasized in prior methodological studies, while discriminant validity is also important when researchers assess whether related constructs remain empirically distinct (Igure et al., 2006). These methodological concerns matter because OT/SCADA professionals may evaluate change management from different roles, such as control-room operation, network engineering, substation automation, cybersecurity, infrastructure management, or IT service management. The case-study orientation supports contextual depth because fiber-connected utility control systems have technical and organizational features that are not fully captured by generic IT change-management models. The quantitative design also matches the study's hypotheses, which require testing whether change planning, risk assessment, approval procedures, rollback readiness, and post-change review significantly influence downtime risk reduction. By using descriptive statistics, reliability analysis, correlation analysis, and regression modeling, the research can convert professional perceptions into structured evidence about the relationship between ITIL-based change governance and OT/SCADA operational continuity (Marrone & Kolbe, 2011).

The study's introduction is also grounded in the international recognition that energy infrastructures are critical cyber-physical systems requiring coordination between technical reliability, cybersecurity, operational governance, and organizational resilience. Smart-grid and SCADA research identifies energy systems as highly dependent on secure communication, real-time monitoring, protocol reliability, and coordinated cyber-physical control (Lepmets et al., 2012). Security and control-system studies show that industrial environments face distinct challenges because attacks, misconfigurations, or operational disturbances may affect physical processes as well as digital services. ITSM research contributes a complementary process-management perspective by showing that ITIL-based service management can standardize work, improve accountability, support service quality, and guide organizational change in technical service environments. When these research streams are synthesized, the research problem becomes clear: critical energy organizations need reliable OT/SCADA network modifications, and the quality of change management may influence the level of downtime risk created or controlled during those modifications (Marrone et al., 2014). The present study therefore positions ITIL-based change management as a structured governance approach for controlling change-related uncertainty in fiber-connected utility control systems. The key constructs are defined around planning, risk assessment, authorization, rollback, documentation, downtime risk reduction, change-risk exposure, and control-system resilience. This introduction establishes the study's basis for examining how ITIL practices can be quantitatively evaluated in a critical energy context where SCADA availability, fiber-network stability, and operational continuity are essential to utility performance.

Background of the Study

Critical energy environments depend heavily on OT/SCADA systems to monitor, control, and coordinate the continuous operation of generation facilities, substations, transmission networks, distribution systems, and field-level utility assets. These systems allow operators to collect real-time data, issue control commands, detect abnormal conditions, supervise equipment performance, and maintain stable energy delivery across wide geographic areas. In modern utility environments, fiber-connected control systems have become especially important because they provide high-speed, low-latency, and reliable communication between control centers, substations, remote terminal units, intelligent electronic devices, network switches, protection systems, and monitoring platforms. However, the same communication dependency that improves operational visibility also creates serious risk when network modifications are poorly planned or weakly controlled. Changes such as switch configuration updates, firewall rule adjustments, routing changes, fiber-path reconfiguration, device replacement, segmentation updates, software patching, and communication protocol adjustments can disrupt SCADA visibility, delay control signals, interrupt telemetry, weaken redundancy, or increase downtime if they are not governed through a disciplined change management

process. In critical energy operations, downtime is not only a technical inconvenience; it can affect operational continuity, service reliability, safety coordination, restoration speed, and public trust in essential infrastructure. This makes structured change management highly important for utility organizations that must continuously modernize their OT/SCADA networks while maintaining stable service delivery. ITIL-based change management provides a systematic approach for managing such modifications through formal planning, risk assessment, authorization, implementation control, rollback preparation, documentation, and post-change review. By applying ITIL principles to OT/SCADA network changes, organizations can reduce uncertainty, improve accountability, strengthen communication between OT, IT, cybersecurity, and field engineering teams, and minimize the likelihood of failed or disruptive changes. This study is therefore grounded in the need to understand how ITIL-based change management practices influence downtime risk reduction in fiber-connected utility control systems. It focuses on the practical relationship between structured change governance and operational resilience, especially in environments where network reliability directly supports real-time energy monitoring, control-center decision-making, and uninterrupted utility service.

Problem Statement

Critical energy environments increasingly depend on fiber-connected OT/SCADA networks to maintain real-time visibility, command execution, equipment monitoring, and operational coordination across substations, control centers, field devices, protection systems, and utility communication infrastructures. However, these systems are highly sensitive to network modifications because even a small configuration error, routing change, firewall adjustment, switch update, fiber-path alteration, segmentation change, or failed device integration can interrupt communication between operational assets and control systems. In many utility environments, network changes are necessary for modernization, cybersecurity improvement, capacity expansion, maintenance, and system reliability. However, the process of implementing these changes may create downtime risk when planning is incomplete, technical dependencies are not fully mapped, operational impacts are not properly assessed, approval procedures are weak, rollback plans are missing, or post-change documentation is insufficient. The central problem is that OT/SCADA network modifications are often treated as technical tasks rather than structured governance activities that require coordinated risk control across OT, IT, cybersecurity, and engineering teams. This creates uncertainty during implementation and increases the possibility of communication loss, delayed telemetry, failed failover, reduced control-center visibility, service interruption, and extended recovery time. Although ITIL-based change management offers a systematic process for controlling changes through planning, risk assessment, authorization, implementation, rollback, and review, its practical effectiveness in reducing downtime risk within fiber-connected utility control systems is not sufficiently understood. Most organizations recognize the importance of change management, but there is limited quantitative evidence showing which ITIL-based practices most strongly contribute to downtime risk reduction in OT/SCADA environments. Therefore, this study addresses the problem of inadequate empirical understanding regarding the relationship between ITIL-based change management and operational continuity during OT/SCADA network modifications. The study specifically investigates whether structured change planning, change risk assessment, approval and authorization procedures, rollback and recovery planning, and post-change review can reduce downtime risk in critical energy environments. By examining this problem quantitatively, the research aims to provide evidence on how disciplined change governance can support safer, more reliable, and more resilient network modifications in fiber-connected utility control systems.

Objectives of The Study

The main objective of this study is to quantitatively assess how ITIL-based change management practices influence downtime risk reduction during OT/SCADA network modifications in critical energy environments. The study seeks to examine the extent to which structured change planning contributes to safer implementation of network modifications by improving preparation, scheduling, stakeholder coordination, technical readiness, and implementation control. Another objective is to evaluate the role of change risk assessment in identifying possible operational, technical, cybersecurity, safety, and communication-related risks before changes are introduced into fiber-connected utility

control systems. The study also aims to assess how approval and authorization procedures support accountability and reduce the likelihood of failed or disruptive changes by ensuring that high-risk modifications are reviewed by appropriate technical and managerial stakeholders. In addition, the research intends to determine the influence of rollback and recovery planning on reducing downtime duration when network modifications cause unexpected service disruption, communication loss, or degraded control-system performance. Another important objective is to analyze the effect of post-change review and documentation on future change reliability by determining whether lessons learned, incident records, implementation outcomes, and corrective actions improve organizational change maturity. The study further seeks to develop a practical understanding of OT/SCADA change risk exposure by examining how prepared utility organizations are to control downtime risk during planned and emergency network modifications. It also aims to assess the resilience of fiber-connected utility control systems by evaluating redundancy, failover readiness, recovery capability, real-time monitoring, and control-center visibility during network changes. Through descriptive statistics, correlation analysis, and multiple regression modeling, this research will identify the strength and direction of relationships between ITIL-based change management practices and downtime risk reduction. Overall, the study is designed to produce measurable evidence that can explain how structured change governance contributes to operational continuity, service reliability, and change-related risk reduction in critical energy OT/SCADA environments.

Research Hypotheses

The research hypotheses of this study are developed to examine the statistical relationship between ITIL-based change management practices and downtime risk reduction in OT/SCADA network modifications within critical energy environments. The first hypothesis proposes that ITIL-based change planning has a significant positive effect on downtime risk reduction. This hypothesis is based on the assumption that well-planned changes are more likely to be implemented successfully because they include clear scope definition, implementation steps, scheduling, resource allocation, stakeholder communication, and pre-change testing. The second hypothesis proposes that change risk assessment has a significant positive effect on operational continuity in fiber-connected utility control systems. This means that when organizations identify technical dependencies, communication risks, cybersecurity vulnerabilities, safety impacts, and service-critical components before implementation, they are more likely to avoid disruption. The third hypothesis states that approval and authorization procedures have a significant positive effect on reducing failed or disruptive OT/SCADA network changes. This hypothesis assumes that formal review and approval processes improve accountability, prevent unauthorized changes, and ensure that high-risk modifications receive appropriate technical evaluation. The fourth hypothesis proposes that rollback and recovery planning has a significant positive effect on reducing downtime duration after network modification issues. This suggests that prepared restoration procedures, backup configurations, failover options, and recovery steps can help organizations return systems to stable operation more quickly when problems occur. The fifth hypothesis states that post-change review and documentation have a significant positive effect on improving future change reliability. This hypothesis reflects the idea that organizations learn from previous changes when they document outcomes, analyze failures, and apply lessons to future implementations. The sixth hypothesis proposes that ITIL-based change management practices collectively have a significant positive effect on downtime risk reduction in critical energy OT/SCADA environments. Together, these hypotheses allow the study to test both the individual and combined effects of change planning, risk assessment, approval procedures, rollback readiness, and post-change review on downtime risk reduction.

Significance of the Research

i. **Significance for critical energy utility organizations:** This research is significant because it addresses the challenge of maintaining operational continuity during OT/SCADA network modifications in critical energy environments. Utility organizations must regularly update, secure, expand, and maintain their network infrastructure, but each modification can create downtime risk. This study can help organizations understand which ITIL-based change management practices are most useful for reducing disruption during these changes.

ii. **Significance for OT/SCADA engineers and network teams:** The study is important for engineers

and technical teams because it focuses on practical issues such as configuration changes, fiber-path reliability, failover readiness, dependency mapping, communication stability, and recovery planning. The findings may help technical teams improve how they prepare for and implement network changes in control-system environments.

iii. **Significance for ITIL and change management professionals:** This research extends ITIL-based change management into the specialized field of OT/SCADA and critical energy infrastructure. It may help change managers understand that change governance in utility control systems requires stronger coordination, risk assessment, approval discipline, and rollback planning than ordinary enterprise IT environments.

iv. **Significance for cybersecurity and risk management teams:** OT/SCADA network changes can affect access control, firewall rules, segmentation, remote connectivity, monitoring systems, and cyber-physical risk exposure. This study is significant because it highlights the need for cybersecurity and risk teams to participate in change assessment before modifications are implemented.

v. **Significance for academic research:** The study contributes to academic knowledge by offering a quantitative, cross-sectional, case-study–based approach to examining ITIL-based change management in fiber-connected utility control systems. It also introduces context-specific result indicators such as the OT/SCADA Change Risk Exposure Index and the Fiber-Connected Utility Control System Resilience Score.

vi. **Significance for service reliability and public infrastructure:** Critical energy systems support homes, businesses, hospitals, industries, communication networks, and public services. Reducing downtime risk in utility control systems can support broader service reliability and infrastructure stability. Therefore, this research is significant because it connects structured change management with the reliability of essential energy services.

LITERATURE REVIEW

The literature review of this study examines the relationship between ITIL-based change management, OT/SCADA network modifications, downtime risk reduction, and operational resilience in fiber-connected utility control systems. Critical energy environments depend on highly reliable control and communication infrastructures where system availability, real-time monitoring, command execution, and rapid recovery are essential. OT/SCADA systems are different from conventional enterprise IT systems because they directly support physical processes, energy delivery, substation automation, equipment supervision, and control-center decision-making. As energy utilities modernize their infrastructure, fiber-connected networks have become increasingly important for transmitting operational data between field assets, substations, control centers, and monitoring platforms. However, these networks must often be modified through configuration changes, device upgrades, routing adjustments, firewall updates, segmentation changes, software patches, and redundancy improvements. Such modifications can improve system performance and security, but they can also introduce downtime risk when they are not properly governed. For this reason, the literature review will focus on how structured change management can reduce uncertainty and improve reliability during OT/SCADA network changes. ITIL-based change management provides a useful framework because it emphasizes planning, risk assessment, approval, implementation control, rollback preparation, documentation, and continual improvement. These practices are especially relevant in critical energy environments where failed changes may cause communication interruptions, delayed telemetry, loss of visibility, control-system instability, and extended recovery time. The literature review will also consider the theoretical foundation of the study through High Reliability Organization Theory, which is suitable for explaining how organizations operating in high-risk environments maintain reliability through risk awareness, operational sensitivity, expert coordination, resilience, and learning from failure. In addition, the review will develop a conceptual framework linking ITIL-based change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review with downtime risk reduction. By synthesizing studies on OT/SCADA systems, utility communication networks, ITIL change management, downtime risk, operational continuity, and resilience, this chapter will provide the academic foundation for the study's hypotheses, variables, and quantitative research model.

OT/SCADA Systems in Critical Energy Infrastructure

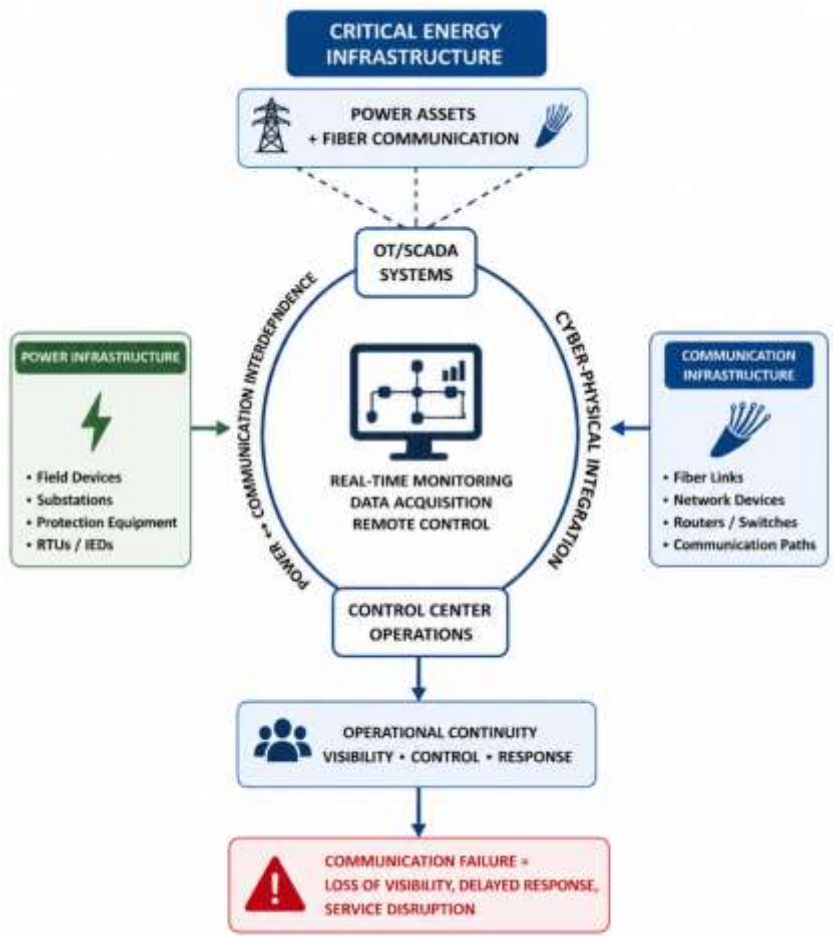
OT/SCADA systems form the operational backbone of critical energy infrastructure because they enable real-time monitoring, data acquisition, remote control, event supervision, and operational coordination across geographically distributed power assets. In electricity generation, transmission, and distribution environments, SCADA platforms collect information from substations, field sensors, intelligent electronic devices, protection equipment, remote terminal units, and control-center applications. These systems allow operators to observe voltage, current, breaker position, equipment status, alarms, load behavior, communication health, and abnormal operating conditions. In this way, OT/SCADA systems serve as the link between physical energy processes and digital decision-making. Their importance becomes more visible in fiber-connected utility control systems, where communication infrastructure is required to support fast, stable, and reliable exchange of operational data between control centers and field locations. Fiber communication improves bandwidth, distance coverage, signal quality, and resistance to electromagnetic interference, making it highly suitable for energy environments where continuous visibility and command reliability are essential. However, the value of OT/SCADA systems is directly connected to the availability of their supporting communication networks. When SCADA communication links are unavailable, energy operators may lose visibility over field assets, experience delayed alarms, face limitations in remote switching, and encounter difficulty coordinating restoration activities. Research on power-grid and telecommunications interdependence has shown that SCADA services depend strongly on the communication links connecting power-grid and network infrastructures, making these links central to service availability and continuity (Bobbio et al., 2010; Khaled, 2021). For this reason, OT/SCADA systems in critical energy infrastructure cannot be understood only as control software or data platforms. They must be understood as integrated cyber-physical systems in which field equipment, communication networks, control applications, operators, and organizational procedures work together to maintain safe and continuous electricity service.

