ESCALATING CYBER RISK TO CRITICAL INFRASTRUCTURE

Geopolitical Conflict, Operational Technology Vulnerabilities, and Resilience Strategies for Energy Systems

WRITTEN BY

Chuck Russell

Israel Reyes

2026

INSTITUTE FOR HOMELAND SECURITY

SAM HOUSTON STATE UNIVERSITY

Escalating Cyber Risk to Critical Infrastructure: Geopolitical Conflict, Operational Technology Vulnerabilities, and Resilience Strategies for Energy Systems

Chuck Russell
Houston, TX, USA
United States

Israel Reyes
Houston, TX, USA
United States

EXECUTIVE SUMMARY

"Operational resilience has become one of the defining engineering challenges of modern critical infrastructure. As cyber-physical systems grow in complexity and geopolitical uncertainty increases, organizations require quantitative methodologies capable of measuring, optimizing, and sustaining mission-essential operations."

Critical infrastructure sectors—including energy, manufacturing, oil and gas, transportation, healthcare, food processing, water, mining, and aerospace—have become increasingly dependent upon complex cyber-physical systems whose disruption may generate significant operational, economic, environmental, and national security consequences. Although existing cybersecurity standards provide valuable guidance for governance, compliance, and risk management, they do not fully address the engineering problem of maintaining operational continuity during sustained cyber-physical disruptions.

This paper introduces Operational Resilience Engineering (ORE), a multidisciplinary engineering methodology that integrates systems engineering, cybersecurity, engineering reliability, quantitative risk management, and executive decision support into a unified framework for evaluating and improving operational resilience.

The proposed methodology introduces several original engineering contributions, including the Reference Critical Infrastructure Architecture (RCIA), Operational Dependency Modeling (ODM), the Operational Dependency Criticality Index (ODCI), the Operational Reliability Index (ORI), quantitative operational risk assessment using Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), Monte Carlo simulation, resilience optimization, and the Return on Resilience Investment (RORI). Collectively, these components provide a systematic methodology for identifying mission-essential assets, quantifying operational dependencies, evaluating engineering reliability, estimating operational risk, and prioritizing resilience investments.

Unlike conventional approaches that primarily emphasize cybersecurity compliance, the proposed framework considers operational resilience as a measurable engineering property that can be continuously evaluated and optimized throughout the lifecycle of critical infrastructure systems. The methodology is applicable across multiple industrial sectors and provides decision-makers with quantitative tools for balancing engineering performance, operational continuity, and resilience investment.

Ultimately, this work establishes the foundation for Operational Resilience Engineering as an emerging engineering discipline that bridges systems engineering, cybersecurity, engineering reliability, quantitative risk management, and executive decision-making. By integrating these complementary disciplines within a unified analytical framework, the proposed methodology supports the long-term resilience and sustainability of critical infrastructure operating under increasingly complex cyber-physical conditions.

Dedication

This work is respectfully dedicated to the

Institute for Homeland Security

Sam Houston State University

In recognition of its commitment to advancing homeland security, critical infrastructure protection, applied research, and executive education in support of national resilience and public safety.

May this work contribute to the continued development of engineering methodologies that strengthen the resilience, security, and sustainability of critical infrastructure throughout the world.

TABLE OF CONTENTS

***Abstract*—Critical infrastructure has entered a new era in which cyber operations have become a preferred instrument of geopolitical competition, capable of disrupting essential services without conventional military engagement. Recent geopolitical tensions have demonstrated that cyberspace has evolved into a strategic domain where state-sponsored and state-aligned actors increasingly target Operational Technology (OT) and Industrial Control Systems (ICS) supporting energy production, transmission, maritime operations, and other critical infrastructure sectors. Simultaneously, the convergence of Information Technology (IT), Operational Technology, Industrial Internet of Things (IIoT), cloud connectivity, and digital transformation has significantly expanded the cyber attack surface, exposing industrial environments to increasingly sophisticated cyber-physical threats with the potential to generate cascading operational, economic, environmental, and national security consequences.**

This paper presents a practitioner-oriented assessment of the evolving cyber threat landscape affecting critical energy infrastructure through the integration of geopolitical analysis, Operational Technology security, resilience engineering, cybersecurity governance, and regulatory compliance. The discussion examines the strategic drivers influencing contemporary cyber operations, analyzes structural vulnerabilities within OT and ICS architectures, evaluates emerging adversary tactics, techniques, and procedures (TTPs), and reviews the operational implica-tions of recent cyber incidents affecting critical infrastructure. Particular attention is given to the growing importance of cybersecurity governance and compliance with nationally recognized frameworks and sector-specific requirements, including the NIST Cybersecurity Framework (CSF) 2.0, NIST Special Publication 800-82 Rev. 3, ISA/IEC 62443, API Standard 1164, and the Transportation Security Administration (TSA) Security Directives for pipeline cybersecurity, as foundational elements for strengthening cyber resilience across industrial environments.

Recognizing that cyber intrusions cannot always be prevented, the paper argues that infrastructure operators must transition from prevention-centric cybersecurity toward engineering-based operational resilience capable of anticipating, detecting, withstanding, responding to, and recovering from sustained cyber disruption while maintaining mission-essential operations. To support this objective, the paper proposes a practical resilience framework integrating cybersecurity governance, asset visibil-ity, cyber-physical situational awareness, early threat detection, quantitative operational risk assessment, incident response, recovery planning, and continuous resilience improvement into a unified decision-support methodology suitable for executive leadership and operational stakeholders.

By bridging geopolitical risk, Operational Technology security, resilience engineering, regulatory compliance, and executive decision-making, this work provides actionable guidance for infrastructure owners, policymakers, and security professionals responsible for protecting critical energy systems against an increasingly dynamic and persistent threat environment. Ultimately, the paper advocates a shift from viewing compliance as a regulatory obligation toward recognizing it as a strategic enabler of measurable operational resilience, supporting the sustained delivery of essential services while strengthening national security, economic continuity, and the long-term resilience of critical infrastructure.

Index Terms—**Critical Infrastructure Protection, Operational Technology, Industrial Control Systems, Cybersecurity, Energy Systems, Operational Resilience, Geopolitical Risk, Critical Infrastructure, Risk Management, Artificial Intelligence**

I. Introduction and Overview

Critical infrastructure constitutes the foundation of modern society, supporting the continuous delivery of electricity, oil and gas, water, transportation, communications, healthcare, manufacturing, and other essential services that sustain economic prosperity, public safety, and national security. Among these sectors, energy systems occupy a uniquely strategic position because virtually every critical service depends directly or indirectly upon the reliable generation, transmission, and distribution of energy. Consequently, disruptions affecting energy infrastructure have the potential to produce cascading operational, economic, and societal consequences that extend far beyond the immediate target.

Over the past two decades, the rapid adoption of digital technologies has fundamentally transformed industrial operations. Operational Technology (OT) and Industrial Control Systems (ICS), once designed as isolated environments focused primarily on reliability and safety, have become increasingly interconnected through enterprise networks, cloud computing, Industrial Internet of Things (IIoT) platforms, remote engineering access, and advanced automation technologies. While this digital transformation has improved operational efficiency, predictive maintenance, and data-driven decision-making, it has simultaneously expanded the cyber attack surface available to increasingly sophisticated adversaries.

Recent geopolitical developments have further accelerated this transformation. Cyber operations have evolved into a strategic instrument of national power, enabling state-sponsored and state-aligned actors to conduct intelligence collection, economic disruption, influence operations, and cyber-physical attacks while remaining below the threshold of conventional military conflict. Unlike traditional cybercrime, attacks directed against critical infrastructure seek not only to compromise information but also to disrupt physical processes, interrupt essential services, erode public confidence, and weaken national resilience.

The convergence of geopolitical instability, expanding digital connectivity, and increasing dependence upon interconnected cyber-physical systems has fundamentally altered the risk landscape confronting infrastructure owners and operators. Cybersecurity can no longer be viewed solely as an Information Technology (IT) function or a regulatory compliance exercise. Instead, it has become an essential component of operational continuity, enterprise risk management, engineering reliability, and national security strategy.

Although numerous cybersecurity frameworks, technical standards, and regulatory requirements have significantly improved defensive capabilities across industrial sectors, recent incidents continue to demonstrate that prevention alone cannot eliminate cyber risk. Sophisticated threat actors increasingly exploit trusted relationships, legitimate credentials, software supply chains, and human decision-making to establish persistent access within operational environments. Consequently, infrastructure operators must develop the capability not only to prevent cyber intrusions, but also to anticipate, detect, with-

stand, respond to, and recover from sustained cyber disruption while preserving mission-essential operations.

This paper presents a practitioner-oriented analysis of the evolving cyber threat landscape affecting critical energy infrastructure. It examines the geopolitical drivers influencing contemporary cyber operations, evaluates structural vulnerabilities within Operational Technology and Industrial Control Systems, reviews emerging adversary tactics, techniques, and procedures (TTPs), and analyzes the growing importance of cybersecurity governance and regulatory compliance in protecting industrial environments. Building upon these foundations, the paper proposes an operational resilience framework that integrates engineering principles, quantitative risk management, cybersecurity governance, and executive decision support to strengthen the resilience of energy systems operating within an increasingly complex geopolitical environment.

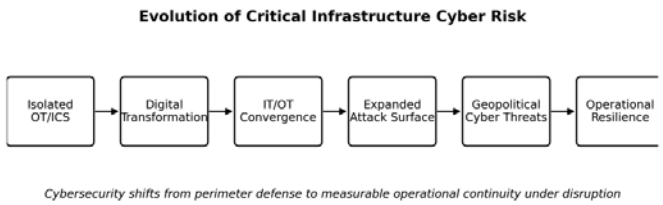

Fig. 1. Evolution of Critical Infrastructure Cyber Risk. The digital transformation of Operational Technology (OT) and Industrial Control Systems (ICS) has expanded the cyber attack surface, increasing exposure to geopolitical cyber threats. As industrial environments become more interconnected, organizations must transition from traditional perimeter defense toward engineering-based operational resilience capable of sustaining mission-essential operations under cyber disruption.

II. Gap Assessment and Problem Statement

"Compliance establishes the minimum cybersecurity baseline; resilience determines whether critical infrastructure continues operating when that baseline is challenged."

The cyber risk landscape confronting critical infrastructure has fundamentally transformed over the past decade. Accelerated digital transformation, increasing geopolitical instability, widespread adoption of Industrial Internet of Things (IIoT) technologies, cloud computing, artificial intelligence, remote operations, and the convergence of Information Technology (IT) with Operational Technology (OT) have collectively reshaped the operating environment of critical infrastructure sectors. While these technological advances have enabled unprecedented improvements in operational efficiency, asset visibility, predictive maintenance, and enterprise integration, they have simultaneously expanded the cyber attack surface available to increasingly sophisticated adversaries.

Unlike traditional Information Technology environments, Operational Technology and Industrial Control Systems directly control physical processes responsible for generating electricity, transporting hydrocarbons, operating pipelines, managing maritime logistics, producing manufactured goods, and maintaining countless essential services upon which modern societies depend. Consequently, successful cyberattacks targeting industrial environments extend beyond the compromise of digital information. They may interrupt production, damage physical assets, compromise safety systems, disrupt supply chains, generate environmental consequences, and ultimately threaten national economic stability and public confidence.

Recognizing these evolving risks, governments, regulatory agencies, and industry organizations have made significant investments in cybersecurity governance through the development of comprehensive standards, regulatory directives, and best-practice frameworks. Initiatives such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, NIST Special Publication 800-82 Revision 3, the ISA/IEC 62443 series of standards, API Standard 1164 for pipeline SCADA security, and the Transportation Security Administration (TSA) Security Directives for pipeline cybersecurity have substantially strengthened the cybersecurity posture of critical infrastructure operators. Collectively, these frameworks establish essential guidance for governance, asset management, network segmentation, access control, incident response, risk management, and continuous monitoring, providing organizations with a structured foundation for reducing cyber risk.

Despite these significant advancements, recent incidents affecting energy systems, industrial facilities, and transportation infrastructure demonstrate that cybersecurity investments alone cannot eliminate operational risk. Nation-state actors, state-sponsored groups, ransomware organizations, hacktivist collectives, and sophisticated criminal enterprises continue to exploit vulnerabilities across interconnected industrial environments. In many cases, attackers leverage legitimate credentials,

trusted vendor relationships, software supply chains, remote access infrastructure, or previously unknown vulnerabilities to establish persistent access while avoiding immediate detection. As a result, organizations may satisfy regulatory requirements and maintain mature cybersecurity programs while remaining vulnerable to operational disruption.

This apparent contradiction exposes one of the most significant challenges facing modern critical infrastructure protection. Existing cybersecurity frameworks primarily define governance structures, technical controls, and organizational processes intended to reduce the likelihood of successful cyber compromise. However, they generally provide limited guidance for quantitatively evaluating the ability of industrial operations to continue performing mission-essential functions during sustained cyber disruption. Compliance therefore represents an essential foundation for cybersecurity maturity but should not be interpreted as a direct measure of operational resilience.

The distinction between cybersecurity compliance and operational resilience has become increasingly important as cyber incidents evolve from isolated information security events into complex cyber-physical disruptions capable of producing cascading operational consequences. Infrastructure operators are no longer confronted solely with questions regarding whether unauthorized access can be prevented. They must also determine how rapidly malicious activity can be detected, how operational dependencies influence cascading failures, how engineering systems degrade during prolonged disruption, how recovery priorities should be established, and how mission-critical services can be sustained under adverse conditions. These questions extend beyond traditional cybersecurity and require the integration of systems engineering, operational risk management, engineering reliability, business continuity, and executive decision-making.

Consequently, the central problem addressed in this paper is not the absence of cybersecurity standards or regulatory requirements. Rather, it is the absence of an integrated operational resilience perspective capable of connecting geopolitical threat intelligence, cybersecurity governance, industrial engineering, quantitative risk assessment, and operational continuity into a unified decision-support framework. As cyber threats continue to evolve in scale, sophistication, and geopolitical significance, critical infrastructure protection must transition from a prevention-centric philosophy toward a resilience engineering approach that emphasizes the ability to anticipate, withstand, adapt to, recover from, and continuously operate despite sustained cyber disruption.

Accordingly, this paper argues that operational resilience should become a measurable engineering objective rather than simply a cybersecurity aspiration. Achieving this objective requires organizations to integrate cybersecurity governance with engineering reliability, cyber-physical dependency analysis, regulatory compliance, quantitative operational risk assessment, and executive decision support. The following sections examine the geopolitical factors driving the current cyber threat environment and establish the technical and operational foundations necessary for developing a comprehensive resilience framework for critical energy infrastructure.

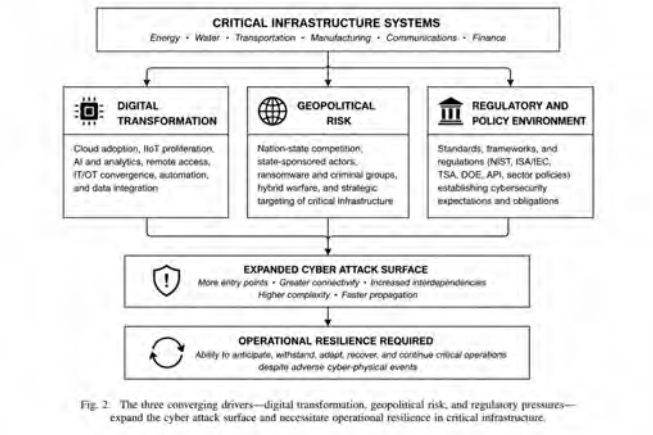

Fig. 2. The three converging drivers—digital transformation, geopolitical risk, and regulatory pressures—expand the cyber attack surface and necessitate operational resilience in critical infrastructure.

Fig. 2. Convergence of digital transformation, geopolitical risk, and regulatory drivers expanding cyber risk across critical infrastructure and increasing the need for operational resilience.

As summarized in Table I, protecting modern critical infrastructure requires an evolution from traditional prevention-centric cybersecurity toward Operational Resilience Engineering (ORE), where cybersecurity, engineering reliability, governance, quantitative risk management, regulatory compliance, and operational continuity become complementary components of a unified resilience strategy. Rather than replacing existing cybersecurity frameworks, ORE extends their value by emphasizing the capability of organizations to sustain mission-essential operations despite increasingly sophisticated cyber-physical disruptions.

A. Evolution of the Critical Infrastructure Risk Landscape

> *"Digital transformation has not merely connected industrial systems; it has fundamentally redefined the operational risk landscape of critical infrastructure."*

The operational environment supporting critical infrastructure has undergone a profound transformation over the past two decades. Historically, Operational Technology (OT) and Industrial Control Systems (ICS) were engineered to prioritize deterministic performance, operational reliability, process safety, and continuous availability. Industrial assets including Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, and Safety Instrumented Systems (SIS) were traditionally deployed within isolated environments where external connectivity was intentionally minimized. In these architectures, operational continuity depended primarily upon engineering reliability, while cybersecurity risks were considered relatively limited due to restricted network exposure and the widespread use of proprietary industrial protocols.