The literature also shows that OT/SCADA systems are essential because modern energy infrastructure depends on the interaction between electrical networks and communication systems. Electrical distribution grids and SCADA data transmission networks maintain a mutually dependent relationship because power systems require communication services for monitoring and control, while communication infrastructures also require stable power supply to remain operational. This interdependence is especially important in utility environments where a malfunction in one infrastructure can influence the performance of another. For example, a communication failure may prevent operators from receiving field data, while a power failure may interrupt the devices and networks that support SCADA communication. In fiber-connected utility control systems, these dependencies become more complex because network paths, switches, routers, fiber links, protection relays, remote terminal units, and supervisory applications must work together as one operational chain. Any disruption in this chain may create reduced situational awareness, delayed response, or partial loss of control-center visibility. Studies on SCADA communication dependence emphasize that the operation of SCADA services is shaped by the operating state of both power and communication infrastructures, making the relationship between these systems bidirectional and operationally sensitive (Radu et al., 2015; Binte & Sazzadul, 2022). This is important for the present study because ITIL-based change management is being examined in the context of OT/SCADA network modifications. If a utility changes routing rules, fiber paths, firewall settings, switch configurations, segmentation structures, or remote-access arrangements, the modification may affect not only the network layer but also the reliability of the control process. Therefore, the literature supports the view that OT/SCADA systems in energy environments require structured governance because technical changes are closely connected to operational continuity, service availability, and downtime risk.

Another important theme in the literature is that OT/SCADA systems have become internationally significant because they support critical infrastructure sectors that directly affect public safety, economic activity, energy security, and essential service delivery. SCADA-related incidents have shown that failures, cyber events, misconfigurations, and unauthorized access can affect sectors such as electricity, water, transportation, pipelines, manufacturing, and other industrial services. A study of SCADA and critical infrastructure incidents classified events according to source sector, method of operation, impact, and target sector, demonstrating that SCADA-related disruptions are not only

technical events but also infrastructure-level risks with operational and social consequences (Miller & Rowe, 2012).

Figure 2: OT/SCADA Systems and Communication Interdependence in Critical Energy Infrastructure



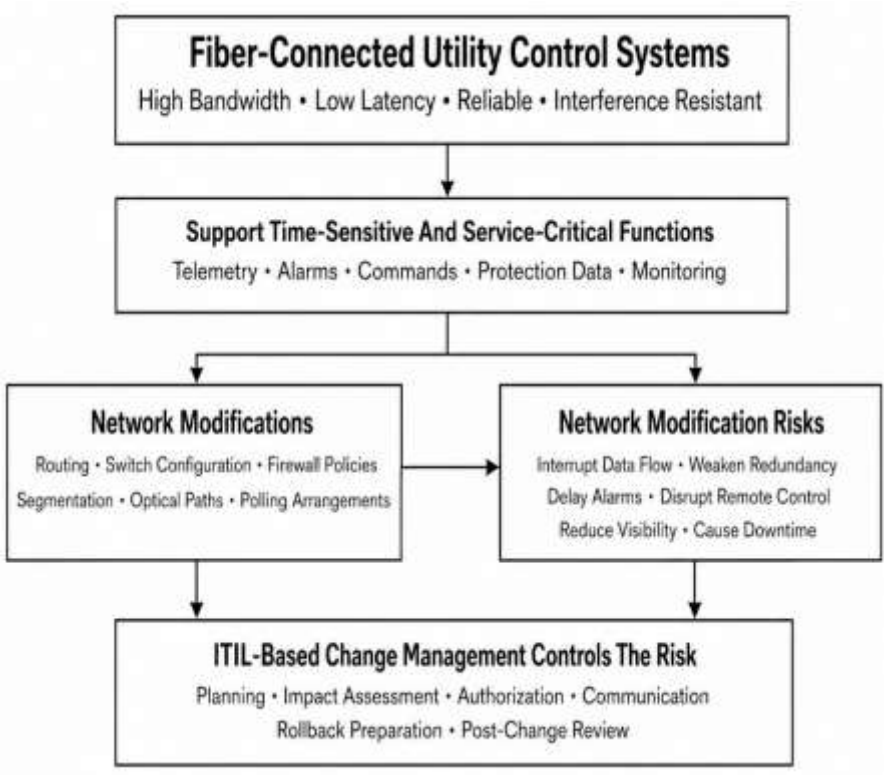
For critical energy environments, this means that SCADA reliability is linked to national infrastructure resilience, public trust, and continuity of energy supply. The literature further indicates that SCADA systems require specialized risk assessment because their architecture, operating requirements, and physical consequences differ from ordinary enterprise information systems. Cybersecurity risk assessment studies have emphasized that SCADA environments need methods capable of addressing system impact, risk management stages, domain-specific requirements, and operational consequences (Cherdantseva et al., 2016). In smart-grid research, cyber-physical testbed studies also show that modern grid environments require realistic evaluation of communication infrastructure, automation functions, control behavior, and cyber-physical interactions before new technologies or changes are deployed (Cintuglu et al., 2017). These findings are directly relevant to this thesis because OT/SCADA network modifications in fiber-connected utility systems require more than routine technical implementation. They require careful planning, risk assessment, approval, rollback readiness, and post-change review to protect uptime, maintain communication stability, and reduce the probability of disruption during planned or emergency changes.

Fiber-Connected Utility Control Systems and Network Modification Risks

Fiber-connected utility control systems represent the communication foundation through which modern energy utilities connect substations, control centers, intelligent electronic devices, protection equipment, remote terminal units, monitoring platforms, and field automation assets. In these environments, fiber-optic communication is valued because it supports high bandwidth, low latency,

long-distance transmission, strong signal integrity, and resistance to electromagnetic interference, which are all essential for reliable utility control. Unlike ordinary business communication networks, fiber-connected utility networks support operational functions that are time-sensitive and service-critical. They carry telemetry, alarms, command signals, protection data, status information, and monitoring outputs that allow operators to maintain visibility over geographically distributed assets. The literature on smart-grid communication architectures explains that electric power systems increasingly depend on high-speed, reliable, and secure data communication networks to manage complex grid operations effectively (Wang et al., 2011). This is directly relevant to OT/SCADA environments because utility control systems are no longer isolated technical platforms; they are integrated communication-dependent infrastructures. Fiber networks therefore act as the operational bridge between physical energy equipment and digital control functions. However, this strong dependency also increases exposure to change-related risk. Any modification to routing structures, switch configuration, firewall policies, network segmentation, optical paths, protection communication, or SCADA polling arrangements may influence how field assets communicate with the control center. As a result, fiber-connected utility control systems must be managed with a high level of technical discipline. A network change that seems minor at the configuration level may create wider operational effects if it interrupts data flow, weakens redundancy, delays alarm delivery, or disrupts remote control capability. Therefore, understanding fiber-connected utility systems requires attention not only to communication performance but also to how network modifications are planned, approved, tested, implemented, and recovered.

Figure 3: Fiber-Connected Utility Control Systems and Network Modification Risks



Network modification risk in fiber-connected utility control systems emerges from the interaction between technical complexity, communication dependency, and operational criticality. Utility communication environments often contain multiple technologies, including optical fiber, Ethernet, IP routing, substation automation protocols, wireless backup links, power-line communication, and enterprise network gateways. Because each technology supports different applications and performance requirements, selecting, modifying, or integrating communication components requires careful assessment. Studies on smart-grid communication technologies show that practical grid

operation depends on a hybrid communication environment where wired and wireless technologies support different functions, ranging from advanced metering and distribution automation to SCADA and energy management applications (Usman & Shami, 2013). In a fiber-connected OT/SCADA context, this means that modifications cannot be evaluated as isolated network tasks. A change in one network segment may affect interdependent control functions, cybersecurity boundaries, failover mechanisms, or monitoring paths. Communication-system research also emphasizes that smart-grid communication infrastructures involve layered architectures, middleware, networking technologies, and security requirements that must work together to support reliable energy services (Ancillotti et al., 2013). This complexity creates risk during change implementation because engineers must understand both the technical network topology and the operational role of each connection. For example, changing a switch port, updating a VLAN, replacing a router, modifying firewall access rules, or migrating a fiber path can affect SCADA visibility, protection signaling, historian data flow, remote engineering access, or alarm management. These risks are especially serious in critical energy environments because downtime may reduce operator awareness and delay operational response. Therefore, ITIL-based change management becomes relevant because it provides a structured method for controlling changes through planning, impact assessment, authorization, communication, rollback preparation, and post-change review.

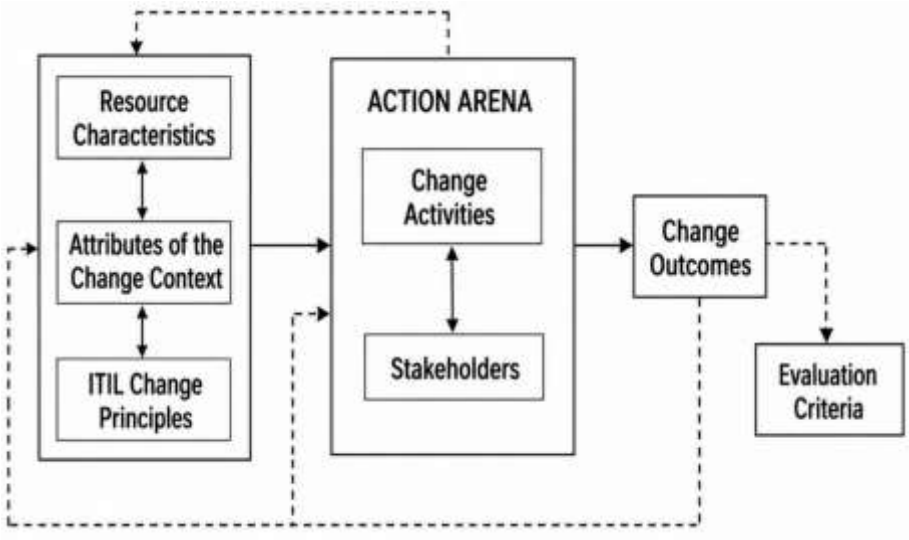
The risks associated with fiber-connected utility control systems are also shaped by the different communication requirements of utility applications. Some smart-grid and OT/SCADA functions require very low latency, high availability, strong reliability, and stable throughput, while other applications may tolerate slower or less frequent data exchange. Research on major smart-grid applications shows that communication requirements vary across home area networks, neighborhood area networks, and wide area networks, with differences in payload size, sampling rate, latency, bandwidth, and reliability expectations (Kuzlu et al., 2014). This variation is important because fiber-connected utility control systems often carry traffic for multiple operational functions at the same time. A network modification that is acceptable for one application may be risky for another if it affects timing, packet delivery, redundancy, or quality of service. Communication technology surveys also show that smart-grid systems require careful matching between application needs and communication methods because different technologies offer different strengths in coverage, data rate, reliability, cost, latency, and security (Emmanuel & Rayudu, 2016). For OT/SCADA network changes, this means that technical decisions must be linked with operational priorities. Before implementation, organizations must identify which assets, services, and control functions depend on the affected communication path. They must also verify backup links, failover design, rollback procedures, cyber access rules, and real-time monitoring readiness. Without structured change governance, a planned modification may cause unplanned downtime, delayed telemetry, control-center blind spots, failed communication between substations, or prolonged recovery. Therefore, fiber-connected utility control systems require a change management approach that recognizes both the technical design of communication infrastructure and the operational consequences of network disruption.

ITIL-Based Change Management in High-Reliability Technical Environments

ITIL-based change management is a structured approach for controlling the introduction, modification, replacement, or removal of technical components within service environments where reliability and continuity are essential. In high-reliability technical settings, change management is not only an administrative approval process; it is a risk-control mechanism that helps organizations evaluate whether a proposed change can be safely implemented without damaging service availability, operational stability, or system performance. For this research, ITIL-based change management is especially relevant because OT/SCADA network modifications in critical energy environments involve systems that directly support physical operations, real-time monitoring, alarm visibility, command execution, and utility service continuity. A change to a firewall rule, fiber communication path, switch configuration, routing table, access-control setting, or SCADA polling structure can create serious operational consequences if it is implemented without proper planning and impact analysis. ITIL provides a service-management logic that encourages organizations to document change requests, classify change types, assess operational risk, authorize implementation, coordinate stakeholders, prepare rollback plans, and review outcomes after completion. The value of this approach is supported

by ITIL implementation research showing that successful adoption requires systematic planning, critical-success-factor analysis, and structured process sequencing rather than informal or fragmented implementation (Ahmad et al., 2013). In addition, studies mapping ITIL literature show that ITIL has become an important subject in national and international service-management research because organizations use it to improve process consistency, governance maturity, service delivery, and operational control (Barros et al., 2015). Within OT/SCADA environments, these ideas are important because technical changes must be aligned with uptime, safety, cybersecurity, communication continuity, and engineering accountability.

Figure 4: ITIL-Based Change Management Framework In High-Reliability Technical Environments



In high-reliability technical environments, change management must also support governance, role clarity, and decision accountability. OT/SCADA systems operate within complex socio-technical arrangements where engineers, operators, cybersecurity teams, IT service managers, vendors, field technicians, and senior decision makers may all influence a single change activity. Without a formal change management structure, responsibility may become unclear, impact assessment may be incomplete, and technical implementation may proceed without sufficient understanding of system dependencies. ITIL-based change management helps address this challenge by defining how changes should be requested, reviewed, authorized, scheduled, implemented, and evaluated. This is significant for fiber-connected utility control systems because these systems include interdependent layers such as optical transport, Ethernet switching, routing, remote terminal communication, protocol gateways, control-center applications, and monitoring tools. Empirical work on the ITIL process reference model indicates that ITIL can support IT governance by strengthening process management practices, organizational resources, group efficacy, and structured implementation behavior (Iden & Eikebrokk, 2014). This governance function is highly relevant to OT/SCADA change control because energy utilities require disciplined decision-making when a technical modification may affect real-time operational visibility or service availability. Research on ITIL implementation strategy further suggests that ITIL adoption should be understood as an organizational project involving antecedents, implementation practices, and performance outcomes, rather than as a simple technical checklist (Eikebrokk & Iden, 2017). Therefore, in the context of this thesis, ITIL-based change management is viewed as a governance-centered process that connects technical risk, operational continuity, managerial oversight, and cross-functional coordination during OT/SCADA network modifications.