Driven by increasing demands for operational efficiency, sustainability, predictive maintenance, and data-driven decision making, industrial organizations have progressively adopted digital technologies that fundamentally alter the ar-

TABLE I
EVOLUTION FROM TRADITIONAL CYBERSECURITY TO OPERATIONAL RESILIENCE ENGINEERING (ORE). THE TABLE ILLUSTRATES THE TRANSITION FROM PREVENTION-CENTRIC CYBERSECURITY TOWARD AN ENGINEERING-BASED OPERATIONAL RESILIENCE PHILOSOPHY FOR PROTECTING CRITICAL INFRASTRUCTURE.

Traditional Cybersecurity	**Operational Resilience Engineering (ORE)**
Primary objective is preventing cyber compromise.	Primary objective is sustaining mission-essential operations despite cyber disruption.
Focuses primarily on Information Technology (IT) assets.	Integrates Information Technology (IT), Operational Technology (OT), engineering systems, and business operations.
Measures cybersecurity maturity through technical controls and regulatory compliance.	Measures resilience through operational continuity, recovery capability, engineering performance, and mission assurance.
Emphasizes Confidentiality, Integrity, and Availability (CIA).	Balances cybersecurity with safety, reliability, operational continuity, and resilience.
Evaluates individual cyber incidents.	Evaluates cascading operational consequences across interconnected cyber-physical systems.
Incident response focuses on restoring information systems.	Recovery focuses on preserving operational capability while minimizing disruption to essential services.
Risk assessments estimate the likelihood of cyber compromise.	Risk assessments quantify operational, economic, safety, environmental, and national security consequences.
Compliance demonstrates implementation of cybersecurity controls.	Compliance establishes the foundation for Operational Resilience Engineering.
Decision-making is primarily technology driven.	Decision-making integrates engineering, quantitative risk, executive governance, and operational priorities.
Success is measured by preventing successful cyberattacks.	Success is measured by the ability to anticipate, withstand, adapt, recover, and continuously operate during cyber disruption.

chitecture of critical infrastructure. Enterprise integration, Industrial Internet of Things (IIoT) devices, cloud computing, advanced analytics, artificial intelligence, digital twins, edge computing, and remote engineering capabilities have become integral components of modern industrial operations. These technologies provide unprecedented operational visibility, enhance asset performance, improve maintenance planning, and enable executive decision-makers to optimize complex industrial processes through real-time operational intelligence.

The convergence of Information Technology (IT) and Operational Technology has consequently generated significant economic and operational benefits across the energy sector. Modern industrial environments increasingly rely upon interconnected cyber-physical systems capable of continuously exchanging operational data between field devices, control networks, enterprise applications, cloud platforms, and executive dashboards. This integration enables predictive maintenance, remote asset management, production optimization, and AI-assisted operational decision support that were previously unattainable within isolated industrial environments.

However, the same technological advances that improve operational performance simultaneously introduce new pathways through which cyber threats may propagate across interconnected systems. Every remote engineering workstation, cloud interface, wireless sensor, software update mechanism, vendor connection, application programming interface (API), enterprise integration point, and third-party service expands the potential attack surface available to malicious actors. Consequently, cyber risk is no longer confined to isolated technical assets but has evolved into a systemic property of highly interconnected cyber-physical ecosystems where digital compromise may rapidly produce cascading operational consequences.

Unlike traditional Information Technology environments, successful cyberattacks against Operational Technology directly influence physical processes responsible for generating electricity, transporting hydrocarbons, operating pipelines, controlling manufacturing facilities, managing maritime logistics, and delivering other mission-essential services. The operational consequences may therefore extend well beyond data loss or service interruption, potentially resulting in equipment damage, production outages, environmental releases, safety incidents, regulatory violations, financial losses, supply chain disruption, and degradation of public confidence in critical

infrastructure.

This transformation represents a fundamental shift in the engineering assumptions upon which industrial systems were originally designed. Historically, cybersecurity focused primarily on protecting information assets from unauthorized access. Modern critical infrastructure, however, requires protecting the continuous operation of complex cyber-physical systems whose performance depends upon the dynamic interaction of engineering assets, digital technologies, organizational processes, external service providers, regulatory obligations, and human decision-making. Consequently, operational resilience must be viewed as an emergent systems property rather than simply the outcome of implementing individual cybersecurity controls.

Figure 2 illustrates the convergence of three principal forces reshaping the cyber risk landscape of modern critical infrastructure: digital transformation, geopolitical instability, and the evolving regulatory environment. These forces do not operate independently. Instead, they reinforce one another, collectively expanding the cyber attack surface while simultaneously increasing the operational consequences associated with successful cyber compromise. Understanding this convergence provides the foundation for examining the limitations of traditional cybersecurity approaches and motivates the transition toward Operational Resilience Engineering (ORE) as a multidisciplinary framework for sustaining mission-essential operations under increasingly complex cyber-physical threat conditions.

Definition 1 (Operational Dependency). An operational dependency is defined as the reliance of one mission-essential function, engineering process, industrial asset, or organizational capability upon the continuous availability, integrity, or performance of another interconnected cyber-physical component whose disruption may propagate cascading operational consequences throughout the system.

B. Limitations of Traditional Cybersecurity

> *"Cybersecurity reduces the probability of compromise; Operational Resilience Engineering reduces the operational consequences of compromise."*

The rapid evolution of cyber threats affecting critical infrastructure has demonstrated that cybersecurity, while indispensable, cannot by itself guarantee the sustained operation of mission-essential services. Over the past decade, governments, regulatory agencies, and private-sector organizations have invested billions of dollars in strengthening cybersecurity capabilities through governance frameworks, technical controls, continuous monitoring, threat intelligence, and regulatory compliance. These investments have significantly improved the cybersecurity posture of critical infrastructure sectors and have reduced the likelihood of successful cyber compromise across many operational environments.

Nevertheless, recent cyber incidents affecting energy systems, industrial facilities, pipelines, transportation networks, and other critical infrastructure sectors continue to demonstrate that determined adversaries remain capable of disrupting industrial operations despite the implementation of mature cybersecurity programs. Nation-state actors increasingly exploit trusted relationships, software supply chains, legitimate credentials, remote access infrastructure, zero-day vulnerabilities, and human decision-making rather than relying exclusively upon traditional technical exploits. Consequently, preventing every cyber intrusion has become an increasingly unrealistic objective within highly interconnected cyber-physical environments.

Traditional cybersecurity has historically emphasized protecting digital assets through preventive, detective, and corrective security controls. This philosophy has proven highly effective within conventional Information Technology (IT) environments where the principal objectives involve preserving the confidentiality, integrity, and availability of information. Critical infrastructure, however, presents a fundamentally different engineering challenge. Operational Technology (OT) environments exist primarily to control physical processes whose disruption may interrupt electricity generation, hydrocarbon transportation, manufacturing production, water treatment, maritime logistics, and numerous other mission-essential services.

From an operational perspective, cyber incidents should therefore be evaluated not only according to their technical characteristics but also according to their ability to degrade industrial processes, interrupt production, compromise safety, generate environmental consequences, disrupt supply chains, and weaken organizational resilience. The engineering objective consequently extends beyond preventing cyber compromise toward ensuring the continuous operation of critical infrastructure despite adverse cyber conditions.

An equally important limitation of traditional cybersecurity lies in its strong emphasis on regulatory compliance and implementation of prescribed security controls. Frameworks such as the NIST Cybersecurity Framework (CSF), NIST Special Publication 800-82 Revision 3, ISA/IEC 62443, API Standard 1164, and the Transportation Security Administration (TSA) Security Directives provide essential guidance for cybersecurity governance, asset management, network segmentation, identity management, incident response, and continuous monitoring. These frameworks have substantially strengthened cybersecurity maturity and should remain indispensable components of industrial cybersecurity programs.

Compliance, however, should not be interpreted as direct evidence of operational resilience. Organizations may successfully implement recognized cybersecurity controls while remaining vulnerable to operational disruption resulting from engineering dependencies, supply chain failures, third-party services, human factors, or prolonged loss of critical digital capabilities. Compliance therefore establishes the minimum acceptable cybersecurity baseline, whereas Operational Resilience Engineering (ORE) evaluates the capability of organizations to anticipate, withstand, adapt to, recover from, and continuously operate during sustained cyber disruption.

Accordingly, this paper proposes Operational Resilience Engineering (ORE) as a multidisciplinary systems engineering

discipline that extends traditional cybersecurity by integrating cybersecurity governance, engineering reliability, operational continuity, dependency analysis, quantitative risk management, and executive decision support into a unified operational framework. To formally establish this framework, the proposed **Operational Resilience Engineering (ORE) Fundamental Equation** is introduced as follows:

$$ORE = f(C_s, G, E, D, R_c, C_o) \tag{1}$$

where

- C_s represents cybersecurity capability and technical protection,
- G represents governance, regulatory compliance, and organizational oversight,
- E represents engineering reliability of cyber-physical systems,
- D represents operational dependency analysis across interconnected assets,
- R_c represents recovery capability following cyber disruption, and
- C_o represents the ability to sustain mission-essential operational continuity.

Equation (1), hereafter referred to as the *Operational Resilience Engineering (ORE) Fundamental Equation*, defines the conceptual architecture of the proposed Operational Resilience Engineering framework by identifying the essential engineering disciplines required to sustain mission-essential operations under cyber disruption.

The ORE Fundamental Equation should be interpreted as a conceptual systems engineering model rather than a final mathematical formulation. It establishes the theoretical foundation upon which the quantitative Operational Resilience Engineering framework developed throughout the remainder of this paper is constructed. Specifically, each component of the equation is progressively expanded through operational dependency modeling, engineering reliability analysis, quantitative risk assessment, resilience metrics, Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), Monte Carlo simulation, and executive decision-support methodologies. Within this integrated framework, cybersecurity becomes one essential component of a broader Operational Resilience Engineering strategy whose ultimate objective is preserving the continuous operation of mission-essential systems while ensuring the uninterrupted delivery of essential services despite increasingly complex cyber-physical threats.

This multidisciplinary perspective establishes the conceptual foundation for the remainder of the paper and motivates the transition from prevention-centric cybersecurity toward engineering-based Operational Resilience Engineering as a measurable discipline for protecting modern critical infrastructure.

C. Cybersecurity Governance and Regulatory Compliance

> *"Compliance establishes the cybersecurity foundation; governance transforms compliance into measurable operational resilience."*

Cybersecurity governance has evolved into one of the most important strategic responsibilities within modern critical infrastructure organizations. As Operational Technology (OT), Industrial Control Systems (ICS), cloud computing, Industrial Internet of Things (IIoT), and enterprise Information Technology (IT) become increasingly interconnected, cybersecurity decisions directly influence operational reliability, business continuity, regulatory compliance, enterprise risk management, and ultimately national resilience. Consequently, cybersecurity governance should no longer be regarded solely as a technical or compliance function, but rather as an enterprise-wide capability that aligns cybersecurity strategy with engineering objectives and executive decision-making.

Recognizing the growing strategic importance of cyber resilience, governments and international standards organizations have developed comprehensive cybersecurity frameworks that provide structured guidance for protecting industrial environments. These frameworks establish common principles for governance, asset management, cybersecurity architecture, risk management, incident response, recovery planning, continuous monitoring, and organizational accountability, thereby providing a consistent foundation for improving cybersecurity maturity across critical infrastructure sectors.

Among the most influential initiatives, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 establishes a flexible risk-based methodology organized around the functions of Govern, Identify, Protect, Detect, Respond, and Recover. Complementing this framework, NIST Special Publication 800-82 Revision 3 provides detailed technical guidance for securing Operational Technology and Industrial Control Systems, emphasizing secure architecture, network segmentation, asset inventories, remote access management, industrial communications, and continuous monitoring.

Similarly, the ISA/IEC 62443 series introduces a comprehensive lifecycle methodology specifically developed for Industrial Automation and Control Systems (IACS). Through concepts including security zones, conduits, defense-in-depth architectures, and security levels, ISA/IEC 62443 enables organizations to systematically design, operate, and maintain secure industrial environments while balancing cybersecurity with operational reliability and process safety.

Within the energy sector, additional sector-specific guidance further strengthens cybersecurity governance. API Standard 1164 provides cybersecurity recommendations for Supervisory Control and Data Acquisition (SCADA) systems supporting pipeline operations, while the Transportation Security Administration (TSA) Security Directives establish mandatory cybersecurity requirements for designated pipeline operators, including cybersecurity implementation plans, vulnerability assessments, multifactor authentication, network segmentation, incident reporting, and executive accountability. Collectively, these initiatives significantly enhance the cybersecurity posture of critical energy infrastructure while promoting greater organizational preparedness against evolving cyber threats.

The collective value of these frameworks extends beyond

regulatory compliance. They establish a common governance language that enables executive leadership, engineering organizations, cybersecurity teams, regulators, and operational personnel to coordinate cybersecurity activities using consistent risk management principles. Consequently, these frameworks represent the essential governance foundation upon which resilient industrial operations can be developed.

Nevertheless, governance and compliance should not be interpreted as direct measures of operational resilience. Existing frameworks primarily establish what organizations should implement in order to reduce cybersecurity risk; they intentionally avoid prescribing how organizations should quantitatively evaluate their capability to sustain mission-essential operations during prolonged cyber disruption. This distinction is particularly important within critical infrastructure environments where engineering dependencies, physical processes, operational priorities, supply chain relationships, and human decision-making collectively determine the actual resilience of industrial operations.

Operational Resilience Engineering (ORE) builds directly upon these internationally recognized governance frameworks rather than replacing them. Within the proposed ORE framework, cybersecurity governance establishes strategic direction, regulatory compliance defines the minimum acceptable cybersecurity baseline, engineering reliability supports dependable physical operation, quantitative risk assessment measures operational exposure, dependency analysis identifies cascading vulnerabilities, and executive decision support enables informed resource allocation under uncertain operating conditions. Together, these complementary disciplines create a unified resilience capability whose objective extends beyond preventing cyber compromise toward sustaining mission-essential operations throughout the complete lifecycle of disruptive events.

Accordingly, this paper proposes that cybersecurity governance should progressively evolve from demonstrating regulatory compliance toward continuously measuring operational resilience. Such an evolution enables organizations not only to verify that cybersecurity controls have been implemented, but also to evaluate whether those controls effectively preserve operational continuity under increasingly sophisticated cyber-physical threat conditions. This governance perspective establishes the conceptual bridge between internationally recognized cybersecurity standards and the multidisciplinary Operational Resilience Engineering framework developed throughout the remainder of this paper.

D. The Operational Resilience Gap

> *"The question is no longer whether critical infrastructure can resist cyberattack, but whether it can continue operating when resistance is no longer sufficient."*

The preceding discussion demonstrates that cybersecurity has evolved significantly over the past two decades. Advances in cybersecurity governance, regulatory compliance, industrial standards, network segmentation, asset visibility, threat intelligence, identity management, and incident response have substantially strengthened the defensive posture of critical infrastructure operators. Frameworks including the NIST Cybersecurity Framework (CSF) 2.0, NIST Special Publication 800-82 Revision 3, ISA/IEC 62443, API Standard 1164, and the Transportation Security Administration (TSA) Security Directives collectively represent an internationally recognized foundation for improving cybersecurity maturity across industrial environments.

Despite these significant advances, recent cyber incidents affecting energy systems, manufacturing facilities, transportation networks, and other critical infrastructure sectors continue to demonstrate that mature cybersecurity programs cannot completely eliminate operational risk. Highly capable adversaries increasingly exploit trusted relationships, software supply chains, legitimate credentials, third-party service providers, remote engineering access, and previously unknown vulnerabilities to establish persistent access within industrial environments. Consequently, preventing every cyber intrusion has become an increasingly unrealistic objective for organizations operating within highly interconnected cyber-physical ecosystems.

This reality exposes a critical gap within current cybersecurity practice. Existing governance frameworks and regulatory standards primarily define the cybersecurity controls that organizations should implement to reduce the probability of successful compromise. However, they generally provide limited guidance for quantitatively evaluating an organization's capability to sustain mission-essential operations during prolonged cyber disruption. In other words, cybersecurity maturity and regulatory compliance do not necessarily provide a measurable indication of operational resilience.

This distinction is particularly significant within Operational Technology (OT) environments, where cyber incidents directly influence physical processes responsible for electricity generation, hydrocarbon transportation, manufacturing production, water treatment, maritime logistics, and other essential services. Within these environments, the operational consequences of cyber disruption are determined not only by technical vulnerabilities but also by engineering reliability, operational dependencies, recovery capability, human decision-making, supply chain resilience, and the ability of organizations to adapt under rapidly changing conditions.

Current cybersecurity frameworks likewise provide limited mechanisms for quantifying cascading operational dependencies across interconnected cyber-physical systems. Modern critical infrastructure rarely operates as isolated assets. Instead, industrial facilities depend upon complex interactions among engineering equipment, digital communications, cloud services, external suppliers, operational personnel, enterprise applications, and supporting infrastructure. The disruption of a single critical dependency may therefore propagate throughout multiple operational layers, producing cascading consequences whose cumulative impact substantially exceeds the initiating cyber event.

An equally important limitation concerns executive decision-making. While cybersecurity programs routinely measure vulnerabilities, security controls, compliance status,

and incident metrics, executive leadership must ultimately make decisions based upon operational continuity, financial exposure, production capability, regulatory consequences, safety, enterprise value, and national resilience. Existing cybersecurity frameworks rarely integrate these engineering and business dimensions into a unified quantitative methodology capable of supporting strategic investment decisions under uncertainty.

Accordingly, this paper identifies the Operational Resilience Gap as the absence of an integrated systems engineering methodology capable of quantitatively connecting cybersecurity governance, engineering reliability, operational dependency analysis, regulatory compliance, operational continuity, and executive decision support within a single measurable framework. Closing this gap requires moving beyond a prevention-centric cybersecurity philosophy toward an engineering discipline capable of continuously evaluating how industrial systems anticipate, withstand, adapt to, recover from, and continue operating during sustained cyber disruption.

Operational Resilience Engineering (ORE) is proposed as the multidisciplinary engineering discipline that addresses this gap. Rather than replacing established cybersecurity frameworks, ORE extends their value by integrating cybersecurity governance with engineering reliability, operational dependency modeling, quantitative risk assessment, resilience metrics, and executive decision support into a unified operational methodology. Within this framework, cybersecurity becomes one essential component of a broader resilience strategy whose objective is preserving mission-essential operations while minimizing operational, economic, environmental, and societal consequences arising from cyber-physical disruption.

Figure 3 illustrates the proposed Operational Resilience Engineering governance model. The model demonstrates how internationally recognized cybersecurity frameworks establish the governance foundation upon which engineering reliability, operational continuity, quantitative risk assessment, and executive decision support collectively create measurable operational resilience. This integrated perspective provides the conceptual bridge between existing cybersecurity practice and the quantitative Operational Resilience Engineering framework developed throughout the remainder of this paper.

Definition 2 (Operational Resilience Engineering).
Operational Resilience Engineering (ORE) is defined as the multidisciplinary systems engineering discipline that integrates cybersecurity governance, engineering reliability, operational dependency analysis, quantitative risk assessment, regulatory compliance, operational continuity, and executive decision support to sustain mission-essential operations before, during, and after cyber-physical disruption.

III. Geopolitical Drivers of Cyber Conflict

"Cyber conflict has become the preferred instrument of strategic competition below the threshold of conventional warfare, where the objective is not necessarily destruction, but persistent influence over the operation of critical infrastructure."

Fig. 4. Operational Resilience Engineering (ORE) governance model.

Fig. 3. Operational Resilience Engineering (ORE) governance model.

The geopolitical environment surrounding critical infrastructure has changed fundamentally during the past decade. Increasing strategic competition among nation-states has expanded the use of cyberspace as an operational domain through which governments pursue political influence, economic advantage, intelligence collection, and military objectives without engaging in conventional armed conflict. Unlike traditional military operations, cyber campaigns provide adversaries with the ability to operate across national boundaries while maintaining varying degrees of anonymity, plausible deniability, and operational persistence. Consequently, cyber operations have become an increasingly attractive instrument for achieving strategic objectives below the threshold of conventional warfare.

This evolution coincides with the rapid digital transformation of critical infrastructure sectors. Modern energy systems, industrial facilities, transportation networks, water treatment plants, and manufacturing environments have become increasingly dependent upon interconnected Operational Technology (OT), Industrial Control Systems (ICS), cloud computing, Industrial Internet of Things (IIoT) devices, remote engineering platforms, and artificial intelligence. While these technologies significantly improve operational efficiency and decision-making, they simultaneously expand the cyber attack surface available to sophisticated adversaries capable of exploiting interconnected cyber-physical systems.

Unlike financially motivated cybercrime, geopolitical cyber operations frequently pursue long-term strategic objectives. These campaigns often emphasize persistent access, intelligence collection, operational reconnaissance, supply chain compromise, credential theft, and the establishment of latent capabilities that may be activated during periods of heightened geopolitical tension. As a result, the success of these operations should not be measured solely by immediate operational disruption, but rather by the adversary's ability to maintain long-term influence over critical infrastructure while remaining undetected.

The strategic importance of critical infrastructure further

increases its attractiveness as a target for geopolitical cyber operations. Energy generation, electricity transmission, natural gas pipelines, petroleum infrastructure, transportation systems, communications networks, manufacturing facilities, and water treatment operations collectively support nearly every sector of modern society. Disruption affecting any of these interconnected systems may rapidly propagate across dependent infrastructure, producing cascading operational, economic, environmental, and societal consequences that extend well beyond the initially compromised organization.

Consequently, the engineering challenge confronting critical infrastructure extends beyond protecting individual industrial assets against isolated cyber incidents. Modern infrastructure operators must instead evaluate resilience from a systems perspective in which geopolitical uncertainty, engineering reliability, cybersecurity governance, operational dependencies, organizational preparedness, and executive decision-making collectively determine the capability to sustain mission-essential operations during prolonged cyber disruption.

This changing threat environment provides the strategic context for Operational Resilience Engineering (ORE). As cyber conflict increasingly becomes an instrument of geopolitical competition, organizations must transition from security strategies that primarily emphasize prevention toward engineering methodologies capable of anticipating disruption, sustaining operational continuity, adapting to degraded operating conditions, and recovering critical services while minimizing operational, economic, environmental, and societal consequences.

The following subsections examine the principal geopolitical factors driving this transformation and explain why Operational Resilience Engineering provides an appropriate systems engineering framework for protecting modern energy infrastructure under increasingly complex cyber-physical threat conditions.

A. Evolution of Geopolitical Cyber Conflict

> *"The evolution of cyber conflict reflects a strategic transition from isolated technical attacks toward persistent campaigns capable of influencing national security, economic stability, and the resilience of critical infrastructure."*

The geopolitical role of cyberspace has evolved significantly over the past two decades. Initially regarded primarily as a domain supporting information exchange and commercial innovation, cyberspace has progressively emerged as a strategic operational environment through which governments pursue political, economic, military, and intelligence objectives. This transformation has fundamentally altered the security landscape confronting critical infrastructure operators, requiring organizations to evaluate cyber risk not only from a technical perspective but also within the broader context of geopolitical competition and national resilience.

Unlike conventional military operations, cyber campaigns offer several strategic advantages. They may be conducted remotely across national boundaries, often with limited attribution, relatively low operational cost, and varying degrees of plausible deniability. These characteristics enable adversaries to conduct continuous intelligence collection, infrastructure reconnaissance, influence operations, and strategic positioning without necessarily escalating to conventional armed conflict. Consequently, cyberspace has become an increasingly attractive domain for achieving national objectives while operating below the traditional threshold of war.

The rapid digital transformation of critical infrastructure has further amplified this strategic environment. Energy systems, industrial manufacturing, transportation networks, water treatment facilities, communications infrastructure, and other mission-essential services increasingly depend upon highly interconnected Operational Technology (OT), Industrial Control Systems (ICS), cloud platforms, Industrial Internet of Things (IIoT) devices, remote engineering capabilities, and artificial intelligence. While these technologies significantly improve operational efficiency, productivity, and decision-making, they also increase the potential exposure of cyber-physical systems to sophisticated threat actors operating within an evolving geopolitical landscape.

Modern geopolitical cyber campaigns differ substantially from the opportunistic attacks commonly associated with financially motivated cybercrime. Rather than pursuing immediate financial gain, sophisticated threat actors frequently conduct long-term operations designed to establish persistent access, collect strategic intelligence, map operational dependencies, compromise trusted relationships, and position themselves for future influence or disruption. Consequently, the operational success of these campaigns is often measured not by immediate damage, but by their ability to remain undetected while preserving strategic access to critical infrastructure over extended periods.

The increasing convergence of geopolitical competition and digital transformation has elevated critical infrastructure to a strategic national asset whose disruption may generate consequences extending well beyond individual organizations. Successful cyber operations affecting energy production, pipeline transportation, manufacturing facilities, or other industrial environments may produce cascading effects across interconnected economic sectors, supply chains, public services, and national security functions. Accordingly, cyber conflict should no longer be viewed exclusively as an information security problem, but rather as a multidisciplinary systems engineering challenge requiring the integration of cybersecurity, engineering reliability, operational continuity, governance, and quantitative risk management.

This evolution provides the strategic context for Operational Resilience Engineering (ORE). As geopolitical competition increasingly manifests through persistent cyber operations, organizations must complement traditional cybersecurity controls with engineering methodologies capable of anticipating disruption, maintaining operational continuity, adapting to degraded operating conditions, and recovering critical services while minimizing operational, economic, environmental, and societal consequences. This perspective establishes the foundation for examining the characteristics of modern nation-state cyber operations discussed in the following subsection.

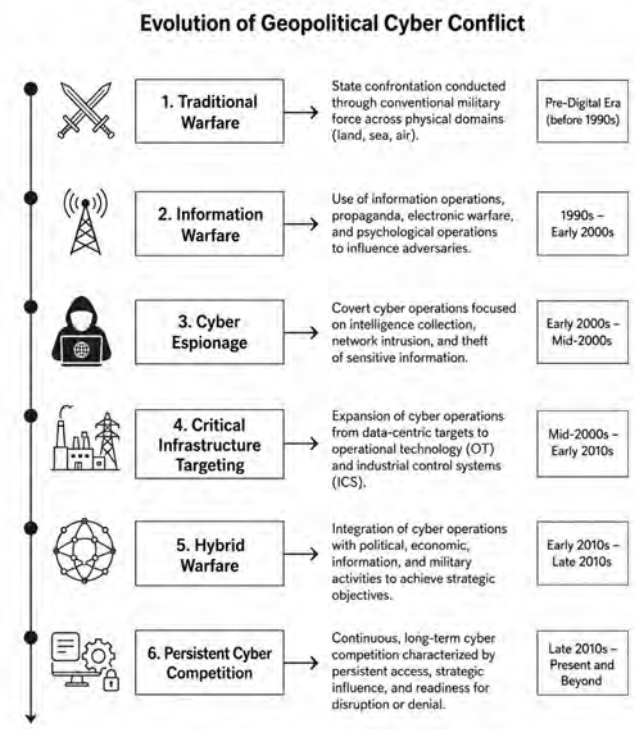

Figure 4. Evolution of Geopolitical Cyber Conflict.

Fig. 4. Evolution of geopolitical cyber conflict from conventional warfare toward persistent cyber competition targeting critical infrastructure. The progression illustrates how cyber operations have evolved into a strategic instrument capable of influencing national security, economic stability, and the operational resilience of critical infrastructure.

B. Nation-State Threat Actors

> *"The distinguishing characteristic of nation-state cyber operations is not merely technical sophistication, but the ability to pursue long-term strategic objectives through persistent cyber-physical influence."*

The threat landscape confronting critical infrastructure has evolved from predominantly opportunistic cybercrime toward increasingly sophisticated campaigns conducted by highly capable and well-resourced threat actors. Unlike financially motivated adversaries whose primary objective is immediate economic gain, nation-state cyber operations frequently pursue strategic objectives that extend well beyond individual organizations. These campaigns are often designed to support national interests through intelligence collection, geopolitical influence, strategic positioning, economic disruption, or preparation for future conflict.

One of the defining characteristics of nation-state cyber operations is persistence. Rather than seeking immediate operational disruption, sophisticated threat actors frequently conduct prolonged campaigns that may remain active for months or even years before producing observable operational effects. During this period, adversaries typically perform infrastructure reconnaissance, credential acquisition, privilege escalation, network mapping, supply-chain compromise, and operational dependency analysis to develop a comprehensive understanding of the targeted environment.

These operations increasingly exploit trusted relationships rather than relying exclusively on direct technical compromise. Third-party vendors, software suppliers, cloud service providers, remote engineering platforms, maintenance contractors, and managed service providers may unintentionally introduce additional pathways into Operational Technology (OT) environments. Consequently, modern cyber defense must evaluate the resilience of the entire operational ecosystem rather than focusing exclusively upon individual industrial assets.

Another distinguishing characteristic of nation-state campaigns is their emphasis on operational preparation rather than immediate execution. Threat actors often establish persistent access within industrial environments while deliberately avoiding actions that would reveal their presence. This strategy enables adversaries to maintain long-term operational awareness and preserves the capability to influence or disrupt critical infrastructure should geopolitical circumstances change. As a result, the operational significance of a cyber intrusion cannot always be evaluated according to its immediate consequences, but rather according to the strategic opportunities created through sustained unauthorized access.

Unlike conventional Information Technology environments, Operational Technology presents unique engineering challenges for sophisticated adversaries. Industrial control systems operate under stringent requirements for safety, reliability, deterministic performance, and continuous availability. Consequently, successful cyber operations targeting critical infrastructure require not only advanced cybersecurity capabilities but also a detailed understanding of engineering processes, industrial control logic, communication protocols, safety systems, and operational dependencies. This convergence of cybersecurity expertise and engineering knowledge significantly increases both the complexity and the potential consequences of nation-state cyber operations.

The strategic objectives of these campaigns therefore extend beyond compromising individual digital assets. Instead, sophisticated threat actors increasingly seek to understand how cyber-physical systems interact, identify critical operational dependencies, evaluate recovery capabilities, and determine how localized disruptions may propagate across interconnected infrastructure sectors. From an Operational Resilience Engineering perspective, these activities directly influence the resilience posture of industrial organizations by exposing vulnerabilities that extend beyond traditional cybersecurity controls.

Consequently, defending critical infrastructure requires a multidisciplinary engineering approach capable of integrating cybersecurity, engineering reliability, operational dependency analysis, governance, quantitative risk assessment, and operational continuity into a unified resilience strategy. This perspective recognizes that the principal challenge posed by nation-state cyber operations is not solely preventing unauthorized access, but sustaining mission-essential operations

despite persistent and strategically coordinated cyber threats.

The following subsection examines why critical infrastructure itself has become a strategic geopolitical target and explores how interconnected industrial dependencies amplify the potential consequences of cyber disruption across modern society.

C. Critical Infrastructure as a Strategic Target

> *"Critical infrastructure is targeted not because individual assets are valuable in isolation, but because their interdependencies amplify the operational consequences of disruption across society."*

Critical infrastructure constitutes the operational foundation of modern society by providing the essential services that enable economic activity, public safety, national security, and governmental continuity. Energy production, electricity transmission, natural gas pipelines, water treatment facilities, transportation systems, manufacturing operations, communications networks, and financial services collectively form an interconnected ecosystem whose continuous operation is fundamental to national resilience. Consequently, the strategic importance of these sectors extends far beyond the organizations that own or operate them.

The increasing digital transformation of industrial environments has substantially improved operational efficiency, automation, predictive maintenance, and decision-making capabilities. However, this transformation has simultaneously increased the degree of interconnection among Operational Technology (OT), Industrial Control Systems (ICS), enterprise Information Technology (IT), cloud services, Industrial Internet of Things (IIoT) devices, remote engineering platforms, and external service providers. As a result, critical infrastructure should no longer be viewed as a collection of independent industrial assets but rather as an integrated cyber-physical system characterized by complex operational dependencies.

These dependencies significantly influence the operational consequences of cyber disruption. The temporary loss of a single industrial component may produce limited operational impact when evaluated independently. However, the disruption of assets supporting multiple downstream processes may propagate rapidly throughout interconnected systems, producing cascading failures that extend well beyond the initially affected facility. Consequently, evaluating cyber risk exclusively at the individual asset level may underestimate the true operational consequences associated with highly interconnected critical infrastructure.

This systems perspective represents a fundamental principle of Operational Resilience Engineering (ORE). Rather than evaluating cybersecurity solely through the protection of individual devices or information systems, ORE considers how engineering dependencies, operational workflows, recovery capability, organizational preparedness, and infrastructure interconnections collectively influence the ability of mission-essential services to continue operating during adverse conditions. From this perspective, resilience becomes an emergent property of the entire operational ecosystem rather than a characteristic of isolated technological components.

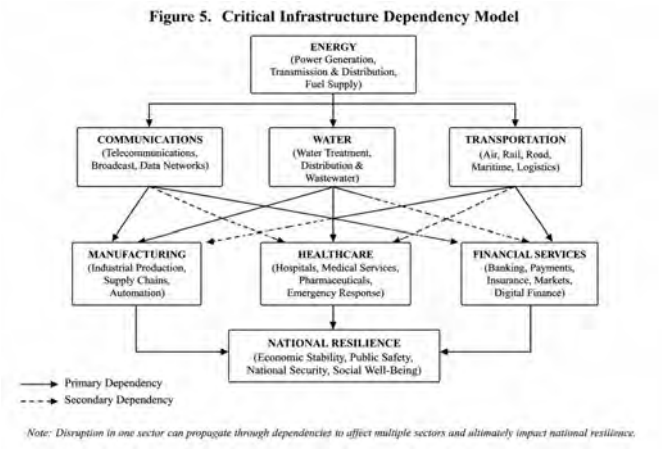

Fig. 5. Critical infrastructure dependency model illustrating how disruption in one sector may propagate through primary and secondary dependencies to affect national resilience.

The strategic value of critical infrastructure therefore arises from its role within a broader network of societal dependencies. Electrical power enables water treatment and distribution, transportation systems depend upon reliable energy and communications, manufacturing facilities rely upon stable supply chains and industrial automation, healthcare organizations require continuous power and telecommunications, and financial institutions depend upon resilient digital communications. Disruption affecting one sector may therefore propagate across multiple infrastructure domains, producing operational, economic, environmental, and societal consequences whose cumulative impact substantially exceeds the initiating event.