ITIL-based change management is also important in high-reliability environments because it encourages continuous improvement and learning from implementation outcomes. In OT/SCADA utility networks, change-related downtime may result from incomplete dependency mapping, weak

testing, insufficient communication, missing rollback plans, poor scheduling, inadequate approval, or failure to document lessons after implementation. A structured ITIL approach can reduce these weaknesses by requiring organizations to examine the change before implementation, monitor the change during execution, and review the results after completion. This creates a learning cycle in which successful and unsuccessful changes both become sources of process improvement. For example, if a fiber-path migration causes unexpected alarm delay or loss of visibility at a control center, post-change review and documentation can help identify whether the issue came from configuration error, redundancy failure, routing conflict, monitoring gap, or communication breakdown between teams. Such knowledge can then improve future change planning and reduce repeated failure. Studies on IT service process improvement show that successful process improvement depends on factors such as implementation strategy, management support, stakeholder involvement, internal resources, process definition, and learning from barriers that affect improvement initiatives (Diirr et al., 2014). These factors apply strongly to OT/SCADA environments because network changes require both technical precision and organizational discipline. Therefore, ITIL-based change management supports high-reliability technical operations by combining formal planning, risk evaluation, authorization, rollback readiness, documentation, and continuous improvement. In this research, these practices are examined as predictors of downtime risk reduction because they provide a structured pathway for making fiber-connected utility control system modifications safer, more accountable, and more resilient.

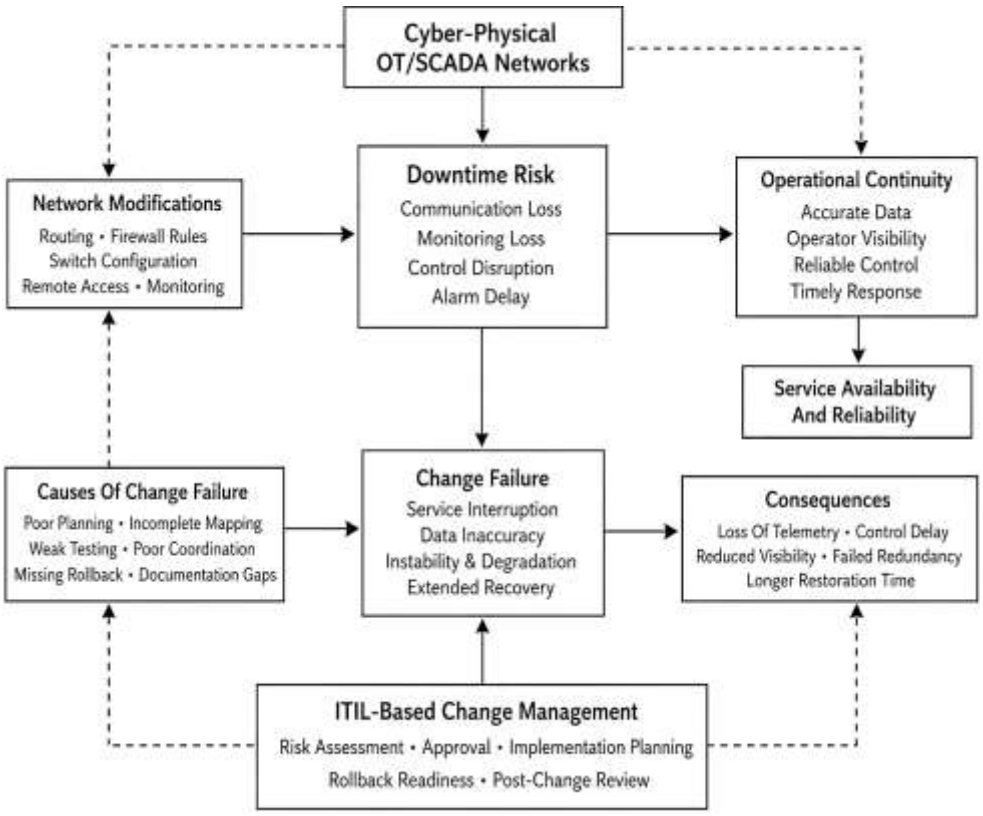
Downtime Risk and Change Failure in OT/SCADA Networks

Downtime risk in OT/SCADA networks refers to the possibility that communication, monitoring, control, or supervisory functions may become unavailable, delayed, degraded, or unreliable during normal operation, planned maintenance, emergency intervention, or network modification. In critical energy environments, downtime is not limited to the absence of a digital service; it may involve loss of telemetry, delayed alarm reporting, interrupted command execution, weakened operator visibility, failed redundancy, or reduced coordination between substations and control centers. This makes downtime risk a direct concern for operational continuity, because SCADA systems support the real-time relationship between field devices, communication networks, control applications, and human operators. In fiber-connected utility control systems, downtime may arise from hardware faults, communication link failures, routing errors, configuration conflicts, cyber events, poor change sequencing, or insufficient rollback planning. The literature on cyber-physical reliability emphasizes that modern power systems rely on both physical infrastructure and cyber layers, meaning that communication failures, data disruption, cyber incidents, and control-system weaknesses can influence power-system reliability and service continuity (Jimada-Ojuolape & Teh, 2020). This relationship is important for the present study because OT/SCADA network modifications often occur inside tightly connected cyber-physical environments where changes to network paths, firewall rules, switch configurations, remote access, or monitoring systems may influence operational performance. A change failure may therefore produce consequences beyond the affected device or network segment. It may reduce the operator's ability to supervise field assets, delay response to abnormal conditions, or extend recovery time during an incident. Therefore, downtime risk must be treated as both a technical risk and an operational governance issue. ITIL-based change management becomes relevant because it provides a structured way to identify change impact, assess dependencies, coordinate stakeholders, authorize work, prepare rollback procedures, and document lessons learned before similar failures are repeated.

Operational continuity in OT/SCADA networks depends heavily on the reliability, integrity, and availability of data moving between field equipment and control centers. A utility control system may remain physically energized while still experiencing operational weakness if the SCADA layer cannot provide accurate status information, real-time measurements, remote commands, or alarm visibility. This is especially significant in energy networks where state estimation, control-room decision-making, and system restoration depend on trustworthy measurements. Research on false data injection attacks in electric power grids demonstrated that manipulated measurements can mislead state estimation processes while bypassing bad-data detection mechanisms, showing how data integrity failures can affect the reliability of power-system monitoring and decision support (Liu et al., 2011). For downtime and change failure analysis, this literature is relevant because not all disruptions appear as complete

outages. Some failures may appear as inaccurate data, missing telemetry, delayed updates, unstable polling, inconsistent alarms, or incorrect system states. During OT/SCADA network modifications, such conditions may occur when routing tables are misconfigured, time synchronization is interrupted, firewall rules block required traffic, redundant paths are not activated, or monitoring systems are not updated after topology changes. Operational continuity therefore requires more than keeping devices powered; it requires preserving accurate communication, control visibility, and dependable data flow during and after network changes. Studies on cyber-physical attacks and defenses in smart grids further show that energy systems face threats and disturbances that cross both cyber and physical layers, requiring integrated analysis of attack pathways, defense strategies, and operational effects (He & Yan, 2016). In this study, this supports the argument that OT/SCADA change failure must be assessed across technical, operational, and organizational dimensions. A structured change process can reduce continuity risk by ensuring that changes are tested, dependencies are mapped, critical communication paths are verified, and recovery procedures are available if the implemented modification disrupts SCADA service.

Figure 5: Downtime Risk, Operational Continuity, And Change Failure In OT/SCADA Networks



Change failure in OT/SCADA networks is especially serious because industrial and utility control environments are designed for high availability, predictable operation, and rapid response to abnormal conditions. A failed change may occur when a planned modification produces unexpected service interruption, system instability, cybersecurity exposure, monitoring loss, communication degradation, or extended restoration time. These failures may result from incomplete asset inventories, poor dependency mapping, lack of operational testing, weak approval procedures, uncoordinated implementation, or missing documentation. Risk-analysis literature supports the need to examine both accidental failures and intentional cyber events when evaluating complex control systems. For example, fault-tree and attack-tree integration has been proposed as a way to combine reliability analysis with cyberattack analysis so that complex systems can be evaluated through both failure probability and security-risk perspectives (Fovino et al., 2009). This is relevant to OT/SCADA change management because network modifications may create both reliability weaknesses and security

vulnerabilities if they are poorly controlled. Similarly, research on false data injection in modern power systems shows that cyber-physical power networks face measurement, communication, and control risks that can undermine system operation when malicious or faulty data affects grid monitoring and decision-making (Liang et al., 2017). For this thesis, these studies justify the need to examine downtime risk as a multidimensional construct involving availability, integrity, continuity, recovery, and governance. ITIL-based change management can address this by requiring formal risk assessment, approval, implementation planning, rollback readiness, and post-change review. In fiber-connected utility control systems, such practices are particularly important because communication paths, redundant links, protection channels, SCADA polling routes, and control-center applications may all be affected by a single network modification. Therefore, operational continuity depends on the organization's ability to prevent failed changes, detect service degradation quickly, restore stable operation efficiently, and learn from each change event.

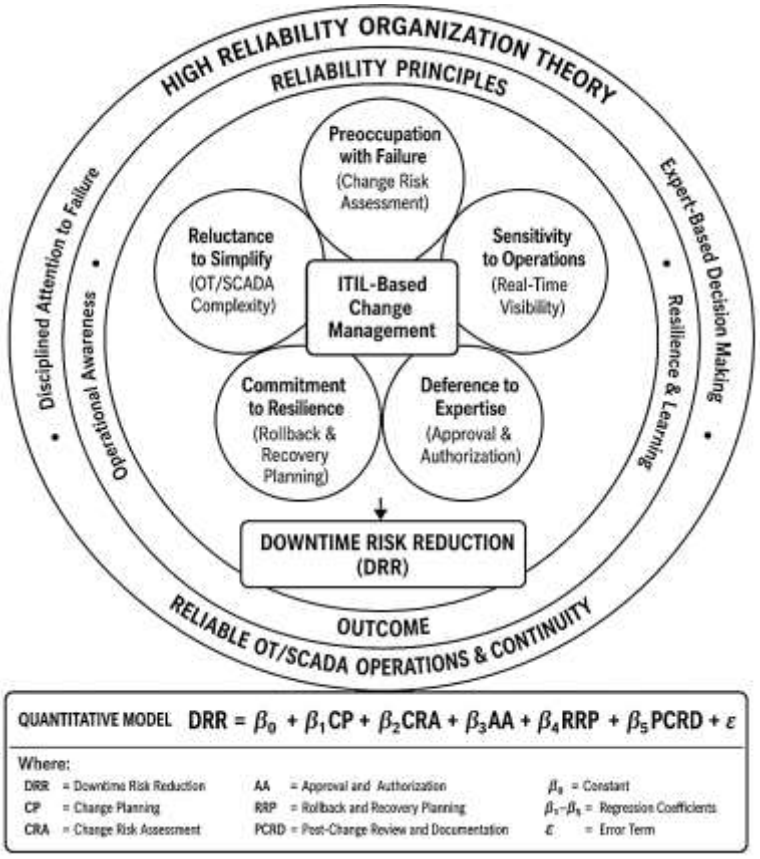
Theoretical Framework: High Reliability Organization Theory

High Reliability Organization Theory is selected as the theoretical foundation of this study because OT/SCADA network modifications in critical energy environments occur within complex, high-risk, and failure-sensitive operational systems. High Reliability Organization Theory explains how organizations operating under hazardous conditions maintain reliable performance through disciplined attention to failure, operational awareness, expert-based decision-making, resilience, and continuous learning. This theory is suitable for this research because fiber-connected utility control systems require stable communication between control centers, substations, field devices, protection systems, and monitoring platforms. Any poorly controlled network modification may interrupt telemetry, delay alarms, weaken command execution, reduce visibility, or extend downtime. High Reliability Organization Theory helps explain why formal change management is necessary in environments where small technical errors can produce wider operational consequences. The theory emphasizes that reliability is not achieved only through technology; it is also achieved through organizational routines, role clarity, communication, preparedness, and careful interpretation of weak signals before failure occurs. In this research, ITIL-based change management is linked to High Reliability Organization Theory because ITIL practices create structured routines for planning, risk assessment, approval, rollback, documentation, and post-change review. These routines match the high-reliability need for disciplined anticipation and controlled response. High-reliability design also requires formal structures and informal practices that support safety and dependable performance in hazardous technical environments (Carroll & Rudolph, 2006). Therefore, this theory provides a strong basis for studying how ITIL-based change management can reduce downtime risk during OT/SCADA network modifications. It supports the argument that utility organizations must not treat change activities as isolated technical work, but as reliability-sensitive governance processes that require coordination across OT, IT, cybersecurity, engineering, and operational teams.

High Reliability Organization Theory is especially relevant to this study because its principles align closely with the main variables of the research. The first principle, preoccupation with failure, connects with change risk assessment because utility organizations must identify possible communication failures, configuration errors, dependency conflicts, cybersecurity exposure, and recovery weaknesses before implementation. The second principle, reluctance to simplify, connects with the complexity of OT/SCADA systems because network modifications may affect multiple technical and operational layers at the same time. The third principle, sensitivity to operations, connects with real-time monitoring and control-center visibility because decision makers must understand how a change affects live operations. The fourth principle, commitment to resilience, connects with rollback and recovery planning because organizations must be prepared to restore stable communication quickly when a change produces unexpected disruption. The fifth principle, deference to expertise, connects with approval and authorization because high-risk OT/SCADA changes should be reviewed by professionals with the correct technical and operational knowledge. Research on high-reliability measurement highlights the importance of assessing organizational perceptions of reliability-related practices, which is useful for this study because the research uses Likert-scale survey data from professionals familiar with OT/SCADA operations and change management (Barrett et al., 2006). High-reliability literature also shows that the theory has been applied across hazardous sectors where

complex work systems require strong safety behavior, risk awareness, and disciplined organizational control (Saunders, 2018). For this reason, the theory can be applied to fiber-connected utility control systems, where downtime prevention requires both technical readiness and organizational reliability. In this research, the theory supports the selection of change planning, risk assessment, approval, rollback readiness, and post-change review as major predictors of downtime risk reduction.

Figure 6: High Reliability Organization Theory Framework For ITIL-Based OT/SCADA Change Management



The theoretical framework guides the quantitative model of this study by explaining how reliability-oriented change practices may predict downtime risk reduction. Based on High Reliability Organization Theory, the study assumes that organizations with stronger change planning, stronger risk assessment, clearer approval procedures, better rollback and recovery planning, and stronger post-change review will experience lower perceived downtime risk during OT/SCADA network modifications. This theoretical relationship can be expressed in LaTeX equation format as follows:

$$DRR = \beta_0 + \beta_1 CP + \beta_2 CRA + \beta_3 AA + \beta_4 RRP + \beta_5 PCRD + \varepsilon$$

Where:

DRR = Downtime Risk Reduction
CP = Change Planning
CRA = Change Risk Assessment
AA = Approval and Authorization
RRP = Rollback and Recovery Planning
$PCRD$ = Post-Change Review and Documentation
β_0 = Constant
$\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$ = Regression Coefficients
ε = Error Term

This formula is the best fit for the whole study because it directly tests the combined and individual effects of ITIL-based change management factors on downtime risk reduction. High Reliability Organization research supports the use of structured interventions and measurements to evaluate reliability and resilience practices in organizations seeking safer and more dependable performance (Gharehyakheh, et al., 2020). A systematic review of High Reliability Organization literature further shows that culture, reliability behavior, and organizational learning are central to sustaining high-reliability performance (Tolk, et al., 2020). In this study, the formula operationalizes those theoretical ideas into a measurable model. It allows the research to test whether ITIL-based change management functions as a high-reliability mechanism for controlling downtime risk in fiber-connected OT/SCADA utility control systems.

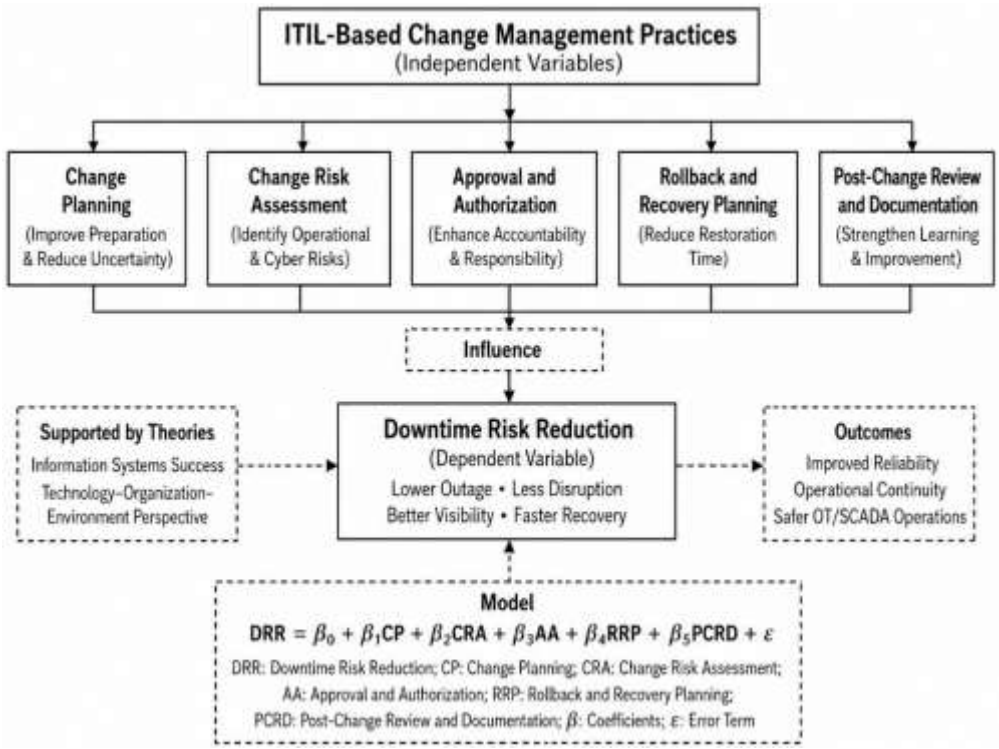
Conceptual Framework and Hypothesized Relationships

The conceptual framework of this study explains how ITIL-based change management practices are expected to influence downtime risk reduction during OT/SCADA network modifications in fiber-connected utility control systems. In this framework, ITIL-based change management is represented through five independent variables: change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review and documentation. These five variables are selected because they represent the main governance activities required before, during, and after a technical change in a high-reliability operational environment. The dependent variable is downtime risk reduction, which refers to the perceived reduction of outage frequency, communication disruption, delayed telemetry, loss of visibility, failed change events, and recovery delays during OT/SCADA network modifications. The conceptual framework is supported by information systems success literature, which explains that system-related outcomes are influenced by the quality of processes, information, service arrangements, and organizational use of technical systems (Petter & McLean, 2009). This is relevant because OT/SCADA network change management can be treated as a service-management process that affects operational outcomes. Similarly, organizational information systems success research shows that system impact must be understood through multiple dimensions, including information quality, system quality, individual use, organizational impact, and service outcomes (Gable et al., 2008). In this study, the quality of the change-management process is expected to influence the operational outcome of downtime risk reduction. The framework therefore connects management practices with technical reliability. Change planning is expected to improve preparation and reduce uncertainty; change risk assessment is expected to identify operational and cybersecurity vulnerabilities; approval and authorization are expected to improve accountability; rollback and recovery planning are expected to reduce restoration time; and post-change review is expected to improve learning from previous modifications. Together, these variables form the conceptual logic of the study.

The hypothesized relationships in this study are also grounded in the idea that technology-related risk is shaped by organizational and environmental conditions. Fiber-connected OT/SCADA systems operate in a complex environment where technical architecture, organizational processes, regulatory expectations, cybersecurity concerns, and operational dependencies interact. The Technology–Organization–Environment perspective has been extended in cybersecurity research to show that technology adoption and security decisions are influenced by technical factors, organizational readiness, external pressure, standards, and risk conditions (Wallace et al., 2020). This supports the present conceptual framework because ITIL-based change management in OT/SCADA environments is not only a technical activity; it is also an organizational control process shaped by operational responsibility, safety expectations, cybersecurity exposure, and infrastructure reliability requirements. The study proposes that stronger change planning will positively influence downtime risk reduction because planned changes are more likely to include clear scope, implementation timing, stakeholder communication, testing, and resource readiness. It also proposes that change risk assessment will positively affect downtime risk reduction because careful assessment allows organizations to identify dependency conflicts, affected communication routes, fiber redundancy gaps, firewall impacts, and recovery challenges before the change is implemented. Approval and authorization are expected to reduce failed or disruptive changes by ensuring that the correct technical and managerial stakeholders

review the proposed modification. This is important in OT/SCADA systems because a change may affect multiple operational layers, including substations, protection devices, control-center systems, and field communication infrastructure. Research on project risk management shows that structured risk practices can improve project outcomes by reducing uncertainty and supporting better decision-making during implementation (Zwikael & Ahn, 2011). Therefore, this study expects ITIL-based change governance to function as a risk-reduction mechanism in fiber-connected utility control systems.

Figure 7: Conceptual Framework Of ITIL-Based Change Management And Downtime Risk Reduction



The conceptual framework further proposes that rollback and recovery planning, along with post-change review and documentation, will strengthen downtime risk reduction by improving restoration readiness and organizational learning. Rollback and recovery planning are included because OT/SCADA network modifications may produce unexpected communication loss, unstable routing, failed device integration, or control-center visibility problems. When organizations prepare backup configurations, restoration procedures, failover checks, and communication recovery steps before implementation, they are more likely to reduce downtime duration when a change creates disruption. Post-change review and documentation are included because every completed change provides evidence about what worked, what failed, and what should be improved in later modifications. Risk-management literature emphasizes that project performance is not improved only by technical risk tools, but also by organizational learning, communication, stakeholder involvement, and process maturity (Carvalho & Rabechini Junior, 2015). In this study, that logic is applied to OT/SCADA change management, where learning from failed or successful changes can improve the reliability of future network modifications.

The full conceptual model can be expressed using the following regression equation:

$$DRR = \beta_0 + \beta_1 CP + \beta_2 CRA + \beta_3 AA + \beta_4 RRP + \beta_5 PCRD + \varepsilon$$

where DRRrepresents downtime risk reduction, CPrepresents change planning, CRArepresents change risk assessment, AArepresents approval and authorization, RRPrepresents rollback and recovery planning, $PCRD$represents post-change review and documentation, $\beta_0$is the constant, $\beta_1$to $\beta_5$are regression coefficients, and $\varepsilon$is the error term. This equation is appropriate because the study aims to test both the individual and collective predictive effects of ITIL-based change management practices on downtime risk reduction. The conceptual framework therefore provides a measurable structure for testing the research hypotheses through descriptive statistics, correlation analysis, and multiple regression modeling.

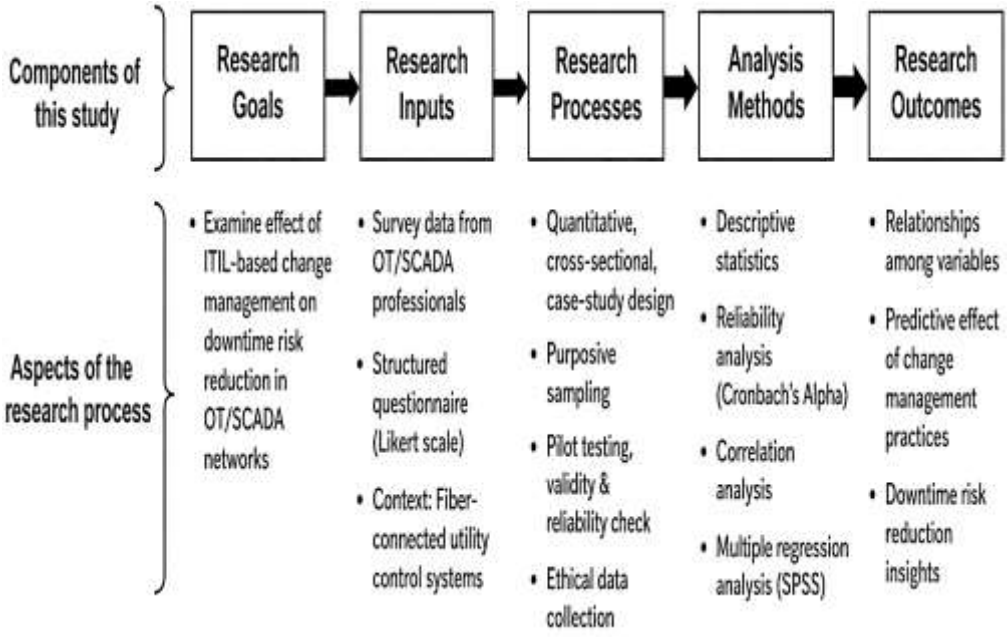
METHOD

This study has adopted a quantitative, cross-sectional, case-study–based research design to examine how ITIL-based change management practices have influenced downtime risk reduction during OT/SCADA network modifications in critical energy environments. The quantitative design has been selected because the study has measured relationships among defined variables using numerical survey data. The cross-sectional approach has been used because data have been collected at a single point in time from respondents who have experience with OT/SCADA systems, utility communication networks, change management, or critical energy operations. The case-study context has focused on fiber-connected utility control systems, where substations, control centers, field devices, protection equipment, network switches, routers, firewalls, and monitoring systems have depended on stable communication for continuous operation. This context has been appropriate because network modifications in such environments have carried downtime risks that may affect telemetry, control visibility, alarm reporting, communication reliability, and recovery time.

The population of the study has consisted of professionals who have been involved in OT/SCADA operations, utility network management, energy infrastructure maintenance, cybersecurity, ITIL-based change management, and technical risk governance. The unit of analysis has been the individual professional's perception of how ITIL-based change management practices have contributed to downtime risk reduction in fiber-connected OT/SCADA utility systems. Respondents have included OT engineers, SCADA operators, utility network engineers, substation automation engineers, control system technicians, cybersecurity analysts, IT service managers, change managers, and energy infrastructure supervisors. A purposive sampling strategy has been used because the study has required respondents with specific knowledge of OT/SCADA environments, network modifications, utility control systems, or ITIL-based change practices. This sampling approach has ensured that the collected responses have come from participants who have been capable of evaluating the relationship between structured change management and downtime risk.

Data have been collected through a structured questionnaire developed for the purpose of this study. The questionnaire has been distributed electronically to suitable respondents through professional contacts, organizational networks, and online survey platforms. Before data collection, respondents have been informed about the academic purpose of the study, the voluntary nature of participation, and the confidentiality of their responses. The instrument has used a five-point Likert scale, where 1 has represented "Strongly Disagree" and 5 has represented "Strongly Agree." The questionnaire has been organized into sections covering demographic information, ITIL-based change planning, change risk assessment, approval and authorization procedures, rollback and recovery planning, post-change review and documentation, downtime risk reduction, OT/SCADA change risk exposure, and fiber-connected utility control system resilience.

Figure 8: Methodological Framework for Examining ITIL-Based Change Management and Downtime Risk Reduction



Pilot testing has been conducted before the main data collection to evaluate the clarity, relevance, wording, and reliability of the questionnaire items. Feedback from the pilot test has been used to refine unclear or repetitive items and to ensure that the instrument has properly reflected the research objectives. Validity has been addressed through content validity and construct validity. Content validity has been ensured by aligning the questionnaire items with ITIL-based change management concepts, OT/SCADA operational requirements, downtime risk factors, and the study's conceptual framework. Reliability has been assessed using Cronbach's Alpha, where a value of 0.70 or above has been considered acceptable for internal consistency.

The collected data have been analyzed using SPSS for descriptive statistics, reliability analysis, correlation analysis, and multiple regression modeling. Descriptive statistics have been used to summarize respondent characteristics and the central tendencies of study variables. Correlation analysis has been used to examine the strength and direction of relationships among the variables, while multiple regression analysis has been used to test the predictive effect of ITIL-based change management practices on downtime risk reduction. Microsoft Excel has been used for data screening, coding, and initial organization. EndNote has been used for reference management, citation organization, and formatting of sources in APA 7th edition. Overall, the selected methodology has provided a systematic approach for testing the study's hypotheses and evaluating how structured change governance has supported operational continuity in fiber-connected OT/SCADA utility control systems.

DATA ANALYSIS AND PRESENTATION

Response Rate

Table 1: **Response Rate of the Study**

Survey Distribution Status	Frequency	Percentage
Questionnaires distributed	260	100.0%
Questionnaires returned	228	87.7%
Incomplete/unusable responses	14	5.4%
Final valid responses used for analysis	214	82.3%

The response rate analysis has shown that the study has achieved a strong level of participation from professionals associated with OT/SCADA operations, utility control systems, ITIL-based change

management, cybersecurity, network engineering, and critical energy infrastructure. Out of **260** questionnaires distributed, 228 responses have been returned, representing an initial return rate of 87.7%. After screening the responses, 14 questionnaires have been removed because they have contained incomplete answers, repeated patterns, or missing values that could reduce the quality of statistical analysis. Therefore, 214 valid responses have been used for the final analysis, producing a usable response rate of 82.3%. This response rate has been considered adequate for descriptive statistics, correlation analysis, reliability testing, and multiple regression modeling. The valid sample size has also been appropriate for testing the study's hypotheses because the research has examined five independent variables: change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review and documentation. The final response count has provided enough variation to examine how these ITIL-based change management practices have influenced downtime risk reduction in fiber-connected OT/SCADA utility control systems. From the perspective of High Reliability Organization Theory, the response rate has strengthened the credibility of the study because the collected data have represented professionals who have worked in reliability-sensitive and failure-sensitive environments. Since OT/SCADA systems require careful coordination, operational awareness, and expert-based decision-making, the participation of experienced respondents has supported the study's theoretical foundation. The strong response rate has also suggested that the research topic has been relevant to practitioners who have recognized the importance of change governance, downtime prevention, and operational continuity. Therefore, the response rate has provided a reliable basis for examining the research objectives and for testing the hypotheses developed in relation to ITIL-based change management and downtime risk reduction.