Consequently, protecting critical infrastructure requires expanding cybersecurity beyond traditional asset protection toward understanding how operational dependencies influence organizational resilience. This multidisciplinary perspective enables engineering organizations to identify critical operational relationships, prioritize resilience investments, evaluate cascading failure scenarios, and develop recovery strategies capable of sustaining mission-essential operations under increasingly complex cyber-physical conditions.

Figure **??** illustrates the interconnected nature of modern critical infrastructure and demonstrates how operational dependencies transform localized cyber disruptions into broader systemic consequences. This systems engineering perspective establishes the conceptual foundation for the resilience models developed in subsequent sections and provides the basis for the quantitative dependency analysis introduced within the Operational Resilience Engineering framework.

D. Cyber Operations Below the Threshold of War

> *"The most consequential cyber operations are often those that remain invisible, quietly establishing strategic advantage long before operational disruption occurs."*

One of the defining characteristics of contemporary cyber conflict is that many strategic cyber operations occur below the threshold traditionally associated with conventional warfare.

Rather than producing immediate physical destruction or publicly observable disruption, sophisticated cyber campaigns frequently emphasize long-term operational preparation through persistent access, infrastructure reconnaissance, intelligence collection, credential acquisition, supply-chain compromise, and the systematic identification of critical operational dependencies. These activities may remain undetected for extended periods while providing adversaries with the capability to influence future operational conditions.

Unlike conventional military operations, where strategic intent is often immediately apparent, cyber operations frequently evolve gradually through multiple stages that individually appear routine or insignificant. Activities such as vulnerability scanning, software updates, remote maintenance, third-party vendor access, cloud integration, and routine administrative operations may all provide opportunities for adversaries to expand their operational awareness without immediately affecting industrial processes. Consequently, distinguishing legitimate operational activity from malicious preparation becomes increasingly difficult within highly interconnected Operational Technology (OT) environments.

The strategic objective of these campaigns is frequently not immediate disruption but rather the establishment of operational advantage. Persistent access enables adversaries to observe engineering processes, understand operational workflows, identify critical assets, evaluate recovery procedures, and map dependencies among cyber-physical systems. This information significantly increases the ability to influence industrial operations during periods of geopolitical tension while minimizing the likelihood of early detection.

From an engineering perspective, the operational significance of persistent cyber campaigns extends beyond the compromise of individual devices or communication networks. The primary concern is the gradual accumulation of operational knowledge regarding how critical infrastructure functions under both normal and degraded conditions. Understanding equipment dependencies, maintenance schedules, control system logic, production constraints, backup capabilities, and recovery procedures provides valuable insight into the resilience characteristics of complex industrial environments.

This evolving threat environment fundamentally challenges traditional cybersecurity strategies that primarily emphasize prevention and perimeter protection. Although preventive security controls remain indispensable, organizations must also develop the capability to sustain safe and continuous operation when adversaries successfully bypass those controls. Consequently, resilience should not be evaluated solely according to whether unauthorized access occurs, but rather according to the capability of engineering systems to maintain mission-essential functions despite persistent cyber compromise.

Operational Resilience Engineering (ORE) addresses this challenge by shifting the analytical focus from isolated cyber events toward the operational consequences that may emerge from sustained cyber campaigns. Rather than assuming that every intrusion can be prevented, ORE recognizes that organizations must continuously evaluate engineering reliability, operational dependencies, recovery capability, governance, and quantitative risk in order to sustain resilient operations under uncertain and evolving threat conditions.

This perspective reflects an important evolution in the protection of critical infrastructure. Modern resilience strategies must account not only for the probability of cyber compromise but also for the capability of industrial systems to anticipate disruption, adapt to degraded operating conditions, maintain operational continuity, and recover essential services while minimizing operational, economic, environmental, and societal consequences.

Table **??** summarizes the principal operational characteristics of strategic cyber campaigns and their corresponding implications for Operational Resilience Engineering. Collectively, these characteristics demonstrate why resilience has become an engineering problem extending beyond traditional cybersecurity and establish the conceptual foundation for the quantitative resilience models introduced in the following section.

E. Implications for Operational Resilience Engineering

> *"Operational resilience is no longer achieved by preventing every cyber intrusion, but by engineering systems capable of sustaining mission-essential operations despite persistent cyber-physical disruption."*

The preceding discussion demonstrates that the protection of critical infrastructure has evolved beyond the traditional boundaries of cybersecurity. Digital transformation, geopolitical competition, operational interdependencies, and increasingly sophisticated cyber campaigns have collectively transformed cyber risk into a multidimensional engineering challenge whose consequences extend beyond information systems to affect industrial operations, economic stability, public safety, and national resilience.

This transformation fundamentally changes how resilience should be evaluated. Historically, cybersecurity programs have focused primarily on reducing the probability of successful cyber compromise through preventive controls, continuous monitoring, vulnerability management, and regulatory compliance. While these capabilities remain essential, they alone cannot guarantee the sustained operation of complex cyber-physical systems operating within highly dynamic threat environments. Consequently, resilience must be evaluated according to the capability of organizations to continue delivering mission-essential services despite adverse operational conditions.

Operational Resilience Engineering (ORE) provides the multidisciplinary systems engineering framework required to address this challenge. Rather than replacing established cybersecurity standards or regulatory frameworks, ORE integrates cybersecurity governance, engineering reliability, operational dependency analysis, quantitative risk assessment, recovery capability, and operational continuity into a unified methodology for sustaining industrial operations under uncertain conditions. This integrated perspective recognizes that resilience emerges from the interaction of technical, operational, organizational, and engineering capabilities rather than from any individual cybersecurity control.

A fundamental principle of ORE is that operational continuity should be treated as a measurable engineering objective. Consequently, the effectiveness of resilience strategies should be evaluated not only according to cybersecurity performance but also according to their ability to preserve production capability, maintain engineering reliability, minimize cascading operational failures, support executive decision-making, and reduce operational, economic, environmental, and societal consequences arising from cyber-physical disruption.

From this perspective, resilience becomes a continuously measurable property of the operational system rather than a static outcome of regulatory compliance. Engineering organizations must therefore evaluate how infrastructure dependencies evolve over time, how recovery capability changes under degraded operating conditions, how uncertainty influences operational risk, and how resilience investments contribute to sustaining mission-essential services throughout the lifecycle of disruptive events.

Accordingly, the remainder of this paper transitions from the qualitative analysis of geopolitical cyber risk toward the quantitative development of Operational Resilience Engineering. Building upon the ORE Fundamental Equation introduced previously, the following sections develop mathematical models for operational dependency analysis, engineering reliability, quantitative risk assessment, Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), Monte Carlo simulation, and resilience optimization. Collectively, these models establish a comprehensive engineering methodology for measuring, evaluating, and continuously improving the resilience of modern critical infrastructure.

IV. Quantitative Operational Resilience Engineering Framework

> *"Engineering disciplines become transformative when their principles can be measured, modeled, and optimized. Operational Resilience Engineering extends this philosophy to the protection of critical infrastructure."*

The preceding sections established the strategic motivation for Operational Resilience Engineering (ORE) by demonstrating that geopolitical competition, digital transformation, operational dependencies, and increasingly sophisticated cyber campaigns have fundamentally changed the protection requirements of modern critical infrastructure. Collectively, these developments demonstrate that cybersecurity alone cannot guarantee the sustained operation of mission-essential systems operating under persistent cyber-physical disruption. Consequently, resilience must evolve from a qualitative organizational objective into a measurable systems engineering discipline supported by quantitative analysis, engineering models, and continuous executive decision support.

This section presents the quantitative Operational Resilience Engineering framework that constitutes the principal scientific contribution of this paper. Building upon the ORE Fundamental Equation introduced in Section II, the proposed methodology transforms the conceptual principles of Operational Resilience Engineering into a structured mathematical framework capable of measuring, evaluating, and optimizing resilience across complex industrial environments.

Unlike conventional cybersecurity metrics that primarily evaluate technical controls or regulatory compliance, the proposed framework integrates cybersecurity capability, governance, engineering reliability, operational dependency analysis, recovery capability, and operational continuity into a unified quantitative model. Together, these engineering domains characterize the capability of industrial organizations to anticipate disruption, withstand adverse operating conditions, adapt to changing operational environments, recover essential functions, and sustain mission-essential services throughout the lifecycle of cyber-physical incidents.

From an engineering perspective, resilience should be regarded as a dynamic system property rather than a static compliance outcome. The resilience of industrial operations continuously evolves as infrastructure ages, operational dependencies change, cyber threats emerge, engineering configurations are modified, maintenance activities are performed, and organizational capabilities mature. Consequently, quantitative resilience assessment requires mathematical models capable of representing uncertainty, time-dependent behavior, engineering reliability, cascading dependencies, and operational risk across multiple organizational layers.

Accordingly, the quantitative framework developed throughout this section progressively expands the ORE Fundamental Equation through weighted resilience modeling, operational dependency analysis, engineering reliability theory, quantitative risk assessment, stochastic simulation, and resilience optimization. Collectively, these analytical models establish a rigorous mathematical foundation capable of supporting engineering design, operational planning, executive decision-making, investment prioritization, and continuous resilience improvement for modern critical infrastructure.

A. Mathematical Foundations of Operational Resilience Engineering

> *"A scientific discipline achieves engineering maturity when its principles can be expressed through measurable variables, quantitative models, and mathematically verifiable relationships."*

The ORE Fundamental Equation introduced in Section II establishes the conceptual architecture of Operational Resilience Engineering by identifying the principal engineering domains required to sustain mission-essential operations during cyber-physical disruption. While this conceptual framework provides the theoretical foundation of ORE, practical implementation requires transforming these principles into quantitative models capable of supporting engineering analysis, operational planning, investment prioritization, and executive decision-making.

From a systems engineering perspective, operational resilience should not be regarded as a binary condition in which organizations are classified simply as resilient or non-resilient. Instead, resilience represents a continuous engineering property whose value evolves according to changes in cybersecurity capability, governance maturity, engineering reliability,

operational dependencies, recovery capability, and operational continuity. Consequently, Operational Resilience Engineering requires mathematical models capable of integrating these multidimensional characteristics into a unified quantitative framework.

To establish this framework, the conceptual variables introduced in the ORE Fundamental Equation are represented as normalized engineering state variables whose values range from zero to one, where zero represents the absence of the corresponding capability and one represents the theoretical optimum under the defined evaluation criteria. Normalization provides a common mathematical scale that enables heterogeneous engineering disciplines to be integrated into a single resilience model while preserving interpretability across different industrial sectors.

Accordingly, the Operational Resilience Engineering score may be expressed as a weighted linear combination of the normalized engineering state variables:

$$ORE = w_1 C_s + w_2 G + w_3 E + w_4 D + w_5 R_c + w_6 C_o \quad (2)$$

subject to

$$\sum_{i=1}^{6} w_i = 1, \qquad 0 \leq w_i \leq 1 \quad (3)$$

where

- C_s represents Cybersecurity Capability;
- G represents Governance and Regulatory Compliance;
- E represents Engineering Reliability;
- D represents Operational Dependency Resilience;
- R_c represents Recovery Capability;
- C_o represents Operational Continuity;
- w_i represents the relative importance assigned to each engineering domain.

Equation (2) defines the first quantitative Operational Resilience Engineering model proposed in this paper. Unlike traditional cybersecurity maturity models that primarily assess technical controls or regulatory compliance, the Weighted ORE Model integrates technical, operational, organizational, and engineering dimensions into a unified resilience metric capable of supporting objective performance evaluation across complex cyber-physical environments.

The weighting coefficients provide the flexibility necessary to adapt the model to different critical infrastructure sectors and organizational priorities. For example, an electrical transmission operator may assign greater importance to engineering reliability and operational continuity, whereas a pipeline operator may emphasize dependency management and recovery capability. Consequently, the proposed framework accommodates sector-specific operational characteristics while preserving a common mathematical structure applicable across diverse industrial environments.

An important characteristic of the Weighted ORE Model is its extensibility. Additional engineering variables, organizational factors, or sector-specific resilience indicators may be incorporated through the introduction of additional weighted terms without altering the underlying mathematical formulation. This scalability enables the framework to evolve alongside emerging technologies, regulatory requirements, and operational practices while maintaining methodological consistency.

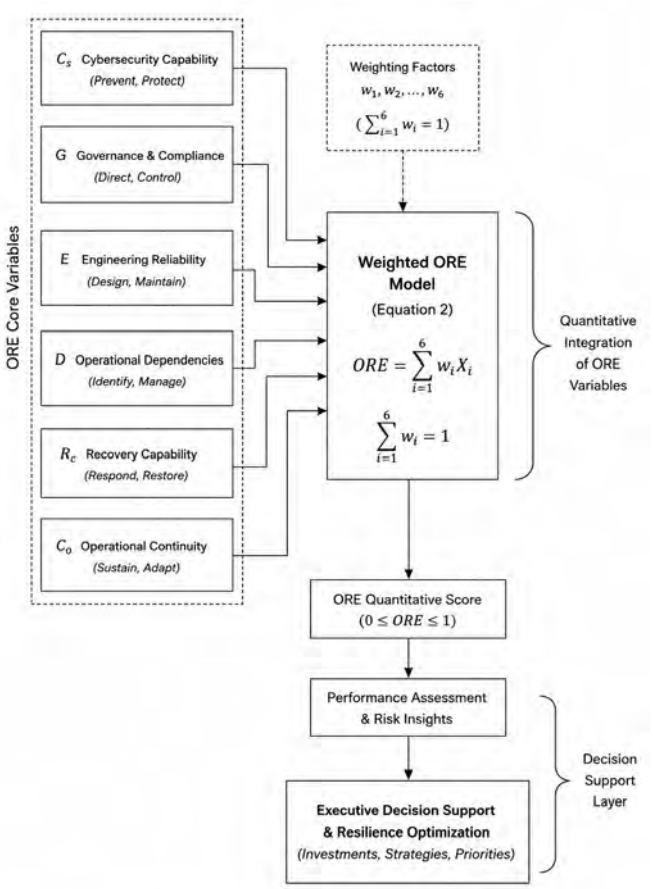

Figure 6. Quantitative Operational Resilience Engineering (ORE) Framework.

Fig. 6. Quantitative Operational Resilience Engineering (ORE) framework. The model integrates cybersecurity capability (C_s), governance (G), engineering reliability (E), operational dependency analysis (D), recovery capability (R_c), and operational continuity (C_o) into the Weighted ORE Model, providing a quantitative resilience score to support engineering assessment, executive decision-making, and resilience optimization.

The Weighted ORE Model therefore establishes the quantitative foundation of Operational Resilience Engineering upon which the subsequent analytical models developed throughout this paper are constructed. In the following subsections, this deterministic formulation is progressively expanded through operational dependency modeling, engineering reliability theory, quantitative risk assessment, stochastic simulation, and optimization techniques that collectively provide a comprehensive methodology for evaluating and improving the resilience of modern critical infrastructure.

B. Operational Dependency Modeling

> *"The resilience of critical infrastructure is determined not only by the reliability of individual assets, but by the strength and complexity of the operational dependencies that connect them."*

Operational dependency constitutes one of the fundamental principles of Operational Resilience Engineering (ORE). Modern critical infrastructure should not be regarded as a collection of independent engineering assets but rather as a highly interconnected cyber-physical ecosystem in which the performance of individual components directly influences the operational capability of the entire system. Consequently, resilience cannot be evaluated exclusively through isolated asset assessments; instead, it must consider the dynamic relationships that exist among engineering processes, industrial control systems, communications networks, external services, human operators, and supporting infrastructure.

Within complex industrial environments, operational dependencies may exist across multiple organizational and technical layers. Physical processes depend upon reliable instrumentation, programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, communication networks, electrical power, maintenance personnel, cloud-based services, and external suppliers. A disruption affecting any of these elements may propagate through interconnected processes, producing cascading operational consequences that substantially exceed the impact of the initiating event.

From an engineering perspective, dependency modeling provides a systematic methodology for identifying these relationships and evaluating how localized failures influence the resilience of the broader operational system. Unlike conventional asset inventories, dependency models explicitly represent the directional relationships among critical assets, enabling organizations to evaluate failure propagation, identify single points of failure, prioritize resilience investments, and improve recovery planning.

Mathematically, the operational dependencies within a critical infrastructure system may be represented by a directed dependency matrix,

$$\mathbf{D} = [d_{ij}], \tag{4}$$

where each element d_{ij} represents the dependency of asset i upon asset j. The dependency coefficient is normalized such that

$$0 \leq d_{ij} \leq 1,$$

where

- $d_{ij} = 0$ indicates no operational dependency,
- $0 < d_{ij} < 1$ represents partial dependency, and
- $d_{ij} = 1$ denotes complete operational dependency.

The overall operational dependency of the system may then be expressed as

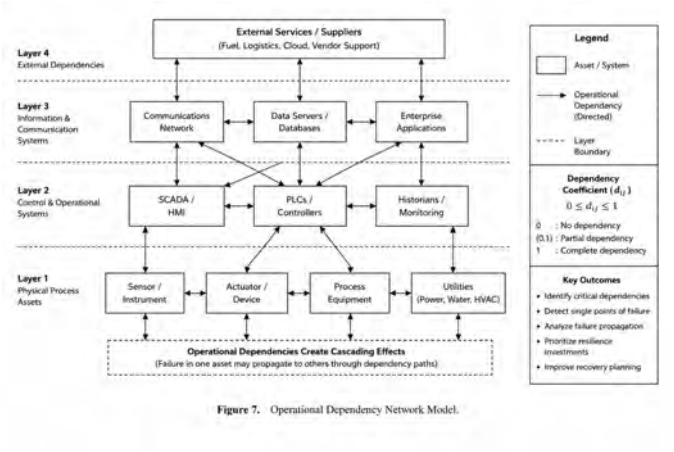

Figure 7. Operational Dependency Network Model.

Fig. 7. Operational Dependency Network Model illustrating the multi-layer interdependencies among cyber-physical assets within critical infrastructure. The model demonstrates how localized disruptions may propagate through operational dependency paths, producing cascading effects that influence overall system resilience.

$$D = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{\substack{j=1 \\ j \neq i}}^{N} d_{ij}, \tag{5}$$

where N denotes the total number of critical assets within the operational environment. This normalized metric provides a quantitative measure of the degree of interdependence across the system and enables comparative evaluation among different facilities, sectors, or engineering architectures.

The proposed dependency model also provides the mathematical basis for evaluating cascading operational failures. As dependency values increase, localized disruptions are more likely to propagate across interconnected assets, reducing the overall resilience of the operational system. Conversely, engineering strategies such as redundancy, segmentation, isolation, and graceful degradation reduce effective dependency values and improve the capability of critical infrastructure to sustain mission-essential operations during cyber-physical disruption.

Figure 7 illustrates the proposed Operational Dependency Model and demonstrates how engineering assets interact through multiple layers of cyber-physical dependencies. The model provides the conceptual foundation for the engineering reliability analysis presented in the following subsection and establishes the mathematical linkage between infrastructure interdependencies and the quantitative Operational Resilience Engineering framework.

Figure 7 illustrates the proposed Operational Dependency Model and demonstrates how engineering assets interact through multiple layers of cyber-physical dependencies. The model provides the conceptual foundation for the engineering reliability analysis presented in the following subsection and establishes the mathematical linkage between infrastructure interdependencies and the quantitative Operational Resilience Engineering framework.

C. Engineering Reliability Modeling

> *"Operational resilience depends not only upon preventing failure, but upon understanding how engineering systems degrade, recover, and continue operating under adverse conditions."*

Engineering reliability has long served as one of the fundamental disciplines supporting the design, operation, and maintenance of complex industrial systems. Traditionally, reliability engineering evaluates the probability that physical assets perform their intended functions under specified operating conditions throughout a defined period of time. Within modern critical infrastructure, however, engineering reliability extends beyond mechanical degradation to encompass cyber-physical interactions, operational dependencies, control systems, digital communications, and human decision-making.

From the perspective of Operational Resilience Engineering (ORE), reliability should be interpreted as the capability of an operational system to continue performing mission-essential functions despite component degradation, cyber disruption, equipment failures, or adverse operating conditions. Consequently, resilience depends not only upon the reliability of individual assets but also upon the collective reliability of the interconnected engineering system.

The reliability of an individual engineering asset may be represented by the classical reliability function

$$R(t) = P(T > t), \tag{6}$$

where T denotes the random time to failure and $R(t)$ represents the probability that the asset continues operating successfully beyond time t.

For many industrial systems, the Weibull distribution provides an effective representation of engineering degradation and failure behavior. Accordingly, the reliability function may be expressed as

$$R(t) = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right], \tag{7}$$

where

- η represents the characteristic life,
- β denotes the Weibull shape parameter, and
- t represents operating time.

The value of the shape parameter provides valuable engineering insight into asset behavior. Values of $\beta < 1$ typically indicate early-life failures, $\beta = 1$ represents approximately constant failure rates, while $\beta > 1$ characterizes progressive aging and wear-out mechanisms commonly observed in industrial equipment operating under long-term service conditions.

Although individual asset reliability remains important, Operational Resilience Engineering extends reliability analysis to the operational system level. Modern industrial environments consist of numerous interconnected assets whose combined behavior determines the capability of the organization to sustain mission-essential operations. Consequently, overall operational reliability depends upon both component reliability and the dependency relationships introduced in the previous subsection.

Accordingly, the operational reliability of a system containing N critical assets may be approximated by

$$R_{sys} = \prod_{i=1}^{N} R_i^{\alpha_i}, \tag{8}$$

where

- R_i represents the reliability of asset i, and
- α_i denotes the operational criticality weighting factor associated with each asset, satisfying

$$\sum_{i=1}^{N} \alpha_i = 1.$$

The operational criticality coefficients enable the model to recognize that not all engineering assets contribute equally to mission continuity. Assets supporting essential operational processes may therefore receive greater weighting than redundant or non-critical components. This weighted formulation better reflects the operational characteristics of modern industrial systems than conventional reliability models that assume equal importance among system components.

Figure 8 illustrates the Engineering Reliability Model proposed within the Operational Resilience Engineering framework. The figure demonstrates how individual asset reliability, degradation mechanisms, operational criticality, and dependency relationships collectively determine overall system reliability and operational resilience.

The reliability models introduced in this subsection establish the engineering foundation required for the quantitative risk models developed in the following subsection. Specifically, the system reliability metrics derived here provide essential inputs for estimating Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and the stochastic resilience simulations that follow.

Figure 8 illustrates the Engineering Reliability Model proposed within the Operational Resilience Engineering framework. The figure demonstrates how individual asset reliability, degradation mechanisms, operational criticality, and dependency relationships collectively determine overall system reliability and operational resilience.

D. Quantitative Risk Assessment for Operational Resilience

> *"Operational resilience cannot be effectively managed unless uncertainty, potential losses, and extreme operational scenarios are quantified through objective engineering models."*

Engineering decisions supporting critical infrastructure increasingly require quantitative methodologies capable of evaluating uncertainty, estimating potential operational losses, and supporting resilience investment decisions under adverse conditions. While traditional cybersecurity assessments frequently rely upon qualitative risk matrices or maturity-based evaluations, Operational Resilience Engineering (ORE) extends risk assessment through probabilistic models capable of

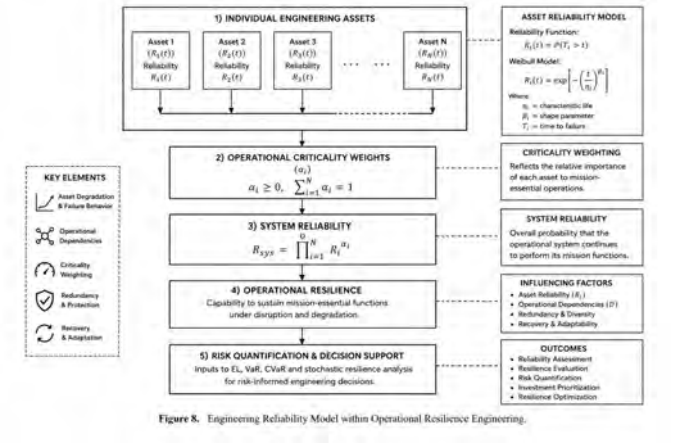

Fig. 8. Engineering Reliability Model within the Operational Resilience Engineering (ORE) framework. Individual engineering asset reliability is integrated through operational criticality weighting to estimate system reliability, providing the analytical foundation for resilience evaluation, quantitative risk assessment, and executive decision support.

quantifying both expected operational performance and low-probability, high-consequence events.

From the perspective of Operational Resilience Engineering, risk should be interpreted as the combination of uncertainty, operational consequences, infrastructure dependencies, engineering reliability, and recovery capability. Consequently, quantitative risk assessment provides the analytical foundation for evaluating how cyber-physical disruptions influence mission-essential operations and for identifying engineering strategies capable of minimizing operational degradation.

The first quantitative metric considered within the proposed framework is the Expected Loss (EL), representing the average operational consequence associated with a defined set of disruptive scenarios. Expected Loss may be expressed as

$$EL = \sum_{i=1}^{N} P_i L_i, \tag{9}$$

where

- P_i denotes the probability of scenario i, and
- L_i represents the corresponding operational, financial, environmental, or societal loss.

Although Expected Loss provides an estimate of average operational impact, it does not adequately represent the consequences of extreme but plausible events that frequently dominate executive decision-making within critical infrastructure. Accordingly, Value at Risk (VaR) is introduced to estimate the maximum expected operational loss that will not be exceeded for a specified confidence level α.

The Value at Risk is defined as

$$VaR_\alpha = \inf \{x : F(x) \geq \alpha\}, \tag{10}$$

where $F(x)$ denotes the cumulative distribution function of operational losses.

Because VaR does not provide information regarding losses exceeding the selected confidence threshold, Conditional Value at Risk (CVaR) is incorporated to evaluate the expected consequence of extreme operational scenarios. CVaR therefore provides a more informative measure of tail risk within complex cyber-physical environments and is expressed as

$$CVaR_\alpha = E\left[L \mid L > VaR_\alpha\right]. \tag{11}$$

Collectively, Expected Loss, Value at Risk, and Conditional Value at Risk provide complementary perspectives for evaluating operational resilience. Expected Loss characterizes average system performance, Value at Risk quantifies probable worst-case operational losses at a specified confidence level, and Conditional Value at Risk measures the severity of extreme disruption scenarios that extend beyond conventional planning assumptions. Together, these metrics provide executive decision-makers with a comprehensive quantitative understanding of operational risk across both routine and catastrophic conditions.

To evaluate uncertainty arising from complex dependency relationships and engineering variability, Operational Resilience Engineering incorporates Monte Carlo simulation. Random sampling of failure probabilities, dependency relationships, degradation mechanisms, recovery times, and operational consequences enables the estimation of complete probability distributions rather than single deterministic values. This stochastic methodology supports sensitivity analysis, resilience optimization, investment prioritization, and strategic planning under uncertain operating conditions.

Figure 9 illustrates the quantitative risk assessment framework proposed within Operational Resilience Engineering and demonstrates the integration of Expected Loss, Value at Risk, Conditional Value at Risk, and Monte Carlo simulation into a unified executive decision-support methodology. Collectively, these analytical models establish the quantitative foundation required for optimizing operational resilience under uncertain cyber-physical conditions.

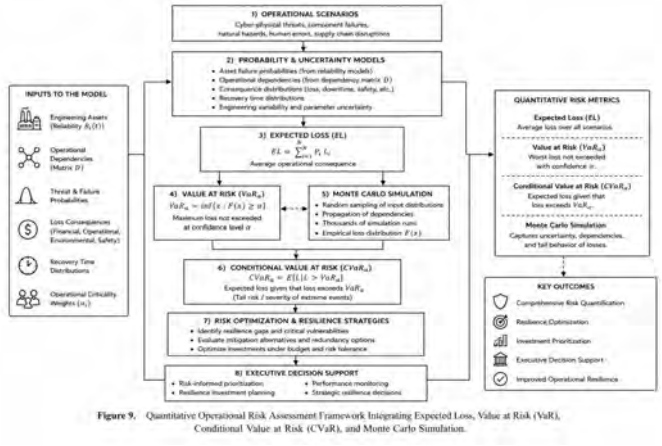

Figure 9. Quantitative Operational Risk Assessment Framework Integrating Expected Loss, Value at Risk (VaR), Conditional Value at Risk (CVaR), and Monte Carlo Simulation.

Fig. 9. Quantitative Operational Risk Assessment Framework integrating Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and Monte Carlo simulation. The framework combines engineering reliability, operational dependencies, uncertainty modeling, and probabilistic risk metrics to support resilience optimization and executive decision-making under cyber-physical disruption.

E. Dynamic Operational Resilience Model

> *"Operational resilience is not a static attribute but a continuously evolving engineering property influenced by changing operational conditions, infrastructure dependencies, degradation mechanisms, recovery capability, and uncertainty."*

The quantitative models developed throughout the preceding subsections establish the principal engineering components required to evaluate Operational Resilience Engineering (ORE). However, modern critical infrastructure operates within continuously changing operational environments characterized by equipment aging, evolving cyber threats, maintenance activities, operational reconfiguration, changing dependency relationships, and dynamic recovery conditions. Consequently, operational resilience should not be represented as a fixed value but rather as a time-dependent engineering state that evolves throughout the lifecycle of industrial operations.

This dynamic perspective extends the deterministic Weighted ORE Model introduced previously by allowing each engineering variable to vary as operational conditions change. Accordingly, the resilience state of an operational system may be expressed as

$$\begin{aligned} ORE(t) = {} & w_1 C_s(t) + w_2 G(t) + w_3 E(t) \\ & + w_4 D(t) + w_5 R_c(t) + w_6 C_o(t) \end{aligned} \tag{12}$$

subject to

$$\sum_{i=1}^{6} w_i = 1, \qquad 0 \le w_i \le 1. \tag{13}$$

Equation (12) represents the Dynamic Operational Resilience Engineering Model proposed in this paper. Unlike static resilience assessments that provide only a snapshot of organizational capability, the proposed formulation continuously reflects changes in cybersecurity capability, governance maturity, engineering reliability, operational dependencies, recovery capability, and operational continuity throughout the operational lifecycle.

The time dependency introduced in Equation (12) enables the framework to incorporate evolving engineering conditions such as equipment degradation, maintenance activities, operational reconfiguration, cyber threat intelligence, environmental conditions, supply chain disruptions, and organizational adaptation. Consequently, the resilience score becomes a continuously updated engineering indicator capable of supporting both operational monitoring and strategic planning.

The Dynamic ORE Model also provides the mathematical foundation for integrating Digital Twins, Industrial Internet of Things (IIoT) platforms, supervisory control and data acquisition (SCADA) systems, engineering analytics, and artificial intelligence into a unified resilience assessment environment. Real-time operational measurements may continuously update the engineering state variables, allowing the resilience score to evolve automatically as industrial conditions change.

Within this dynamic framework, quantitative risk metrics such as Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and Monte Carlo simulation become continuously adaptive rather than periodically evaluated. This capability enables engineering organizations to identify emerging operational vulnerabilities, evaluate alternative resilience strategies, prioritize engineering investments, and optimize recovery planning before localized failures propagate throughout interconnected critical infrastructure.

Accordingly, Operational Resilience Engineering evolves from a periodic assessment methodology into a continuously operating engineering decision-support system capable of monitoring resilience, forecasting degradation, evaluating uncertainty, and supporting executive decision-making in real time. This dynamic perspective represents one of the principal contributions of the proposed ORE framework and establishes the mathematical foundation for future resilience-oriented Digital Twin architectures and autonomous engineering optimization systems.

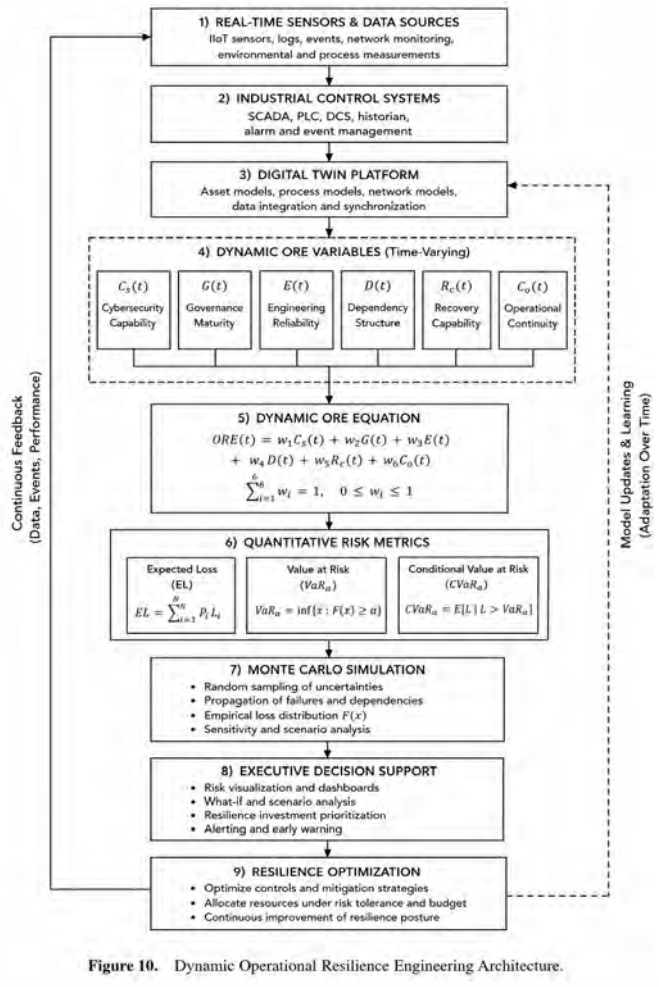

Figure 10. Dynamic Operational Resilience Engineering Architecture.

Fig. 10. Dynamic Operational Resilience Engineering architecture integrating real-time data sources, industrial control systems, digital twin models, time-varying ORE variables, quantitative risk metrics, Monte Carlo simulation, executive decision support, and resilience optimization.