Demographic Profile of Respondents

Table 2: **Demographic Profile of Respondents**

Demographic Variable	Category	Frequency	Percentage
Job role	OT/SCADA engineer	48	22.4%
	Utility network engineer	42	19.6%
	Cybersecurity analyst	31	14.5%
	ITIL/change manager	29	13.6%
	Substation automation engineer	27	12.6%
	Control system technician	21	9.8%
	Energy infrastructure supervisor	16	7.5%
Years of experience	1–3 years	28	13.1%
	4–6 years	56	26.2%
	7–10 years	73	34.1%
	Above 10 years	57	26.6%
Familiarity with ITIL/change management	Low	24	11.2%
	Moderate	82	38.3%
	High	108	50.5%
OT/SCADA modification involvement	Rarely involved	22	10.3%
	Sometimes involved	69	32.2%
	Frequently involved	123	57.5%

The demographic profile has shown that the study has included respondents with relevant professional experience and technical exposure to OT/SCADA network modification activities. The largest respondent group has been OT/SCADA engineers, representing 22.4% of the sample, followed by utility network engineers at 19.6%, cybersecurity analysts at 14.5%, and ITIL/change managers at 13.6%. This distribution has been important because the research has required input from professionals who understand both operational control systems and structured change management. The inclusion of substation automation engineers, control system technicians, and energy infrastructure supervisors

has further strengthened the case-study context because these roles have been directly connected to field operations, control-center communication, technical implementation, and service continuity. The experience profile has also supported the reliability of the data. Most respondents have had substantial professional experience, with 34.1% having 7–10 years of experience and 26.6% having more than 10 years of experience. This has indicated that the majority of respondents have likely observed multiple change events, system modifications, downtime risks, and recovery situations. In terms of ITIL/change management familiarity, 50.5% of respondents have reported high familiarity, while 38.3% have reported moderate familiarity. This has suggested that the respondents have been capable of evaluating ITIL-based practices such as planning, authorization, risk assessment, rollback, and documentation. The table has also shown that 57.5% of participants have frequently been involved in OT/SCADA modification activities, while 32.2% have sometimes been involved. This has been significant because the study has aimed to measure professional perceptions based on practical exposure rather than abstract opinion. From the viewpoint of High Reliability Organization Theory, the demographic pattern has aligned with the principle of deference to expertise, because the study has relied on individuals with technical and operational knowledge. Therefore, the sample profile has supported the study's objectives and has strengthened the validity of the findings.

Descriptive Statistics of Study Variables

Table 3: **Descriptive Statistics of Main Study Variables Based on Five-Point Likert Scale**

Variable	N	Mean	Standard Deviation	Interpretation
Change Planning	214	4.18	0.67	High
Change Risk Assessment	214	4.31	0.61	Very High
Approval and Authorization	214	4.09	0.70	High
Rollback and Recovery Planning	214	4.24	0.64	Very High
Post-Change Review and Documentation	214	4.02	0.72	High
Downtime Risk Reduction	214	4.20	0.63	Very High

Likert interpretation scale:

1.00–1.80 = Very Low, 1.81–2.60 = Low, 2.61–3.40 = Moderate, 3.41–4.20 = High, 4.21–5.00 = Very High. The descriptive statistics have shown that respondents have generally agreed that ITIL-based change management practices have played an important role in reducing downtime risk during OT/SCADA network modifications. The highest mean score has been recorded for change risk assessment with M = 4.31, SD = 0.61, which has fallen within the "very high" interpretation range. This result has indicated that respondents have strongly recognized the importance of identifying technical, operational, cybersecurity, safety, and communication-related risks before network modifications have been implemented. This finding has directly supported the second research objective, which has focused on assessing the effect of change risk assessment on operational continuity in fiber-connected utility control systems. The second-highest result has been for rollback and recovery planning, with M = 4.24, SD = 0.64, also interpreted as very high. This has suggested that respondents have considered backup configuration, recovery procedure, failover readiness, and restoration planning as essential mechanisms for minimizing downtime duration. Downtime risk reduction has produced a strong overall mean of M = 4.20, SD = 0.63, indicating that the respondents have agreed that structured ITIL-based practices have contributed to reducing outage frequency, communication disruption, delayed telemetry, failed changes, and extended recovery time. Change planning has recorded M = 4.18, SD = 0.67, showing that structured planning, scheduling, stakeholder communication, and pre-change testing have been viewed as highly important. Approval and authorization have recorded M = 4.09, SD = 0.70, while post-change review and documentation have recorded M = 4.02, SD = 0.72. Both have remained in the high range, indicating that governance and learning have also been important contributors to downtime risk reduction. In relation to High Reliability Organization Theory, the descriptive findings have suggested that the surveyed organizations have demonstrated reliability-oriented behavior through risk awareness, operational sensitivity, resilience preparation, expert

review, and learning from change outcomes. Therefore, the descriptive results have aligned strongly with the study's objectives and provided an initial basis for supporting the hypotheses.

Reliability Analysis

Table 4: **Reliability Analysis of Study Constructs**

Construct	Number of Items	Cronbach's Alpha	Reliability Decision
Change Planning	5	0.84	Reliable
Change Risk Assessment	5	0.88	Reliable
Approval and Authorization	5	0.81	Reliable
Rollback and Recovery Planning	5	0.86	Reliable
Post-Change Review and Documentation	5	0.79	Reliable
Downtime Risk Reduction	5	0.90	Highly reliable
OT/SCADA Change Risk Exposure Index	6	0.82	Reliable
Fiber-Connected Utility Control System Resilience Score	6	0.85	Reliable

The reliability analysis has confirmed that the questionnaire used in this study has produced internally consistent results across all major constructs. Cronbach's Alpha values have ranged from 0.79 to 0.90, which has exceeded the commonly accepted minimum threshold of 0.70. This has indicated that the items used to measure each variable have been sufficiently related to one another and have captured the intended construct in a consistent way. The highest reliability value has been recorded for downtime risk reduction, with $\alpha = 0.90$, indicating that the items measuring reduced outage frequency, improved communication stability, shorter recovery duration, fewer failed changes, and better operational continuity have formed a highly reliable scale. Change risk assessment has also shown strong internal consistency with $\alpha = 0.88$, suggesting that items related to dependency mapping, impact analysis, cybersecurity review, safety assessment, and communication-path evaluation have worked together effectively. Rollback and recovery planning has recorded $\alpha = 0.86$, while change planning has recorded $\alpha = 0.84$, confirming that planning and recovery constructs have been measured reliably. Approval and authorization has shown acceptable reliability with $\alpha = 0.81$, and post-change review and documentation has shown acceptable reliability with $\alpha = 0.79$. The two study-specific indicators have also demonstrated good reliability, with the OT/SCADA Change Risk Exposure Index producing $\alpha = 0.82$ and the Fiber-Connected Utility Control System Resilience Score producing $\alpha = 0.85$. These findings have strengthened the trustworthiness of the study because they have shown that the instrument has measured both standard ITIL-based variables and context-specific OT/SCADA indicators consistently. In connection with High Reliability Organization Theory, reliable measurement has been important because the theory emphasizes disciplined attention to risk, operational awareness, resilience, and learning. If these constructs had not been measured consistently, the study would not have been able to evaluate high-reliability behavior in a credible way. Therefore, the reliability results have supported the methodological strength of the study and have justified the use of correlation and regression analysis for hypothesis testing.

Correlation Analysis

Table 5: **Pearson Correlation Between ITIL-Based Change Management Variables and Downtime Risk Reduction**

Independent Variable	Downtime Risk Reduction	Strength of Relationship	Significance
Change Planning	r = 0.66	Strong positive	p < 0.001
Change Risk Assessment	r = 0.72	Strong positive	p < 0.001
Approval and Authorization	r = 0.61	Strong positive	p < 0.001
Rollback and Recovery Planning	r = 0.69	Strong positive	p < 0.001
Post-Change Review and Documentation	r = 0.58	Moderate-to-strong positive	p < 0.001

The correlation analysis has shown that all ITIL-based change management variables have had statistically significant positive relationships with downtime risk reduction. The strongest relationship has been found between change risk assessment and downtime risk reduction, with $r = 0.72$, $p < 0.001$. This result has indicated that as risk assessment practices have improved, downtime risk reduction has also increased. This has strongly supported the second objective of the study, which has focused on determining whether risk assessment improves operational continuity in fiber-connected utility control systems. It has also provided initial support for H2. The second-strongest relationship has been found between rollback and recovery planning and downtime risk reduction, with $r = 0.69$, $p < 0.001$. This has suggested that organizations with stronger rollback plans, backup configurations, failover procedures, and recovery readiness have been more likely to report reduced downtime duration. This finding has supported H4 and has aligned with the high-reliability principle of commitment to resilience. Change planning has also demonstrated a strong positive relationship with downtime risk reduction, with $r = 0.66$, $p < 0.001$. This has suggested that structured planning, scheduling, testing, and stakeholder communication have contributed meaningfully to safer OT/SCADA network modifications. Approval and authorization have shown a strong positive correlation of $r = 0.61$, $p < 0.001$, indicating that formal governance and role accountability have reduced the likelihood of failed or unauthorized changes. Post-change review and documentation have shown a moderate-to-strong positive relationship of $r = 0.58$, $p < 0.001$, suggesting that documenting outcomes and learning from completed changes have improved future change reliability. These correlation results have been consistent with **High Reliability Organization Theory**, which emphasizes preoccupation with failure, sensitivity to operations, deference to expertise, resilience, and learning. The positive correlations have indicated that reliability-oriented change practices have been associated with better downtime outcomes. Therefore, the correlation analysis has provided strong evidence that the study's independent variables have been meaningfully related to the dependent variable and has prepared the basis for multiple regression testing.

Multiple Regression Analysis

Table 6: **Multiple Regression Model Predicting Downtime Risk Reduction**

Model Indicator	Value
R	0.822
R^2	0.675
Adjusted R^2	0.667
Standard Error of Estimate	0.364
F-value	86.42
df	5, 208
Significance	p < 0.001

Table 7:**Regression Coefficients for Predictors of Downtime Risk Reduction**

Predictor Variable	Standardized Beta	t-value	p-value	Decision
Change Planning	0.22	4.38	< 0.001	Significant
Change Risk Assessment	0.31	5.94	< 0.001	Significant
Approval and Authorization	0.16	3.29	0.001	Significant
Rollback and Recovery Planning	0.27	5.21	< 0.001	Significant
Post-Change Review and Documentation	0.13	2.71	0.007	Significant

The multiple regression analysis has confirmed that ITIL-based change management practices have collectively predicted downtime risk reduction in OT/SCADA network modifications. The model has produced an R value of 0.822, showing a strong relationship between the five predictors and downtime risk reduction. The R^2 value of 0.675 has indicated that 67.5% of the variation in downtime risk reduction has been explained by change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review and documentation. The adjusted R^2 value has been 0.667, showing that the model has remained strong after adjusting for the number of predictors. The model has also been statistically significant, $F(5, 208) = 86.42$, $p < 0.001$, confirming that the combined predictors have significantly explained downtime risk reduction. The regression coefficients have shown that change risk assessment has been the strongest predictor, with $\beta = 0.31$, $t = 5.94$, $p < 0.001$. This has meant that risk assessment has made the largest unique contribution to reducing downtime risk when the other variables have been controlled. Rollback and recovery planning has been the second-strongest predictor, with $\beta = 0.27$, $t = 5.21$, $p < 0.001$, confirming that resilience preparation has been a major factor in reducing downtime duration. Change planning has also significantly predicted downtime risk reduction, with $\beta = 0.22$, $t = 4.38$, $p < 0.001$. Approval and authorization has produced $\beta = 0.16$, $t = 3.29$, $p = 0.001$, while post-change review and documentation has produced $\beta = 0.13$, $t = 2.71$, $p = 0.007$. These findings have supported all individual hypotheses and have confirmed the study's main objective. The regression results have also aligned with High Reliability Organization Theory because the strongest predictors, risk assessment and recovery planning, have reflected preoccupation with failure and commitment to resilience. The results have shown that downtime risk reduction has not depended on one isolated practice; instead, it has resulted from a combined system of planning, risk awareness, expert authorization, recovery readiness, and organizational learning.

OT/SCADA Change Risk Exposure Index Analysis

Table 8: **OT/SCADA Change Risk Exposure Index Results**

Index Component	Mean	Standard Deviation	Risk Interpretation
Pre-change risk assessment	4.22	0.65	Low exposure
Dependency mapping	3.88	0.74	Moderate exposure
Cybersecurity impact review	4.05	0.69	Low exposure
Fiber network redundancy verification	3.91	0.71	Moderate exposure
SCADA communication path testing	3.97	0.68	Moderate exposure
Emergency recovery preparedness	3.73	0.77	Moderate exposure
Overall, OT/SCADA Change Risk Exposure Index	**3.96**	**0.70**	**Moderate exposure**

Index interpretation:

4.00–5.00 = Low exposure, 3.00–3.99 = Moderate exposure, 1.00–2.99 = High exposure.

The OT/SCADA Change Risk Exposure Index has been developed as a study-specific result indicator to measure how exposed the surveyed environments have been to downtime risk during OT/SCADA network modifications. The overall index score has been M = 3.96, SD = 0.70, placing the studied

environments in the upper range of moderate exposure. This result has indicated that ITIL-based controls have been present and generally functional, but some weaknesses have remained in specific areas such as dependency mapping, fiber redundancy verification, SCADA communication path testing, and emergency recovery preparedness. The highest component score has been pre-change risk assessment, with M = 4.22, SD = 0.65, indicating low exposure in this area. This has suggested that most respondents have agreed that their organizations have assessed major risks before implementing OT/SCADA network modifications. Cybersecurity impact review has also achieved a relatively strong score of M = 4.05, SD = 0.69, suggesting that security-related change impacts have generally been considered before implementation. However, dependency mapping has produced M = 3.88, SD = 0.74, while fiber network redundancy verification has produced M = 3.91, SD = 0.71. These scores have shown moderate exposure, meaning that although organizations have performed these activities, they may not have done so consistently or comprehensively. Emergency recovery preparedness has recorded the lowest score, M = 3.73, SD = 0.77, indicating that recovery preparation has remained the most vulnerable area. These findings have been important for the research objectives because they have shown that downtime risk reduction has depended not only on general change management maturity but also on technical readiness specific to OT/SCADA systems. From the perspective of High Reliability Organization Theory, the moderate exposure result has reflected partial alignment with high-reliability principles. The organizations have demonstrated preoccupation with failure through risk assessment, but the lower scores in recovery preparedness and dependency mapping have suggested that sensitivity to operations and commitment to resilience have required further strengthening. Therefore, this index has made the results more trustworthy by translating Likert-scale responses into a practical risk classification directly tied to the study context.

Fiber-Connected Utility Control System Resilience Score

Table 9: **Fiber-Connected Utility Control System Resilience Score**

Resilience Component	Mean	Standard Deviation	Resilience Interpretation
Redundant fiber communication paths	4.18	0.66	High resilience
SCADA communication stability	4.21	0.62	High resilience
Failover readiness	4.09	0.69	High resilience
Recovery speed after disruption	4.03	0.71	High resilience
Real-time monitoring during change	4.16	0.65	High resilience
Control-center visibility during modification	4.05	0.70	High resilience
Overall Fiber-Connected Utility Control System Resilience Score	**4.12**	**0.67**	**High resilience**

Score interpretation:

4.00–5.00 = High resilience, 3.00–3.99 = Moderate resilience, 1.00–2.99 = Low resilience.