V. Application of the Operational Resilience Engineering Framework

"The ultimate value of an engineering methodology lies not only in its theoretical rigor but also in its practical ability to support better operational decisions under uncertainty."

The quantitative Operational Resilience Engineering (ORE) framework developed throughout the previous section provides a systematic methodology for measuring, evaluating, and optimizing resilience within complex cyber-physical environments. This section demonstrates how the proposed framework may be applied to representative critical infrastructure systems to support engineering analysis, resilience assessment, operational planning, and executive decision-making.

Rather than focusing on a single industrial sector, the proposed methodology is intentionally designed to be sector-independent and scalable across energy systems, manufacturing facilities, transportation networks, water treatment plants, healthcare infrastructure, telecommunications, and other mission-essential environments. Although engineering configurations differ among sectors, the underlying principles governing operational dependencies, engineering reliability, quantitative risk, and operational continuity remain fundamentally consistent.

The application methodology presented herein follows a structured engineering workflow beginning with infrastructure characterization, followed by dependency identification, reliability assessment, quantitative risk modeling, resilience optimization, and executive decision support. This systematic process enables organizations to continuously evaluate resilience, prioritize engineering investments, quantify operational uncertainty, and support informed strategic decision-making throughout the lifecycle of cyber-physical operations.

The following subsections illustrate each stage of the proposed implementation methodology and demonstrate how the Operational Resilience Engineering framework may be incorporated into existing industrial engineering practices without replacing established cybersecurity or operational governance frameworks.

A. Reference Critical Infrastructure Architecture (RCIA)

"Operational resilience begins with understanding the engineering architecture of the systems that sustain mission-essential operations."

The practical implementation of Operational Resilience Engineering (ORE) begins with the characterization of the operational environment under evaluation. Because modern critical infrastructure encompasses a wide range of industrial sectors—including energy, water, manufacturing, transportation, healthcare, telecommunications, mining, and food processing—a generalized engineering architecture is required to provide a consistent basis for resilience assessment. Accordingly, this paper introduces the Reference Critical Infrastructure Architecture (RCIA), a sector-independent systems engineering model that captures the principal cyber-physical components commonly found across modern industrial environments.

The purpose of the RCIA is not to replicate the detailed configuration of any individual facility but rather to establish a representative engineering architecture capable of supporting quantitative resilience analysis across multiple infrastructure sectors. By defining a standardized reference model, organizations may apply the Operational Resilience Engineering framework using a common analytical methodology while adapting individual engineering parameters to their specific operational environments.

The proposed RCIA consists of six interrelated engineering layers that collectively represent the operational structure of modern critical infrastructure:

1) **Physical Process Layer**, comprising industrial equipment, production assets, field instrumentation, sensors, actuators, electrical systems, rotating machinery, and process equipment responsible for delivering mission-essential services.
2) **Operational Control Layer**, consisting of programmable logic controllers (PLCs), distributed control

systems (DCS), remote terminal units (RTUs), supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMIs), and safety instrumented systems (SIS) responsible for monitoring and controlling physical processes.

3) **Industrial Communications Layer**, including industrial Ethernet, fieldbus protocols, wireless communications, fiber-optic networks, industrial gateways, and secure communication infrastructure supporting operational data exchange.
4) **Operational Information Layer**, incorporating historians, engineering workstations, asset management systems, maintenance platforms, Digital Twin models, Industrial Internet of Things (IIoT) platforms, artificial intelligence services, and operational analytics.
5) **Enterprise Integration Layer**, representing enterprise resource planning (ERP), manufacturing execution systems (MES), business applications, cloud services, remote support capabilities, cybersecurity monitoring platforms, and executive decision-support systems.
6) **External Dependency Layer**, representing the external services upon which industrial operations depend, including electrical power, telecommunications, cloud providers, supply-chain partners, logistics services, regulatory agencies, emergency response organizations, and critical third-party vendors.

Unlike conventional network architectures that primarily emphasize communication pathways, the RCIA explicitly represents operational dependencies among engineering functions. Consequently, every layer contributes not only to information exchange but also to the capability of the organization to sustain mission-essential operations under degraded operating conditions. This systems engineering perspective enables resilience assessment to incorporate technical performance, engineering reliability, operational continuity, organizational governance, and external dependencies within a unified analytical framework.

Figure 11 illustrates the proposed Reference Critical Infrastructure Architecture and identifies the principal engineering domains evaluated throughout the Operational Resilience Engineering methodology. The layered architecture provides the structural foundation upon which dependency analysis, engineering reliability modeling, quantitative risk assessment, and resilience optimization are subsequently performed.

The RCIA serves as the baseline engineering model for the remainder of this paper. All subsequent analyses—including operational dependency mapping, engineering reliability assessment, Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), Monte Carlo simulation, and resilience optimization—are developed with reference to this generalized architecture. Consequently, the proposed methodology remains applicable across diverse critical infrastructure sectors while preserving a consistent mathematical and engineering framework for resilience evaluation.

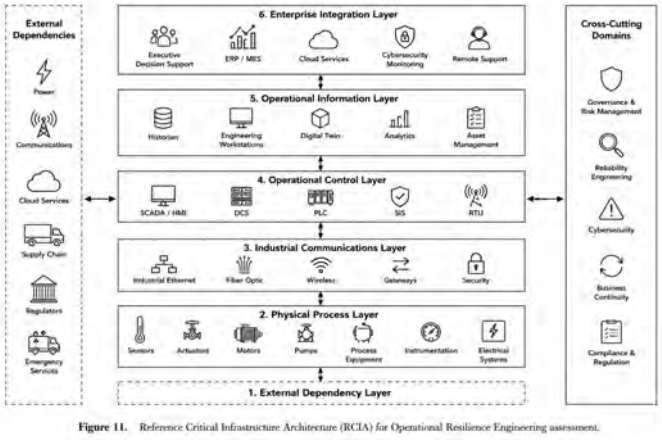

Figure 11. Reference Critical Infrastructure Architecture (RCIA) for Operational Resilience Engineering assessment.

Fig. 11. Reference Critical Infrastructure Architecture (RCIA) for Operational Resilience Engineering assessment.

B. Operational Dependency Assessment

> *"Understanding operational dependencies is essential for identifying how localized failures propagate throughout interconnected cyber-physical systems and ultimately influence mission continuity."*

The second stage of the Operational Resilience Engineering (ORE) methodology consists of evaluating the operational dependencies that exist among the critical assets identified within the Reference Critical Infrastructure Architecture (RCIA). Modern industrial facilities operate as highly interconnected cyber-physical ecosystems in which the operational state of one asset frequently depends upon the availability, performance, and reliability of numerous supporting systems. Consequently, resilience assessment requires understanding not only the characteristics of individual assets but also the relationships that govern the propagation of operational disruption.

The proposed dependency assessment methodology begins by identifying mission-essential assets and the operational services they provide. Typical assets include industrial controllers, supervisory control systems, communication infrastructure, safety systems, engineering workstations, electrical power, cloud services, maintenance resources, and critical third-party providers. Once these assets have been identified, their operational relationships are represented through a directed dependency network in which each connection describes the degree to which one asset depends upon another for continued operation.

The dependency relationships are represented by the Operational Dependency Matrix introduced in Section IV,

$$\mathbf{D} = [d_{ij}], \tag{14}$$

where each element d_{ij} represents the normalized operational dependency of asset i upon asset j, with values ranging from zero (no dependency) to one (complete dependency).

While the dependency matrix describes the structure of the operational network, executive decision-making requires identifying which assets exert the greatest influence on mission

continuity. Accordingly, this paper introduces the **Operational Dependency Criticality Index (ODCI)**, defined as

$$ODCI_i = \sum_{j=1}^{N} w_j d_{ij}, \tag{15}$$

where

- d_{ij} represents the dependency coefficient between assets,
- w_j denotes the operational importance assigned to asset j, satisfying

$$\sum_{j=1}^{N} w_j = 1,$$

- $ODCI_i$ represents the overall operational dependency criticality associated with asset i.

The Operational Dependency Criticality Index provides a normalized measure of the influence that each asset exerts on the continuity of mission-essential operations. Assets exhibiting larger ODCI values represent higher-priority engineering components whose disruption may generate significant cascading operational consequences throughout the cyber-physical environment. Conversely, assets with lower dependency criticality generally contribute less to large-scale operational disruption and may therefore receive lower priority during resilience planning.

Figure 12 illustrates the proposed Operational Dependency Assessment methodology. Beginning with the identification of critical operational assets, the methodology progressively develops dependency relationships, constructs the operational dependency matrix, computes the Operational Dependency Criticality Index, and prioritizes engineering investments according to their contribution to overall operational resilience.

The Operational Dependency Assessment establishes the analytical foundation for the engineering reliability evaluation presented in the following subsection. By quantifying operational interdependencies before estimating failure probabilities, the proposed methodology ensures that engineering reliability reflects not only component performance but also the operational significance of each asset within the broader cyber-physical system.

C. Engineering Reliability Assessment

> *"Operational resilience depends not only upon the reliability of engineering assets but also upon the operational significance of those assets within the broader cyber-physical ecosystem."*

Following the identification of operational dependencies, the next stage of the Operational Resilience Engineering (ORE) methodology evaluates the engineering reliability of mission-essential assets. While dependency analysis identifies the operational relationships that exist among interconnected systems, engineering reliability quantifies the probability that individual assets continue performing their intended operational functions throughout a specified mission period.

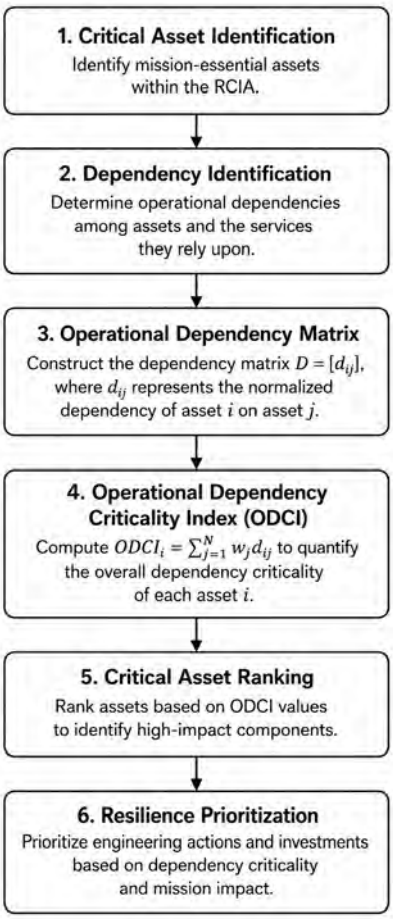

Figure 12. Operational Dependency Assessment Methodology.

Fig. 12. Operational Dependency Assessment methodology for identifying critical assets, constructing the dependency matrix, computing the Operational Dependency Criticality Index (ODCI), and prioritizing resilience investments.

Engineering reliability has traditionally focused on estimating component failure probabilities using statistical degradation models and historical operational data. Within the proposed ORE framework, however, reliability assessment extends beyond individual asset performance by incorporating operational dependency criticality into the overall engineering evaluation. Consequently, resilience assessment reflects not only the probability of asset failure but also the operational consequences associated with that failure.

For each critical asset identified within the Reference Critical Infrastructure Architecture (RCIA), engineering reliability is initially evaluated using the classical reliability function introduced in Section IV,

$$R_i(t) = P(T_i > t), \tag{16}$$

where T_i denotes the time to failure of asset i and $R_i(t)$ represents the probability that the asset continues operating beyond time t.

TABLE II
ILLUSTRATIVE ENGINEERING RELIABILITY ASSESSMENT RESULTS

Asset	R_i	ODCI	ORI	Priority
PLC-1	0.99	0.92	0.91	High
SCADA Server	0.98	0.88	0.86	High
Safety Instrumented System (SIS)	0.99	0.85	0.84	High
Industrial Ethernet	0.97	0.81	0.79	High
Historian	0.95	0.56	0.53	Medium
Engineering Workstation	0.94	0.41	0.39	Medium
Backup Server	0.96	0.18	0.17	Low

When historical degradation information is available, asset reliability may be estimated using the Weibull reliability model

$$R_i(t) = \exp\left[-\left(\frac{t}{\eta_i}\right)^{\beta_i}\right], \tag{17}$$

where η_i denotes the characteristic life and β_i represents the Weibull shape parameter associated with asset i.

Although reliability alone provides valuable engineering information, it does not identify which failures produce the greatest operational disruption. Accordingly, this paper introduces the **Operational Reliability Index (ORI)**, which combines engineering reliability with the Operational Dependency Criticality Index (ODCI) introduced in the previous subsection,

$$ORI_i = R_i \times ODCI_i. \tag{18}$$

where

- R_i represents the engineering reliability of asset i,
- $ODCI_i$ represents the Operational Dependency Criticality Index,
- ORI_i represents the Operational Reliability Index.

The Operational Reliability Index provides a quantitative measure of the contribution that each engineering asset makes to sustained operational performance. Assets exhibiting simultaneously high reliability and high dependency criticality receive larger ORI values and therefore represent mission-essential components requiring continuous monitoring and resilience preservation. Conversely, assets with lower ORI values generally exert less influence upon overall operational continuity and may therefore receive lower engineering priority.

Figure 13 illustrates the Engineering Reliability Assessment methodology. Beginning with engineering asset identification, the methodology evaluates reliability using probabilistic degradation models, integrates operational dependency criticality, computes the Operational Reliability Index, and prioritizes engineering activities according to their contribution to operational resilience.

The Operational Reliability Index (ORI) may be interpreted according to the following engineering classification:

- ORI ≥ 0.80: High engineering priority.
- $0.50 \leq$ ORI < 0.80: Medium engineering priority.
- ORI < 0.50: Low engineering priority.

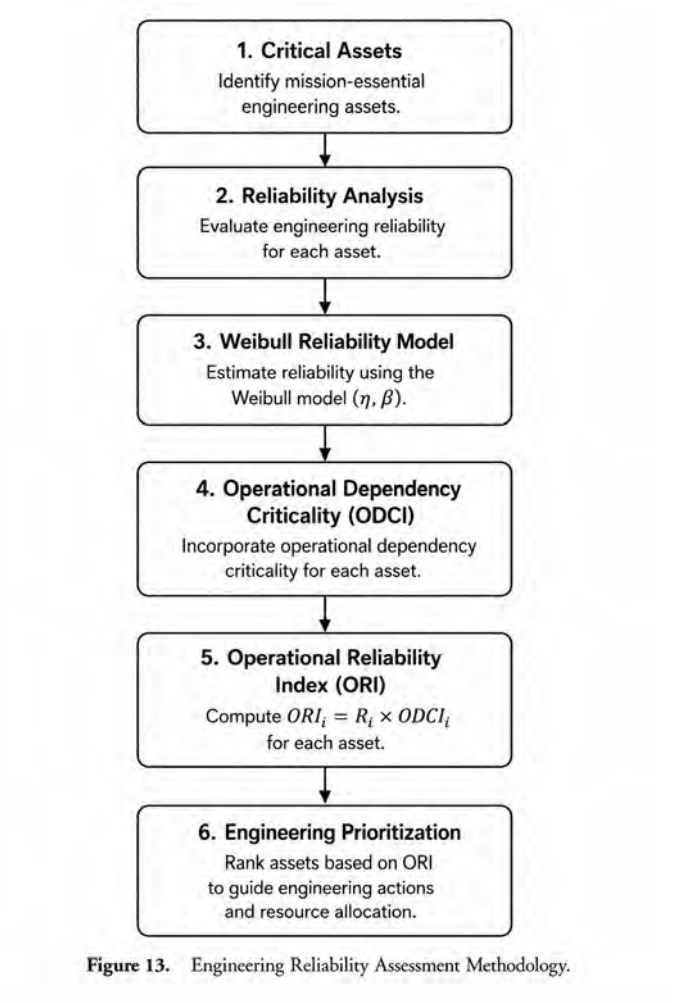

Figure 13. Engineering Reliability Assessment Methodology.

Fig. 13. Engineering Reliability Assessment methodology for evaluating asset reliability, incorporating Operational Dependency Criticality Index (ODCI), computing the Operational Reliability Index (ORI), and prioritizing engineering actions.

The Operational Reliability Index establishes the analytical bridge between engineering reliability and quantitative operational risk. The ORI values obtained in this subsection provide the principal weighting factors used during the quantitative risk assessment developed in the following subsection, thereby ensuring that Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and resilience optimization reflect both engineering performance and operational significance.

D. Quantitative Risk Analysis

> *"Operational resilience is ultimately measured not by the occurrence of disruptive events, but by their quantified operational consequences and the organization's ability to sustain mission-essential services."*

Having established the operational dependency structure and engineering reliability characteristics of the Reference Critical Infrastructure Architecture (RCIA), the next stage of the Operational Resilience Engineering (ORE) methodology consists of quantifying the operational consequences associ-

ated with cyber-physical disruption. Quantitative risk analysis provides the mathematical basis for evaluating uncertainty, estimating potential operational losses, prioritizing resilience investments, and supporting executive decision-making under adverse operating conditions.

Unlike traditional qualitative risk matrices, the proposed methodology incorporates probabilistic engineering models that combine operational dependencies, engineering reliability, and asset criticality into a unified quantitative framework. Consequently, resilience decisions are supported by objective numerical indicators rather than subjective qualitative assessments.

The first quantitative metric employed within the framework is the Expected Loss (EL), representing the average operational consequence associated with the evaluated disruption scenarios,

$$EL = \sum_{i=1}^{N} P_i L_i, \tag{19}$$

where P_i denotes the probability of disruption scenario i, and L_i represents the associated operational loss.

To account for engineering criticality, the Operational Reliability Index (ORI) introduced in the previous subsection is incorporated into the estimation of expected operational losses,

$$EL_{ORE} = \sum_{i=1}^{N} ORI_i P_i L_i. \tag{20}$$

Equation (20) extends the traditional Expected Loss formulation by weighting each disruption scenario according to the operational importance and engineering reliability of the affected asset. Consequently, failures affecting highly reliable but operationally critical assets receive greater consideration during resilience planning than failures involving assets with comparatively lower operational significance.

To evaluate extreme operational scenarios, the methodology further incorporates Value at Risk (VaR) and Conditional Value at Risk (CVaR),

$$VaR_\alpha = \inf\{x : F(x) \geq \alpha\}, \tag{21}$$

$$CVaR_\alpha = E[L|L > VaR_\alpha]. \tag{22}$$

Finally, Monte Carlo simulation is employed to evaluate uncertainty arising from engineering variability, dependency propagation, equipment degradation, recovery capability, and cyber-physical disruption. Thousands of simulated operational scenarios generate empirical probability distributions from which expected operational losses, extreme-event probabilities, confidence intervals, and resilience performance indicators may be estimated.

Figure 14 illustrates the proposed Quantitative Risk Analysis methodology. Beginning with engineering reliability and operational dependency information, the methodology estimates Expected Loss, evaluates tail risk through VaR and CVaR, performs Monte Carlo simulation, and ultimately supports resilience optimization and executive decision-making.

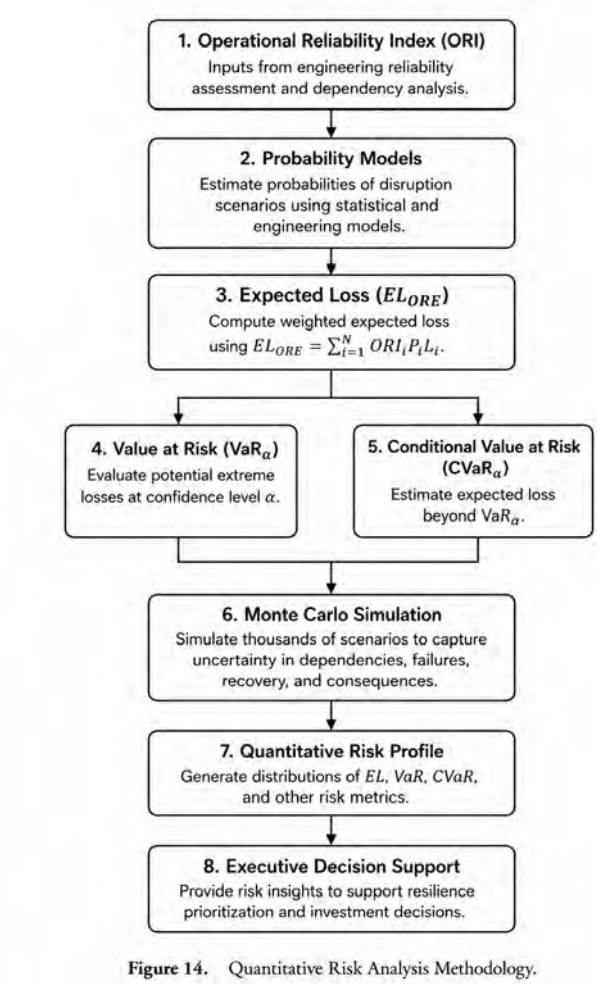

Figure 14. Quantitative Risk Analysis Methodology.

Fig. 14. Quantitative Risk Analysis methodology integrating the Operational Reliability Index (ORI), Expected Loss (EL_{ORE}), Value at Risk (VaR_α), Conditional Value at Risk ($CVaR_\alpha$), Monte Carlo simulation, and executive decision support.

TABLE III
ILLUSTRATIVE QUANTITATIVE RISK ASSESSMENT RESULTS

Scenario	P_i	**Loss (USD M)**	**ORI**	EL_{ORE} **(USD M)**	**Priority**
PLC Failure	0.08	4.5	0.91	0.328	High
SCADA Failure	0.04	9.8	0.86	0.337	High
Power Outage	0.03	15.4	0.88	0.407	High
Communication Loss	0.06	2.7	0.79	0.128	Medium
Cloud Service Outage	0.05	6.1	0.53	0.162	Medium
Engineering WS	0.07	1.9	0.39	0.052	Low
Backup Server	0.05	1.2	0.17	0.010	Low

Table III presents an illustrative application of the proposed quantitative risk methodology and demonstrates how engineering reliability, operational dependency, and probabilistic risk metrics collectively support resilience investment prioritization.

Table III illustrates the application of the proposed Operational Resilience Engineering methodology to a representative set of disruption scenarios. Unlike conventional Expected Loss calculations, the proposed weighted formulation incorporates the Operational Reliability Index (ORI), thereby accounting for both engineering reliability and operational criticality. Consequently, disruption scenarios affecting mission-essential assets receive greater analytical importance, allowing engineering organizations to prioritize resilience investments according to their operational consequences rather than solely their occurrence probabilities.

E. Resilience Optimization

> *"Operational resilience is ultimately strengthened not by eliminating every possible risk, but by allocating limited engineering resources where they produce the greatest reduction in operational consequences."*

The previous subsections established a quantitative methodology for characterizing operational dependencies, evaluating engineering reliability, and estimating operational risk using Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and the Operational Reliability Index (ORI). While these metrics provide valuable situational awareness, they do not directly indicate how engineering resources should be allocated to maximize operational resilience. Consequently, the final stage of the proposed Operational Resilience Engineering (ORE) methodology focuses on resilience optimization.

Engineering organizations routinely operate under constraints including limited financial resources, maintenance personnel, scheduled outage windows, and competing operational priorities. Therefore, resilience improvement should be formulated as an optimization problem in which available resources are allocated to projects that maximize the reduction of operational risk while preserving mission-essential capabilities.

Within the proposed ORE framework, resilience optimization seeks to maximize the operational benefit obtained from each engineering investment. To support this objective, this paper introduces the **Return on Resilience Investment (RORI)**, defined as

$$RORI = \frac{EL_{before} - EL_{after}}{I}, \tag{23}$$

where

- EL_{before} represents the Expected Loss before implementing the resilience improvement,
- EL_{after} represents the Expected Loss after implementation,
- I denotes the total engineering investment associated with the proposed resilience initiative.

The Return on Resilience Investment represents the expected operational loss reduction obtained per unit of investment. Larger RORI values indicate that a proposed engineering initiative produces greater operational benefit relative to its implementation cost and should therefore receive higher priority during resilience planning.

Unlike traditional financial return-on-investment metrics, RORI quantifies value in terms of operational consequence reduction rather than direct revenue generation. Consequently, resilience investments that significantly reduce mission disruption, safety risk, environmental impact, or business interruption may demonstrate substantial organizational value even when their direct financial return is not immediately observable.

Engineering optimization within the ORE framework may therefore be formulated as

$$\max \sum_{i=1}^{N} RORI_i x_i, \tag{24}$$

subject to

$$\sum_{i=1}^{N} C_i x_i \leq B, \tag{25}$$

where

- x_i is a binary decision variable indicating whether resilience project i is selected,
- C_i denotes the implementation cost of project i,
- B represents the available resilience investment budget.

This optimization formulation enables engineering organizations to identify the combination of resilience initiatives that maximizes operational benefit while satisfying budgetary constraints. Candidate investments may include equipment modernization, network segmentation, redundancy implementation, predictive maintenance, Digital Twin deployment, workforce training, supplier diversification, backup power systems, or enhanced monitoring capabilities.

Figure 15 illustrates the proposed Resilience Optimization methodology. Beginning with the quantitative risk assessment developed in the previous subsection, candidate resilience initiatives are evaluated according to their influence on engineering reliability, operational dependencies, and Expected Loss reduction. The resulting Return on Resilience Investment values provide an objective basis for prioritizing engineering projects and supporting executive capital allocation decisions.

Table **??** presents an illustrative resilience investment portfolio demonstrating how engineering initiatives may be ranked according to their expected operational benefit and associated investment requirements.

The proposed optimization methodology transforms Operational Resilience Engineering from a descriptive assessment framework into a prescriptive engineering decision-support methodology. Rather than simply identifying vulnerabilities, the framework quantitatively recommends where organizations should invest limited engineering resources to maximize sustained operational capability and long-term organizational resilience.

F. Executive Decision Support

> *"Engineering analysis creates knowledge; executive decision support transforms that knowledge into strategic action."*

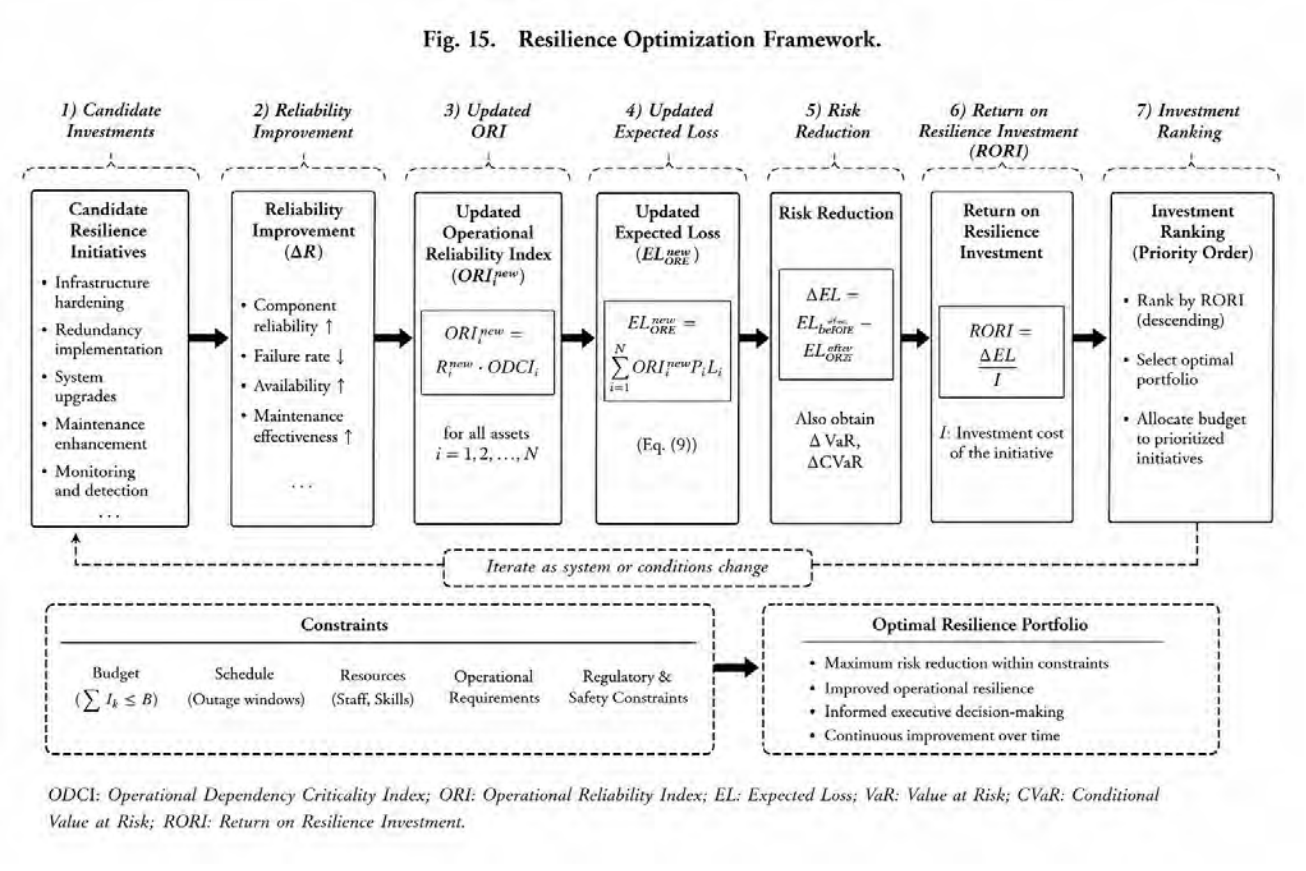

Fig. 15. Resilience Optimization Framework illustrating how candidate resilience initiatives are evaluated through reliability improvement, updated Operational Reliability Index (ORI), Expected Loss reduction, Return on Resilience Investment (RORI), and investment ranking under operational and budgetary constraints.

The ultimate objective of Operational Resilience Engineering (ORE) is not merely to quantify operational risk but to provide executives with objective, data-driven information that supports strategic decision-making under uncertainty. The methodologies presented throughout this paper—including operational dependency analysis, engineering reliability assessment, quantitative risk modeling, and resilience optimization—collectively generate a comprehensive understanding of the operational resilience posture of a critical infrastructure system.

Traditional cybersecurity reporting frequently emphasizes technical vulnerabilities, threat intelligence, or compliance status. Although these indicators remain important, executive leadership is primarily concerned with organizational resilience, operational continuity, financial exposure, investment prioritization, and mission assurance. Consequently, technical engineering results must be translated into decision-oriented performance indicators that support capital allocation and long-term operational planning.

Within the proposed ORE framework, executive decision support integrates the principal engineering metrics developed throughout the assessment process, including the Operational Dependency Criticality Index (ODCI), Operational Reliability Index (ORI), Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and Return on Resilience Investment (RORI). Collectively, these metrics provide a quantitative representation of the organization's operational resilience and enable engineering decisions to be evaluated according to their expected operational impact.

Figure 16 illustrates the Executive Decision Support methodology. Engineering measurements obtained from the previous analytical stages are consolidated into an executive resilience dashboard that provides decision-makers with a prioritized view of critical assets, projected operational losses, resilience investment opportunities, and overall organizational resilience.

Table IV presents an illustrative executive resilience dashboard summarizing the key quantitative indicators generated by the proposed ORE methodology. The dashboard supports resilience monitoring, investment prioritization, and executive decision-making.

By integrating engineering analysis with executive decision-making, the proposed Operational Resilience Engineering (ORE) framework extends beyond conventional cybersecurity assessments to provide quantitative support for protecting mission-essential operations. The resulting methodology enables organizations to continuously monitor resilience, prioritize engineering investments, and strengthen long-term opera-

TABLE IV
EXECUTIVE OPERATIONAL RESILIENCE ASSESSMENT SUMMARY

Metric	Value	Status	Action
ODCI	0.91	High	Protect Assets
ORI	0.87	High	Monitor
EL_{ORE} (USD M)	4.8	Moderate	Reduce Risk
$VaR_{95\%}$ (USD M)	12.5	High	Mitigate
$CVaR_{95\%}$ (USD M)	17.3	High	Increase Resilience
RORI	8.6	Excellent	Prioritize
ORE Score	0.82	Good	Maintain

tional sustainability across complex cyber-physical systems.

VI. DISCUSSION

This section discusses the significance of the proposed Operational Resilience Engineering (ORE) framework, positions it relative to existing cybersecurity and resilience methodologies, highlights its principal engineering contributions, examines potential industrial applications, identifies current research limitations, and outlines future research directions. Collectively, these discussions demonstrate how ORE extends traditional cybersecurity by integrating engineering reliability, operational dependency analysis, quantitative risk assessment, resilience optimization, and executive decision support into a unified engineering discipline.

A. Comparison with Existing Frameworks

> *"Operational Resilience Engineering complements existing cybersecurity and resilience frameworks by integrating engineering reliability, operational dependency analysis, quantitative risk modeling, and executive decision support into a unified methodology for sustaining mission-essential operations."*

The increasing complexity of modern critical infrastructure has motivated the development of numerous cybersecurity, risk management, and operational resilience frameworks. Standards and guidelines such as the NIST Cybersecurity Framework (CSF), ISA/IEC 62443, ISO 31000, ISO 22301, and the Purdue Enterprise Reference Architecture have significantly improved the protection and governance of industrial systems by establishing best practices for cybersecurity, risk management, business continuity, and industrial network architecture.

Each of these frameworks addresses an essential aspect of organizational resilience. The NIST Cybersecurity Framework provides a comprehensive structure for identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. ISA/IEC 62443 establishes cybersecurity requirements for industrial automation and control systems throughout their lifecycle. ISO 31000 provides internationally recognized principles for enterprise risk management, while ISO 22301 focuses on business continuity management systems and organizational recovery capabilities. Likewise, the Purdue Enterprise Reference Architecture remains one of the most widely adopted models for segmenting industrial operational technology networks.

Although these frameworks provide substantial guidance for cybersecurity governance, compliance, and operational management, their primary objective is not the quantitative engineering evaluation of sustained operational capability under cyber-physical disruption. Existing standards generally address cybersecurity controls, governance processes, network segmentation, business continuity planning, or organizational risk management independently. The proposed Operational Resilience Engineering (ORE) methodology instead integrates these disciplines within a single quantitative engineering framework.