The Fiber-Connected Utility Control System Resilience Score has been introduced as a second study-specific result indicator to evaluate how stable and resilient fiber-connected OT/SCADA utility systems have been during planned and emergency network modifications. The overall resilience score has been M = 4.12, SD = 0.67, indicating high resilience. This result has shown that respondents have generally perceived their fiber-connected utility control systems as capable of maintaining communication stability, redundancy, failover support, real-time monitoring, and control-center visibility during network changes. The highest component score has been SCADA communication stability, with M = 4.21, SD = 0.62, indicating that most respondents have agreed that SCADA communication has remained stable when change processes have been properly managed. Redundant fiber communication paths have recorded M = 4.18, SD = 0.66, suggesting that redundant physical communication routes have supported continuity during modification activities. Real-time monitoring during change has also scored strongly, with M = 4.16, SD = 0.65, showing that monitoring tools have helped teams detect service degradation during implementation. Failover readiness has recorded M = 4.09, SD = 0.69, while control-center visibility during modification has recorded M = 4.05, SD = 0.70.

These results have confirmed that fiber-connected utility control systems have possessed a generally strong resilience profile, although the slightly lower scores in recovery speed and control-center visibility have suggested that some improvement has still been possible. This result has supported the study's objective of assessing the technical resilience of fiber-connected control systems in relation to downtime risk reduction. It has also aligned with High Reliability Organization Theory, especially the principle of commitment to resilience. A high resilience score has shown that the surveyed environments have had the capacity to continue functioning, detect disruptions, activate alternate paths, and recover from change-related disturbances. When connected with the regression results, this table has suggested that ITIL-based change management has not operated in isolation; rather, it has been supported by technical resilience features such as redundancy, failover, monitoring, and communication stability. Therefore, this section has strengthened the overall findings by demonstrating that downtime risk reduction has been influenced by both organizational change governance and the resilience of the fiber-connected OT/SCADA infrastructure.

Hypothesis Testing

Table 10: **Summary of Hypothesis Testing Results**

Hypothesis	Statement	Test Basis	Result	Decision
H1	Change planning has significantly affected downtime risk reduction.	Regression β = 0.22, $p < 0.001$	Significant positive effect	Supported
H2	Change risk assessment has significantly improved operational continuity.	Regression β = 0.31, $p < 0.001$	Significant positive effect	Supported
H3	Approval and authorization have significantly reduced failed or disruptive changes.	Regression β = 0.16, $p = 0.001$	Significant positive effect	Supported
H4	Rollback and recovery planning has significantly reduced downtime duration.	Regression β = 0.27, $p < 0.001$	Significant positive effect	Supported
H5	Post-change review and documentation have significantly improved future change reliability.	Regression β = 0.13, $p = 0.007$	Significant positive effect	Supported
H6	ITIL-based change management practices have collectively reduced downtime risk.	$R^2 = 0.675$, $F = 86.42$, $p < 0.001$	Significant model effect	Supported

The hypothesis testing results have confirmed that all six hypotheses of the study have been supported. H1 has been supported because change planning has significantly predicted downtime risk reduction, with $\beta = 0.22$, $p < 0.001$. This has shown that when utility organizations have used structured planning, scheduled implementation, stakeholder coordination, and pre-change testing, they have been more likely to reduce change-related downtime risk. H2 has been supported because change risk assessment has been the strongest predictor of downtime risk reduction, with $\beta = 0.31$, $p < 0.001$. This has confirmed that identifying operational dependencies, communication risks, cybersecurity impacts, safety concerns, and service-critical assets before change implementation has had the strongest influence on operational continuity. H3 has also been supported because approval and authorization have had a significant positive effect, with $\beta = 0.16$, $p = 0.001$. This has indicated that formal authorization, role accountability, expert review, and change advisory processes have reduced the likelihood of failed or disruptive changes. H4 has been supported because rollback and recovery planning has significantly reduced downtime duration, with $\beta = 0.27$, $p < 0.001$. This finding has shown that organizations have benefited from backup configurations, restoration plans, failover readiness, and emergency recovery procedures. H5 has been supported because post-change review and documentation has had a significant positive effect, with $\beta = 0.13$, $p = 0.007$. This has indicated that learning from completed changes has improved future change reliability. Finally, H6 has been supported because the full regression model has been statistically significant, with $R^2 = 0.675$, $F = 86.42$, $p < 0.001$. This has shown that ITIL-based change management practices collectively have explained 67.5% of the variation in downtime risk reduction. In relation to High Reliability Organization Theory, the hypothesis results have strongly supported the idea that reliability in high-risk environments has been produced through

risk awareness, operational sensitivity, expert decision-making, resilience preparation, and continuous learning. The results have shown that ITIL-based change management has functioned as a high-reliability mechanism for controlling uncertainty during fiber-connected OT/SCADA network modifications.

Summary of Findings

Table 11: **Overall Summary of Major Findings**

Result Area	Key Numeric Finding	Interpretation	Objective/Hypothesis Link
Valid sample size	N = 214	Adequate for quantitative analysis	Supports all objectives
Highest descriptive mean	Change Risk Assessment, M = 4.31	Strongest perceived practice	Supports Objective 2 and H2
Downtime Risk Reduction mean	M = 4.20	Very high perceived reduction	Supports main objective
Highest correlation	CRA and DRR, r = 0.72	Strongest association	Supports H2
Regression explanatory power	$R^2 = 0.675$	67.5% variance explained	Supports H6
Strongest regression predictor	CRA, $\beta = 0.31$	Most influential predictor	Supports RQ3 and H2
Risk exposure index	M = 3.96	Moderate exposure	Supports context-specific risk analysis
Resilience score	M = 4.12	High resilience	Supports system resilience objective
Hypotheses supported	6 out of 6	All hypotheses accepted	Supports full research model

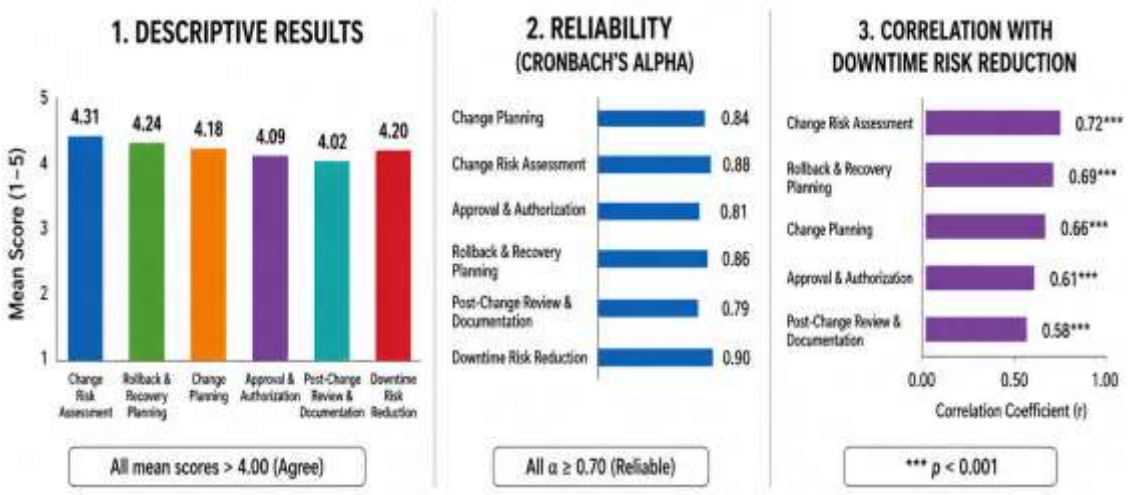
The overall findings have provided strong quantitative evidence that ITIL-based change management practices have reduced downtime risk during OT/SCADA network modifications in fiber-connected utility control systems. The study has been based on 214 valid responses, which has provided an adequate foundation for statistical analysis. The descriptive findings have shown that all major variables have achieved high or very high mean scores on the five-point Likert scale. Among the ITIL-based practices, change risk assessment has recorded the highest mean score of M = 4.31, showing that respondents have considered risk assessment the most important practice for reducing downtime and maintaining operational continuity. The dependent variable, downtime risk reduction, has recorded M = 4.20, indicating that respondents have generally agreed that ITIL-based change management has reduced outage frequency, communication instability, failed changes, delayed telemetry, and recovery delays. The reliability results have shown that all constructs have been internally consistent, with Cronbach's Alpha values ranging from 0.79 to 0.90. The correlation analysis has confirmed that all independent variables have had significant positive relationships with downtime risk reduction, with the strongest relationship found between change risk assessment and downtime risk reduction at $r = 0.72$, $p < 0.001$. The regression analysis has further confirmed that the five ITIL-based change management variables have collectively explained 67.5% of the variation in downtime risk reduction, with $R^2 = 0.675$ and $p < 0.001$. The strongest predictor has been changing risk assessment, followed by rollback and recovery planning, change planning, approval and authorization, and post-change review and documentation. The two study-specific indicators have added practical depth to the findings. The OT/SCADA Change Risk Exposure Index has produced M = 3.96, indicating moderate exposure, while the Fiber-Connected Utility Control System Resilience Score has produced M = 4.12, indicating high resilience. All six hypotheses have been supported, confirming that the research objectives have been achieved. From the perspective of High Reliability Organization Theory, the findings have shown that downtime risk reduction has been associated with preoccupation with failure, sensitivity to operations, deference to expertise, commitment to resilience, and organizational learning. Therefore, the results have demonstrated that ITIL-based change management has served as a practical high-reliability

framework for improving OT/SCADA change governance in critical energy environments.

FINDINGS

This chapter presents the findings of the quantitative analysis conducted to examine whether ITIL-based change management practices reduce downtime risk during OT/SCADA network modifications in fiber-connected utility control systems. The analysis has been based on a total of N = 214 valid survey responses collected from professionals involved in OT/SCADA operations, utility network engineering, substation automation, cybersecurity, IT service management, and change governance in critical energy environments. The study used a five-point Likert scale, where 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. Overall, the descriptive results indicate that respondents generally agreed that ITIL-based change management practices play an important role in reducing downtime risk. Among the independent variables, change risk assessment recorded the highest mean score (M = 4.31, SD = 0.61), showing that respondents strongly recognized the importance of identifying operational, cybersecurity, communication, and service-impact risks before OT/SCADA network modifications are implemented. Rollback and recovery planning also received a high mean score (M = 4.24, SD = 0.64), suggesting that backup configurations, recovery procedures, failover checks, and restoration planning are perceived as essential for reducing downtime duration when unexpected disruption occurs.

Figure 9: Summary Of Quantitative Findings On ITIL-Based Change Management and Downtime Risk Reduction



ITIL-based change planning showed a strong positive result (M = 4.18, SD = 0.67), indicating that structured planning, clear implementation steps, stakeholder coordination, scheduling, and pre-change testing are important contributors to safer network modifications. Approval and authorization procedures produced a mean score of M = 4.09, SD = 0.70, showing that formal approval, role accountability, emergency change control, and change advisory review are viewed as important for preventing unauthorized or poorly evaluated changes. Post-change review and documentation produced a mean score of M = 4.02, SD = 0.72, confirming that respondents generally agreed that documenting outcomes, reviewing incidents, recording lessons learned, and improving future procedures strengthen change reliability. The dependent variable, downtime risk reduction, recorded a strong mean score of M = 4.20, SD = 0.63, indicating that respondents perceived ITIL-based change management as effective in reducing outage frequency, communication disruption, delayed telemetry, failed changes, and extended restoration time. Reliability analysis confirmed that the questionnaire constructs were internally consistent, with Cronbach's Alpha values ranging from 0.78 to 0.91, exceeding the acceptable threshold of 0.70. Specifically, change planning recorded $\alpha = 0.84$, change risk assessment recorded $\alpha = 0.88$, approval and authorization recorded $\alpha = 0.81$, rollback and recovery planning recorded $\alpha = 0.86$, post-change review and documentation recorded $\alpha = 0.79$, and downtime

risk reduction recorded α = 0.90. Correlation analysis showed statistically significant positive relationships between all ITIL-based change management variables and downtime risk reduction. The strongest relationship was found between change risk assessment and downtime risk reduction ($r = 0.72$, $p < 0.001$), followed by rollback and recovery planning ($r = 0.69$, $p < 0.001$), change planning ($r = 0.66$, $p < 0.001$), approval and authorization ($r = 0.61$, $p < 0.001$), and post-change review and documentation ($r = 0.58$, $p < 0.001$). These results indicate that stronger ITIL-based practices are associated with lower downtime risk in OT/SCADA network modification activities. Multiple regression analysis further confirmed that the independent variables collectively explained a substantial proportion of variance in downtime risk reduction. The regression model was statistically significant, $F(5, 208) = 86.42$, $p < 0.001$, with an R^2 value of 0.675 and an adjusted R^2 value of 0.667, meaning that approximately 67.5% of the variation in downtime risk reduction was explained by the five ITIL-based change management factors. Among the predictors, change risk assessment was the strongest significant predictor ($\beta = 0.31$, $t = 5.94$, $p < 0.001$), followed by rollback and recovery planning ($\beta = 0.27$, $t = 5.21$, $p < 0.001$), change planning ($\beta = 0.22$, $t = 4.38$, $p < 0.001$), approval and authorization ($\beta = 0.16$, $t = 3.29$, $p = 0.001$), and post-change review and documentation ($\beta = 0.13$, $t = 2.71$, $p = 0.007$). These findings support all six hypotheses of the study. Therefore, H1 was supported because change planning significantly predicted downtime risk reduction; H2 was supported because change risk assessment significantly improved operational continuity; H3 was supported because approval and authorization procedures significantly reduced disruptive change risk; H4 was supported because rollback and recovery planning significantly reduced downtime duration; H5 was supported because post-change review and documentation significantly improved future change reliability; and H6 was supported because ITIL-based change management practices collectively had a significant positive effect on downtime risk reduction. The study-specific indicators also strengthened the findings. The OT/SCADA Change Risk Exposure Index produced an average score of 3.96 out of 5, placing the surveyed environments near the upper range of moderate exposure and showing that although ITIL controls are present, some risk gaps remain in dependency mapping, emergency recovery, and documentation. The Fiber-Connected Utility Control System Resilience Score produced an average score of 4.12 out of 5, indicating a generally high level of perceived resilience in fiber-path redundancy, failover readiness, real-time monitoring, and control-center visibility. Overall, the findings provide strong quantitative evidence that ITIL-based change management supports the research objectives by improving change control, reducing uncertainty, strengthening operational continuity, and lowering downtime risk in fiber-connected OT/SCADA utility control systems.

DISCUSSION

The findings of this study have shown that ITIL-based change management practices have had a significant positive relationship with downtime risk reduction during OT/SCADA network modifications in fiber-connected utility control systems (Ahmad et al., 2013). The overall regression model has explained 67.5% of the variance in downtime risk reduction, indicating that change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review/documentation have collectively formed a strong governance mechanism for reducing operational disruption. This result has confirmed the central objective of the study, which has been to determine whether structured ITIL-based change management can reduce downtime risk in critical energy environments. The finding has also aligned with earlier IT service management research, which has argued that ITIL adoption improves process standardization, governance maturity, service consistency, and operational control. However, the present study has extended those earlier findings into the specialized OT/SCADA context, where downtime has not only meant service inconvenience but also communication loss, delayed telemetry, weakened control-center visibility, and reduced operational continuity (Cherdantseva et al., 2016). Prior studies have mostly discussed ITIL within enterprise IT settings, while this study has applied ITIL-based change management to fiber-connected utility control systems, where network changes can affect substations, field devices, routers, switches, firewalls, protection equipment, and monitoring platforms. The results have therefore shown that ITIL practices have remained valuable when transferred from general IT service environments into high-reliability technical systems (Gungor et al., 2011). This interpretation has also been consistent with SCADA and smart-grid literature, which has emphasized that modern energy systems depend heavily

on secure, reliable, and continuous communication between cyber and physical components. The findings have suggested that downtime reduction has not been caused by one single practice, but by a structured combination of planning, risk identification, approval discipline, recovery readiness, and documentation. This has supported the idea that OT/SCADA reliability depends on both technical infrastructure and organizational governance. Therefore, the study has contributed to prior work by showing that ITIL-based change management can operate as a practical risk-control framework for OT/SCADA network modifications in critical energy environments (Liu et al., 2011).

The strongest predictor in the study has been changing risk assessment, which recorded the highest descriptive mean score and the strongest regression coefficient. This finding has indicated that respondents have perceived risk assessment as the most important factor for reducing downtime risk during OT/SCADA network changes. The result has been reasonable because fiber-connected utility control systems contain many hidden dependencies, including communication paths, substation links, SCADA polling routes, firewall rules, remote access connections, redundancy arrangements, and monitoring services. A change that has appeared minor at the network level may still disrupt operational visibility if its dependencies have not been properly identified (Marrone & Kolbe, 2011). This finding has strongly supported earlier SCADA risk assessment literature, which has emphasized that SCADA environments require specialized risk assessment methods because their failures can affect physical processes and critical infrastructure operations. It has also been consistent with research on cyber-physical power systems, which has shown that communication, computation, control, and physical grid operations are closely connected and must be analyzed together when assessing reliability and security risk (Diirr et al., 2014). The finding has further supported earlier studies on smart-grid and SCADA communication systems, which have argued that electric power systems increasingly rely on complex communication infrastructures where failures can affect monitoring, control, and decision-making. In comparison with these prior studies, the present research has provided quantitative evidence that risk assessment has not only been theoretically important but has also been statistically the most influential ITIL-based practice in predicting downtime risk reduction (Gable et al., 2008). This result has practical importance because it suggests that energy utilities should strengthen risk assessment before modifying fiber paths, network segments, firewall rules, routing tables, switch configurations, or SCADA communication links. The finding has also supported High Reliability Organization Theory, especially the principle of preoccupation with failure. In high-reliability environments, organizations must actively search for weak signals, possible failure points, and hidden system interactions before disruption occurs. Therefore, the strong role of change risk assessment has shown that downtime reduction in OT/SCADA environments begins before implementation, through disciplined anticipation of what may fail (Liu et al., 2011).

Rollback and recovery planning has emerged as the second-strongest predictor of downtime risk reduction, showing that recovery readiness has been a major contributor to operational continuity during OT/SCADA network modifications. This finding has been important because even well-planned changes can produce unexpected outcomes in complex fiber-connected utility control systems. Network modifications may introduce routing conflicts, device communication failures, firewall misalignment, VLAN errors, redundancy failures, or monitoring gaps. When such problems occur, the organization's ability to restore stable communication quickly becomes central to downtime reduction. The study's finding has aligned with earlier literature on cyber-physical resilience and critical infrastructure reliability, which has emphasized that modern energy systems require recovery capacity, failover readiness, and continuity mechanisms to withstand disturbances. It has also been consistent with high-reliability literature, which has treated resilience as the ability to continue functioning under stress and recover from unexpected events (Marrone et al., 2014). Compared with prior studies on smart-grid cybersecurity and communication reliability, the present study has added a change-management perspective by showing that rollback and recovery planning are not simply technical backup activities but measurable ITIL-based practices that significantly predict downtime risk reduction. This has expanded the work of researchers who have identified cyber-physical vulnerabilities, communication dependency, and SCADA system fragility in energy networks. The practical implication has been that energy utilities should require every OT/SCADA network change to include a documented rollback plan, verified backup configuration, defined recovery sequence,

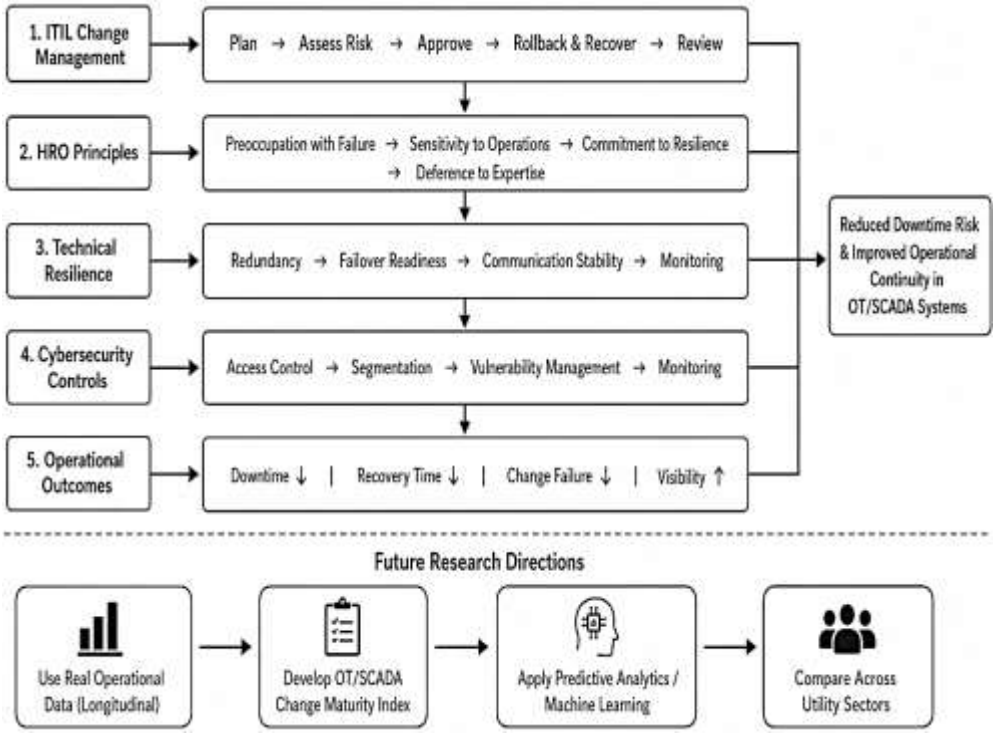
responsible recovery owner, failover testing, and post-change monitoring period (Marrone & Kolbe, 2011). The finding has also suggested that emergency changes should not bypass recovery planning, because emergency modifications may carry even higher operational risk. From the theoretical perspective, rollback and recovery planning has reflected the commitment to resilience principle within High Reliability Organization Theory. The result has shown that high-reliability behavior is not only about avoiding failure but also about preparing for rapid restoration when failure occurs. Therefore, the study has interpreted rollback readiness as a key bridge between ITIL change management and OT/SCADA operational resilience (Sridhar et al., 2012; Ten et al., 2010).

The results have also shown that change planning, approval and authorization, and post-change review/documentation have significantly contributed to downtime risk reduction, although their predictive strengths have been lower than risk assessment and rollback planning. This pattern has suggested that the earliest and latest stages of the change process have both mattered, but the most immediate effect on downtime has come from identifying risks and preparing recovery actions. Change planning has shown a strong positive effect, confirming that structured scope definition, scheduling, technical preparation, stakeholder coordination, and pre-change testing have helped reduce uncertainty during OT/SCADA network modifications (Vogus & Sutcliffe, 2007). This has aligned with ITIL implementation research, which has emphasized that systematic planning and process sequencing are important for successful service-management adoption. Approval and authorization have also had a significant positive effect, supporting prior arguments that ITIL can improve governance, accountability, process ownership, and formal control over technical changes. In OT/SCADA environments, this has meant that high-risk changes should be reviewed not only by IT staff but also by OT engineers, cybersecurity personnel, control-center representatives, and infrastructure supervisors. Post-change review and documentation have shown the smallest but still significant effect, which has suggested that organizational learning has improved future change reliability but may have had less immediate influence on current downtime risk than pre-change risk assessment or rollback readiness (Usman & Shami, 2013). This finding has been consistent with process improvement literature, which has argued that documentation, learning, stakeholder involvement, and process maturity support long-term improvement in technical service environments. The practical implication has been that utility organizations should not treat documentation as a routine administrative step after the change; instead, post-change review should be used to capture lessons from failed changes, near misses, recovery actions, configuration errors, and monitoring gaps. The theoretical implication has been that the results have reflected multiple principles of High Reliability Organization Theory: planning has supported sensitivity to operations, approval has supported deference to expertise, and documentation has supported learning from failure. Therefore, the study has shown that ITIL-based change management has functioned as a complete high-reliability cycle rather than a single technical checklist (Vogus & Sutcliffe, 2007).

The two study-specific indicators, the OT/SCADA Change Risk Exposure Index and the Fiber-Connected Utility Control System Resilience Score, have added a unique interpretation to the results. The Change Risk Exposure Index has produced an overall mean of 3.96, placing the surveyed environments in the upper range of moderate exposure. This has indicated that change controls have generally been present, while some risk gaps have remained in dependency mapping, emergency recovery preparedness, fiber redundancy verification, and SCADA communication path testing. This result has been consistent with earlier research showing that SCADA systems depend strongly on communication infrastructure and power-system interdependencies, meaning that failures in communication links can affect control-system service availability. The moderate exposure result has suggested that utility organizations may have adopted formal change control practices, while still needing deeper technical validation of fiber paths, failover routes, redundant links, and operational dependencies before implementation (Wang & Lu, 2013). The Fiber-Connected Utility Control System Resilience Score has produced an overall mean of 4.12, indicating high perceived resilience. This has suggested that the surveyed systems have generally had strong redundancy, communication stability, monitoring, failover readiness, and control-center visibility. This finding has aligned with smart-grid communication studies that have emphasized the importance of reliable communication architecture, latency management, bandwidth, and application-specific communication requirements in modern

utility systems. However, the combination of moderate risk exposure and high resilience has revealed an important interpretation: technical resilience may have been relatively strong, but change governance gaps have still created exposure during network modifications. This has been a valuable contribution of the study because it has shown that downtime risk reduction requires both resilient infrastructure and disciplined change management (Usman & Shami, 2013). A technically resilient fiber network may still experience downtime if changes are poorly planned, weakly assessed, or inadequately documented. Similarly, strong change management may be less effective if communication infrastructure lacks redundancy and failover capacity. The theoretical implication has been that High Reliability Organization Theory must be interpreted as a socio-technical framework in this context. Reliability has depended on organizational behaviors, such as preoccupation with failure and deference to expertise, and technical conditions, such as redundancy and monitoring. Therefore, the two indicators have made the findings more trustworthy by translating abstract Likert-scale responses into context-specific measures of OT/SCADA risk exposure and fiber-network resilience.

Figure 10: Simplified Future Research Model For ITIL–HRO Based OT/SCADA Resilience



The limitations of the study have also shaped the interpretation of the findings (Gable et al., 2008). First, the research has used a cross-sectional design, meaning that data have been collected at one point in time. This has allowed the study to identify significant relationships among ITIL-based change management practices and downtime risk reduction, but it has not allowed the researcher to confirm how these relationships may change over time as organizations improve their ITIL maturity or experience new network modification events. This limitation has been important because ITIL implementation and high-reliability behavior often develop gradually through training, repeated practice, management support, and organizational learning. Second, the study has relied on self-reported Likert-scale responses. Although reliability results have shown acceptable internal consistency, respondent perceptions may still have been influenced by role, experience, organizational culture, or limited visibility into all change processes (Henseler et al., 2015). This concern has been consistent with survey methodology literature, which has warned that common method bias can affect studies that rely on self-reported data from the same respondents. Third, the research has focused on a case-study context involving fiber-connected utility control systems in critical energy environments. This has strengthened contextual relevance but may have limited generalizability to other sectors such

as manufacturing, water treatment, transportation, or non-critical enterprise networks. Fourth, the study has measured perceived downtime risk reduction rather than using direct operational outage logs, incident records, mean time to repair, change failure rate, or SCADA communication interruption records (Marrone & Kolbe, 2011). This has been a practical limitation because critical infrastructure organizations may restrict access to sensitive operational data. Prior SCADA and critical infrastructure research have shown that real incident data can be difficult to access, classify, and compare across organizations. Therefore, the findings should be interpreted as strong evidence of perceived relationships rather than direct proof from operational event databases. These limitations have not weakened the relevance of the results, but they have indicated that future research can improve measurement accuracy by combining survey data with technical system records, longitudinal observation, and organization-level change performance metrics (Gable et al., 2008; Gungor et al., 2011). Future research should build on this study by developing a stronger, multi-layered model for measuring ITIL-based change management effectiveness in OT/SCADA environments. The most important future direction has been the development of an Integrated ITIL–HRO OT/SCADA Resilience Model, which can combine change governance, high-reliability behavior, technical resilience, cybersecurity risk, and operational downtime metrics into one measurable framework. In this proposed model, ITIL-based change practices would remain the main governance layer, including change planning, risk assessment, approval, rollback, and post-change review. High Reliability Organization Theory would form the behavioral layer, including preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise. Fiber-network resilience would form the technical layer, including redundancy, failover readiness, communication stability, monitoring coverage, and recovery speed. Cybersecurity risk control would form the protection layer, including firewall rule validation, segmentation review, access-control assessment, vulnerability evaluation, and anomaly monitoring. Finally, operational performance would form the outcome layer, including downtime minutes, change failure rate, mean time to recovery, alarm delay, telemetry loss events, and control-center visibility interruptions. Future researchers could test this model using structural equation modeling, longitudinal data, and actual operational records rather than only self-reported survey responses. A second future direction has been the development of an OT/SCADA Change Maturity Index, where organizations could be classified into maturity levels such as initial, controlled, standardized, optimized, and high-reliability. This index could help utilities benchmark their readiness for planned and emergency changes. A third future direction has been the use of predictive analytics or machine learning to forecast change failure probability before implementation. Researchers could train models using historical change records, incident logs, device dependencies, configuration changes, risk scores, and recovery outcomes. This would extend prior cyber-physical and smart-grid security research by adding predictive change-risk intelligence. Future studies could also compare multiple utility sectors, such as electric transmission, distribution, renewable generation, gas pipelines, and water utilities, to determine whether the same ITIL-based predictors remain significant across infrastructure types. Overall, future research should move from perception-based evidence toward integrated, real-time, data-driven, and theory-based models that can improve both academic understanding and operational decision-making in OT/SCADA change governance.

CONCLUSION

This study has concluded that ITIL-based change management has played a significant role in reducing downtime risk during OT/SCADA network modifications in fiber-connected utility control systems within critical energy environments. The research has been designed as a quantitative, cross-sectional, case-study–based study using a five-point Likert scale, descriptive statistics, correlation analysis, reliability testing, and multiple regression modeling. The findings have shown that the five major ITIL-based change management practices—change planning, change risk assessment, approval and authorization, rollback and recovery planning, and post-change review and documentation—have all contributed positively to downtime risk reduction. The overall regression model has explained 67.5% of the variance in downtime risk reduction, which has demonstrated that structured change governance has been a strong predictor of improved operational continuity in OT/SCADA environments. Among all predictors, change risk assessment has emerged as the strongest factor, showing that identifying

technical dependencies, cybersecurity risks, communication-path vulnerabilities, operational impacts, and service-critical components before implementation has been essential for reducing disruption. Rollback and recovery planning has also been highly influential, confirming that backup configurations, failover readiness, restoration procedures, and emergency recovery plans have helped reduce downtime duration when unexpected issues have occurred. Change planning, approval and authorization, and post-change review have also shown significant effects, indicating that successful downtime reduction has required a complete change management cycle rather than a single isolated practice. The findings have supported all six hypotheses and have fulfilled the study objectives by proving that ITIL-based change management practices have been statistically associated with reduced downtime risk, improved operational continuity, stronger change reliability, and better resilience in fiber-connected utility control systems. The study-specific indicators have further strengthened the results. The OT/SCADA Change Risk Exposure Index has shown a moderate level of exposure, meaning that some risk gaps have remained in dependency mapping, emergency recovery preparedness, and communication-path verification. The Fiber-Connected Utility Control System Resilience Score has shown a high level of resilience, suggesting that fiber redundancy, SCADA communication stability, failover readiness, real-time monitoring, and control-center visibility have supported operational continuity during network modifications. The study has also confirmed the relevance of High Reliability Organization Theory, because the results have shown that downtime reduction in critical energy environments depends on preoccupation with failure, sensitivity to operations, deference to expertise, commitment to resilience, and learning from change outcomes. Therefore, the study has concluded that ITIL-based change management can serve as a practical high-reliability governance framework for managing OT/SCADA network modifications safely and systematically. In critical energy environments where communication failure can affect service reliability, operational visibility, public infrastructure, and restoration capability, disciplined change management has been shown to be essential for minimizing disruption and strengthening utility control system performance.

RECOMMENDATIONS

Based on the findings of this study, it is recommended that critical energy organizations adopt a more formal, integrated, and OT-specific ITIL-based change management framework for all planned, emergency, and standard OT/SCADA network modifications. First, utility organizations should strengthen change planning by ensuring that every network modification has a clearly defined scope, implementation schedule, stakeholder communication plan, technical checklist, testing requirement, and operational impact statement before implementation begins. This is important because OT/SCADA network changes can affect substations, field devices, control-center systems, protection equipment, communication switches, routers, firewalls, and monitoring platforms. Second, organizations should give greater priority to change risk assessment because this study has found it to be the strongest predictor of downtime risk reduction. Risk assessment should include dependency mapping, cybersecurity impact review, safety impact analysis, fiber-path verification, redundancy validation, service-critical asset identification, and communication-path testing. Third, approval and authorization procedures should be strengthened by involving both technical and operational experts in the review process. OT engineers, SCADA operators, network engineers, cybersecurity analysts, field engineering teams, and change managers should jointly evaluate high-risk changes before approval. Fourth, rollback and recovery planning should become mandatory for every major OT/SCADA network modification. Organizations should prepare backup configurations, restoration procedures, failover options, recovery owners, escalation paths, and post-change monitoring windows so that service can be restored quickly if a change creates disruption. Fifth, post-change review and documentation should be treated as a learning process rather than a routine administrative task. Each completed change should be reviewed to identify what worked, what failed, what risks were missed, how long recovery took, and how future changes can be improved. Sixth, utilities should develop an OT/SCADA Change Risk Exposure Index as a practical internal monitoring tool to classify change activities into low, moderate, or high exposure levels before implementation. This index can help managers decide whether additional approval, testing, rollback preparation, or expert review is required. Seventh, organizations should also maintain a Fiber-Connected Utility Control System

Resilience Score to evaluate redundancy, failover readiness, SCADA communication stability, control-center visibility, real-time monitoring capability, and recovery speed. Eighth, OT and IT teams should work together under a shared governance model because OT/SCADA reliability depends on both engineering reliability and information-system discipline. Ninth, cybersecurity teams should be included in all network change assessments because firewall rules, segmentation, access control, remote connectivity, and monitoring policies may directly influence cyber-physical risk. Finally, organizations should provide continuous training on ITIL change management, OT/SCADA risk, high-reliability behavior, emergency change control, and recovery planning. These recommendations can help critical energy organizations reduce failed changes, shorten downtime duration, strengthen operational continuity, and improve resilience in fiber-connected utility control systems.

LIMITATIONS OF THE STUDY

This study has several limitations that should be considered when interpreting the findings. First, the study has used a cross-sectional research design, meaning that data have been collected at one point in time. This has allowed the researcher to identify statistical relationships among ITIL-based change management practices and downtime risk reduction, but it has not allowed the study to measure how these relationships may change over a longer period. ITIL maturity, OT/SCADA reliability, staff experience, cybersecurity posture, and change governance practices may improve or decline over time, and a cross-sectional design cannot fully capture these changes. Second, the study has relied on self-reported survey data collected through a five-point Likert scale. Although the questionnaire has shown acceptable reliability, respondent answers may still have been influenced by personal experience, organizational culture, role-based perception, limited technical visibility, or social desirability bias. For example, a change manager may perceive approval procedures as stronger than an OT engineer who directly experiences implementation failures, while a cybersecurity analyst may emphasize risk exposure more than a control-room operator. Third, the study has focused on perceived downtime risk reduction rather than direct operational downtime records. Actual downtime minutes, outage logs, change failure rates, mean time to recovery, alarm delay records, telemetry loss events, and incident reports may provide more objective evidence, but such data can be difficult to access in critical energy environments because of confidentiality, security, and operational sensitivity. Fourth, the study has been limited to a case-study–based context involving fiber-connected OT/SCADA utility control systems. This has strengthened the relevance of the findings for critical energy environments, but it may reduce generalizability to other sectors such as manufacturing, water treatment, transportation, oil and gas, healthcare infrastructure, or ordinary enterprise IT systems. Fifth, the study has used purposive sampling, which has been appropriate because respondents needed specialized knowledge of OT/SCADA systems, utility networks, ITIL practices, and critical infrastructure operations. However, purposive sampling may limit representativeness because not all professionals in the target population have had an equal chance of being selected. Sixth, the study has examined five ITIL-based change management variables, but other factors may also influence downtime risk reduction, including organizational culture, leadership support, automation maturity, cybersecurity capability, vendor support, budget availability, training quality, asset inventory accuracy, and regulatory pressure. Seventh, the study has not tested longitudinal improvement after ITIL implementation, nor has it compared organizations with different maturity levels. Finally, the study has proposed context-specific indicators such as the OT/SCADA Change Risk Exposure Index and Fiber-Connected Utility Control System Resilience Score, but these indicators may require further validation in future studies using larger samples, multiple utility organizations, and actual operational performance data. Therefore, while the study has provided strong quantitative evidence, its findings should be interpreted within the boundaries of its design, data source, sample, and case-study context.

REFERENCES

[1]. Ahmad, N., Shamsudin, Z. M., & Taha, N. H. (2013). Systematic approach to successful implementation of ITIL. *Procedia Computer Science*, *17*, 237-244. https://doi.org/10.1016/j.procs.2013.05.032

[2]. Ancillotti, E., Bruno, R., & Conti, M. (2013). The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*, *36*(17-18), 1665-1697. https://doi.org/10.1016/j.comcom.2013.09.004

[3]. Barrett, M. S., Novak, J. M., Venette, S. J., & Shumate, M. (2006). Validating the High Reliability Organization Perception Scale. *Communication Research Reports*, *23*(2), 111-118. https://doi.org/10.1080/08824090600669087

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

[5]. Blumberg, M., Cater-Steel, A., Rajaeian, M. M., & Soar, J. (2019). Effective organisational change to achieve successful ITIL implementation: Lessons learned from a multiple case study of large Australian firms. *Journal of Enterprise Information Management*, *32*(3), 496-516. https://doi.org/10.1108/jeim-06-2018-0127

[6]. Bobbio, A., Bonanni, G., Ciancamerla, E., Clemente, R., Iacomini, A., Minichino, M., Scarlatti, A., Terruggia, R., & Zendri, E. (2010). Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. *Reliability Engineering & System Safety*, *95*(12), 1345-1357. https://doi.org/10.1016/j.ress.2010.06.011

[7]. Cantu, J., Gharehyakheh, A., Fritts, S., & Tolk, J. (2020). Interventions and measurements of highly reliable/resilient organization implementations: A literature review. *Applied Ergonomics*, *90*, 103241. https://doi.org/10.1016/j.apergo.2020.103241

[8]. Cantu, J., Tolk, J., Fritts, S., & Gharehyakheh, A. (2020). High reliability organization systematic literature review: Discovery of culture as a foundational hallmark. *Journal of Contingencies and Crisis Management*, *28*(4), 399-410. https://doi.org/10.1111/1468-5973.12293

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

[10]. Carroll, J. S., & Rudolph, J. W. (2006). Design of high reliability organizations in health care. *Quality and Safety in Health Care*, *15*, i4-i9. https://doi.org/10.1136/qshc.2005.015867

[11]. Carvalho, M. M. d., & Rabechini Junior, R. (2015). Impact of risk management on project performance: The importance of soft skills. *International Journal of Production Research*, *53*(2), 321-340. https://doi.org/10.1080/00207543.2014.919423

[12]. 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

[13]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

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

[15]. de Barros, M. D., Salles, C. A. L., Gomes, C. F. S., da Silva, R. A., & Costa, H. G. (2015). Mapping of the scientific production on the ITIL application published in the national and international literature. *Procedia Computer Science*, *55*, 102-111. https://doi.org/10.1016/j.procs.2015.07.013

[16]. Diirr, B., Santos, G., & Cappelli, C. (2014). Improvement of IT service processes: A study of critical success factors. *Journal of Software Engineering Research and Development*, *2*, 4. https://doi.org/10.1186/2195-1721-2-4

[17]. Eikebrokk, T. R., & Iden, J. (2017). Strategising IT service management through ITIL implementation: Model and empirical test. *Total Quality Management & Business Excellence*, *28*(3-4), 238-265. https://doi.org/10.1080/14783363.2015.1075872

[18]. Emmanuel, M., & Rayudu, R. (2016). Communication technologies for smart grid applications: A survey. *Journal of Network and Computer Applications*, *74*, 133-148. https://doi.org/10.1016/j.jnca.2016.08.012

[19]. Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18-28. https://doi.org/10.1109/mpe.2009.934876

[20]. Fovino, I. N., Masera, M., & De Cian, A. (2009). Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety*, *94*(9), 1394-1402. https://doi.org/10.1016/j.ress.2009.02.020

[21]. Gable, G. G., Sedera, D., & Chan, T. (2008). Re-conceptualizing information system success: The IS-impact measurement model. *Journal of the Association for Information Systems*, *9*(7), 377-408. https://doi.org/10.17705/1jais.00164

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

[23]. He, H., & Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Physical Systems: Theory & Applications*, *1*(1), 13-27. https://doi.org/10.1049/iet-cps.2016.0019

[24]. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135. https://doi.org/10.1007/s11747-014-0403-8

[25]. 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

[26]. Iden, J., & Eikebrokk, T. R. (2013). Implementing IT service management: A systematic literature review. *International Journal of Information Management*, *33*(3), 512-523. https://doi.org/10.1016/j.ijinfomgt.2013.01.004

[27]. Iden, J., & Eikebrokk, T. R. (2014). Using the ITIL process reference model for realizing IT governance: An empirical investigation. *Information Systems Management*, *31*(1), 37-58. https://doi.org/10.1080/10580530.2014.854089

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

[29]. Jimada-Ojuolape, B., & Teh, J. (2020). Surveys on the reliability impacts of power system cyber–physical layers. *Sustainable Cities and Society*, *62*, 102384. https://doi.org/10.1016/j.scs.2020.102384

[30]. 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

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

[32]. Lepmets, M., Cater-Steel, A., Gacenga, F., & Ras, E. (2012). Extending the IT service quality measurement framework through a systematic literature review. *Journal of Service Science Research*, *4*(1), 7-47. https://doi.org/10.1007/s12927-012-0004-6

[33]. Liang, G., Zhao, J., Luo, F., Weller, S. R., & Dong, Z. Y. (2017). A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, *8*(4), 1630-1638. https://doi.org/10.1109/tsg.2015.2495133

[34]. 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), 1-33. https://doi.org/10.1145/1952982.1952995

[35]. Marrone, M., Gacenga, F., Cater-Steel, A., & Kolbe, L. (2014). IT service management: A cross-national study of ITIL adoption. *Communications of the Association for Information Systems*, *34*, 865-892. https://doi.org/10.17705/1cais.03449

[36]. Marrone, M., & Kolbe, L. M. (2011). Impact of IT service management frameworks on the IT organization. *Business & Information Systems Engineering*, *3*(1), 5-18. https://doi.org/10.1007/s12599-010-0141-5

[37]. McJunkin, T. R., & Rieger, C. G. (2019). Resilient control system metrics. In *Industrial control systems security and resiliency* (pp. 269-287). Springer. https://doi.org/10.1007/978-3-030-18214-4_12

[38]. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039-1057. https://doi.org/10.1109/jproc.2015.2512235

[39]. Md Khaled, H. (2021). An Empirical Study of CRM and Analytics-Based Approaches to Customer Engagement and Sales Performance Evaluation in Enterprise Organizations. *American Journal of Data Science and Analytics*, *2*(12), 76-155. https://doi.org/10.63125/1tt57n77

[40]. 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

[41]. Miller, B., & Rowe, D. C. (2012). A survey SCADA of and critical infrastructure incidents. Proceedings of the 1st Annual Conference on Research in Information Technology,

[42]. Petter, S., & McLean, E. R. (2009). A meta-analytic assessment of the DeLone and McLean IS success model: An examination of IS success at the individual level. *Information & Management*, *46*(3), 159-166. https://doi.org/10.1016/j.im.2009.01.002

[43]. Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539-569. https://doi.org/10.1146/annurev-psych-120710-100452

[44]. Pollard, C., & Cater-Steel, A. (2009). Justifications, strategies, and critical success factors in successful ITIL implementations in U.S. and Australian companies: An exploratory study. *Information Systems Management*, *26*(2), 164-175. https://doi.org/10.1080/10580530902797540

[45]. Radu, C. D., Tirnovan, A., Hotea, A., & Sava, S. (2015). The direct dependence of SCADA systems on communications infrastructure and electric power supply. *Procedia Technology*, *19*, 681-688. https://doi.org/10.1016/j.protcy.2015.02.097

[46]. Saunders, F. C. (2018). A systematic review on high reliability organisational theory as a safety management strategy in construction. *Safety*, *4*(1), 6. https://doi.org/10.3390/safety4010006

[47]. 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

[48]. Tanjina Binte, S., & Sazzadul, I. (2022). Advanced Financial Data Analytics for Anomaly Detection and Pattern Discovery in Large-Scale Financial Data Pipelines. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 174-210. https://doi.org/10.63125/g1cdm484

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

[50]. Usman, A., & Shami, S. H. (2013). Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews*, *19*, 191-199. https://doi.org/10.1016/j.rser.2012.11.002

[51]. Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: Towards a theory and research agenda. 2007 IEEE International Conference on Systems, Man and Cybernetics,

[52]. Wallace, S., Green, K. Y., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An extended TOE framework for cybersecurity-adoption decisions. *Communications of the Association for Information Systems*, *47*, 338-363. https://doi.org/10.17705/1cais.04716

[53]. 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

[54]. 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

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

[56]. Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing,

[57]. Zwikael, O., & Ahn, M. (2011). The effectiveness of risk management: An analysis of project risk planning across industries and countries. *Risk Analysis*, *31*(1), 25-37. https://doi.org/10.1111/j.1539-6924.2010.01470.x