Unlike traditional cybersecurity methodologies that primarily seek to reduce the probability of cyber compromise, ORE focuses on quantifying the operational consequences of disruption and optimizing the capability of organizations to sustain mission-essential services. This objective is achieved by combining Reference Critical Infrastructure Architecture (RCIA), operational dependency analysis, engineering reliability modeling, probabilistic risk assessment, resilience optimization, and executive decision support into a unified analytical methodology.

Another distinguishing characteristic of ORE is the introduction of original engineering metrics specifically designed to quantify operational resilience. The Operational Dependency Criticality Index (ODCI) evaluates the operational importance of assets based upon their dependency relationships, while the Operational Reliability Index (ORI) integrates engineering reliability with operational criticality to prioritize resilience initiatives. Similarly, the proposed Return on Resilience Investment (RORI) provides executives with a quantitative measure for evaluating the operational benefit obtained from resilience investments. These metrics collectively extend traditional cybersecurity assessments toward engineering-based optimization of operational performance.

Table V summarizes the principal characteristics of representative cybersecurity and resilience frameworks and compares them with the proposed Operational Resilience Engineering methodology. Rather than replacing existing standards, ORE should be viewed as a complementary engineering framework that leverages established cybersecurity and governance practices while introducing quantitative engineering models capable of supporting operational decision-making, resilience optimization, and long-term infrastructure sustainability.

Consequently, Operational Resilience Engineering provides a systematic bridge between cybersecurity, systems engineering, engineering reliability, quantitative risk management, and executive decision support. This multidisciplinary integration constitutes one of the principal contributions of the proposed framework and differentiates ORE from existing cybersecurity and business continuity methodologies.

B. Engineering Contributions

> *"Operational Resilience Engineering extends conventional cybersecurity by integrating systems engineering, engineering reliability, quantitative risk analysis, and executive decision-making into a unified methodology for sustaining mission-essential operations."*

The proposed Operational Resilience Engineering (ORE) framework contributes a multidisciplinary methodology that

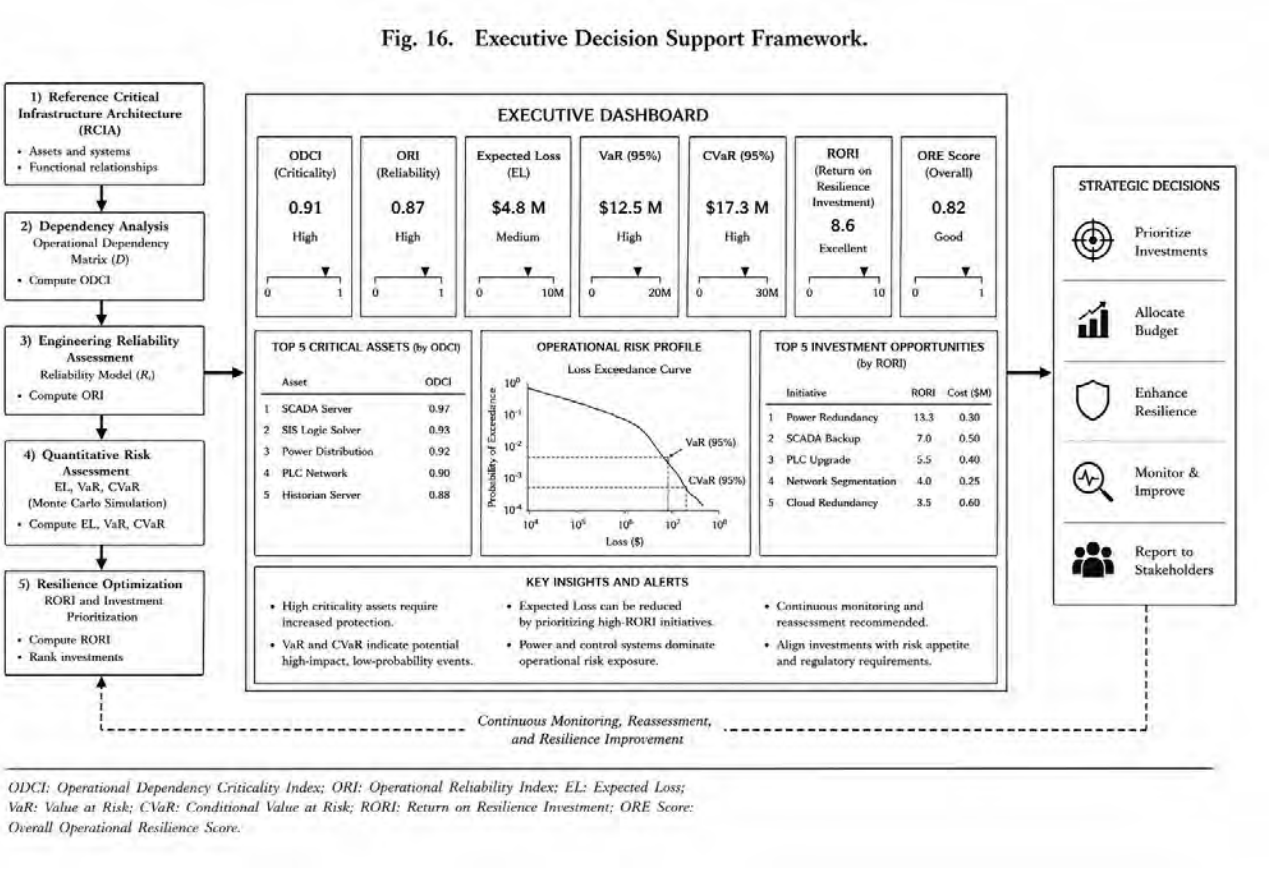

Fig. 16. Executive Decision Support framework integrating the outputs of the Operational Resilience Engineering (ORE) methodology into an executive dashboard for resilience monitoring, risk-informed decision-making, and strategic investment prioritization.

TABLE V
COMPARISON OF OPERATIONAL RESILIENCE ENGINEERING (ORE) WITH REPRESENTATIVE CYBERSECURITY AND RESILIENCE FRAMEWORKS

Capability	**Purdue**	**NIST CSF**	**ISA/IEC 62443**	**ISO 31000**	**ISO 22301**	**ORE**
Primary Objective	Architecture	Cybersecurity	ICS Security	Risk	Business Continuity	Operational Resilience
Industrial Architecture	Yes	Partial	Partial	No	No	Yes
Cybersecurity Governance	No	Yes	Yes	Partial	Partial	Yes
Industrial Control System Security	Partial	Partial	Yes	No	No	Yes
Operational Dependency Modeling	No	No	No	No	No	Yes
Engineering Reliability Assessment	No	No	Partial	No	No	Yes
Business Continuity	No	Partial	Partial	Partial	Yes	Yes
Quantitative Risk Assessment	No	Partial	Partial	Yes	Partial	Yes
Expected Loss (EL)	No	No	No	Partial	No	Yes
Value at Risk (VaR)	No	No	No	Partial	No	Yes
Conditional Value at Risk (CVaR)	No	No	No	Partial	No	Yes
Monte Carlo Simulation	No	No	No	No	No	Yes
Resilience Optimization	No	No	No	No	No	Yes
Executive Decision Support	No	No	No	Partial	Partial	Yes
Operational Dependency Criticality Index (ODCI)	No	No	No	No	No	Yes
Operational Reliability Index (ORI)	No	No	No	No	No	Yes
Return on Resilience Investment (RORI)	No	No	No	No	No	Yes
Unified Engineering Methodology	No	No	No	No	No	Yes

integrates established cybersecurity principles with systems engineering, engineering reliability, quantitative risk management, and operational decision support. Rather than introducing isolated analytical techniques, the framework combines complementary engineering disciplines into a coherent methodology for evaluating, quantifying, and optimizing the

resilience of critical infrastructure systems operating within increasingly complex cyber-physical environments.

The principal engineering contributions of this work may be summarized as follows.

1) **Operational Resilience Engineering (ORE).** The paper establishes Operational Resilience Engineering as a quantitative engineering methodology for evaluating the capability of critical infrastructure systems to sustain mission-essential operations under cyber, physical, environmental, and operational disruptions.
2) **Reference Critical Infrastructure Architecture (RCIA).** The proposed RCIA provides a structured reference architecture for identifying operational assets, engineering functions, external dependencies, and organizational interfaces required for comprehensive resilience assessment.
3) **Operational Dependency Modeling.** The paper introduces a quantitative representation of operational dependencies through the Operational Dependency Matrix, enabling critical infrastructure assets to be analyzed according to their functional interdependencies and potential disruption propagation paths.
4) **Operational Dependency Criticality Index (ODCI).** The proposed ODCI provides a normalized engineering metric for quantifying the operational importance of assets according to their dependency relationships within complex cyber-physical systems.
5) **Operational Reliability Index (ORI).** The Operational Reliability Index integrates engineering reliability with operational dependency criticality to prioritize mission-essential assets according to both their reliability and their operational significance.
6) **Quantitative Operational Risk Assessment.** The framework integrates Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), and Monte Carlo simulation to provide probabilistic estimates of operational disruption and support engineering-based resilience assessment.
7) **Return on Resilience Investment (RORI).** The proposed RORI metric enables resilience initiatives to be evaluated according to their expected reduction in operational consequences relative to implementation cost, thereby supporting engineering optimization and executive investment prioritization.
8) **Integrated Executive Decision Support.** The proposed methodology combines architecture modeling, operational dependency analysis, engineering reliability, probabilistic risk assessment, and resilience optimization into a decision-support framework capable of informing strategic planning, capital allocation, and long-term resilience improvement.

Collectively, these contributions establish Operational Resilience Engineering as a unified quantitative methodology that bridges cybersecurity, systems engineering, engineering reliability, quantitative risk management, and executive decision support. Rather than treating these disciplines independently, the proposed framework integrates them within a common engineering structure for the continuous evaluation and optimization of operational resilience across critical infrastructure systems.

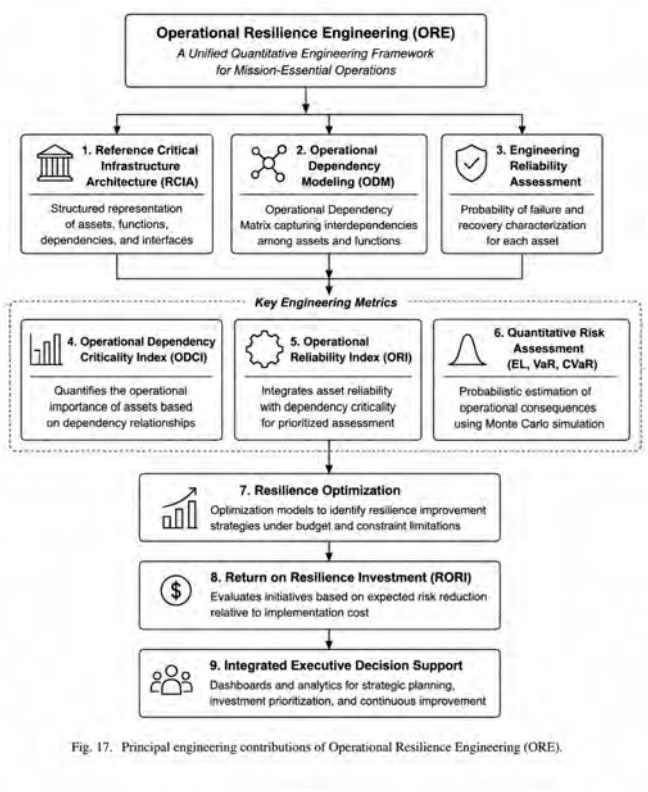

Fig. 17. Principal engineering contributions of Operational Resilience Engineering (ORE).

Fig. 17. Principal engineering contributions of the proposed Operational Resilience Engineering (ORE) framework. The methodology integrates the Reference Critical Infrastructure Architecture (RCIA), Operational Dependency Modeling (ODM), Engineering Reliability Assessment, Operational Dependency Criticality Index (ODCI), Operational Reliability Index (ORI), Quantitative Risk Assessment, Resilience Optimization, Return on Resilience Investment (RORI), and Executive Decision Support into a unified quantitative engineering methodology.

C. Industrial Applications

> *"Operational resilience is a multidisciplinary engineering challenge that transcends industrial sectors. Although operational processes differ across industries, the fundamental engineering principles governing dependency, reliability, risk, and resilience remain remarkably consistent."*

The proposed Operational Resilience Engineering (ORE) methodology is intended to provide a general quantitative framework applicable to a broad range of critical infrastructure sectors. Although the physical processes, operational technologies, regulatory requirements, and business objectives vary among industries, all critical infrastructure systems share common engineering characteristics, including operational dependencies, mission-essential assets, engineering reliability requirements, uncertainty, and resource constraints. Consequently, the mathematical foundations developed throughout

this paper may be adapted to support resilience assessment across numerous industrial domains.

Within electric power systems, ORE may support transmission and distribution networks, substations, renewable energy integration, generation facilities, and smart grid modernization by identifying critical operational dependencies, evaluating equipment reliability, quantifying operational consequences, and prioritizing resilience investments.

Within oil, gas, and petrochemical operations, the proposed methodology may assist in evaluating upstream production facilities, pipelines, refineries, liquefied natural gas (LNG) plants, offshore platforms, and process control environments by integrating operational dependency analysis with engineering reliability and quantitative operational risk assessment.

Manufacturing represents another significant application area. Modern industrial facilities increasingly rely upon Industrial Internet of Things (IIoT) technologies, robotics, advanced process control, Digital Twins, artificial intelligence, and predictive maintenance. ORE provides a quantitative engineering methodology for evaluating how disruptions propagate throughout interconnected manufacturing environments while supporting investment decisions that improve production continuity and operational resilience.

Food processing and agricultural operations similarly depend upon highly integrated cyber-physical infrastructures involving automation systems, refrigeration equipment, logistics networks, quality assurance processes, and supply-chain coordination. Consequently, operational dependency modeling and engineering reliability assessment may assist organizations in reducing production interruptions, minimizing food safety risks, and improving enterprise resilience.

Additional application domains include water and wastewater treatment facilities, transportation systems, mining operations, chemical processing plants, pharmaceutical manufacturing, healthcare infrastructure, telecommunications networks, and smart city environments. Despite substantial differences in operational objectives, each of these sectors requires continuous operation, reliable engineering assets, coordinated decision-making, and effective management of operational uncertainty.

Beyond terrestrial infrastructure, the proposed methodology is also applicable to aerospace systems, including mission control facilities, launch operations, satellite ground systems, and space manufacturing environments. Such systems exhibit complex operational dependencies and stringent reliability requirements, making them particularly suitable candidates for quantitative operational resilience assessment.

Figure 18 summarizes representative industrial application domains for Operational Resilience Engineering. The illustrated sectors demonstrate the versatility of the proposed framework and emphasize that ORE should be viewed as a cross-disciplinary engineering methodology rather than a sector-specific cybersecurity solution.

Collectively, these application domains demonstrate that the fundamental concepts introduced throughout this paper—including Reference Critical Infrastructure Architecture (RCIA), Operational Dependency Modeling, the Operational Dependency Criticality Index (ODCI), the Operational Reliability Index (ORI), quantitative operational risk assessment, resilience optimization, and executive decision support—provide a common engineering foundation for improving operational resilience across diverse critical infrastructure sectors.

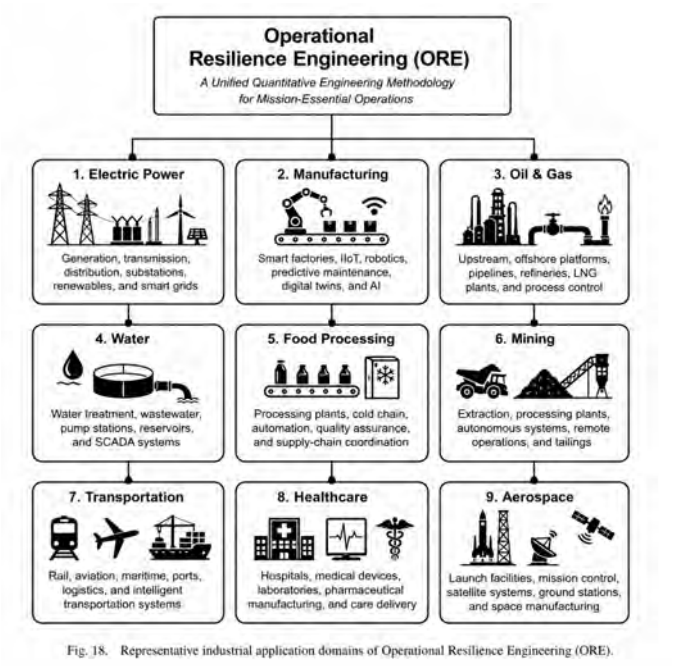

Fig. 18. Representative industrial application domains of the proposed Operational Resilience Engineering (ORE) methodology.

D. Research Limitations

> *"Engineering models provide decision support rather than absolute certainty. Their effectiveness depends upon the quality of available data, the validity of underlying assumptions, and their continuous adaptation to evolving operational environments."*

Although the proposed Operational Resilience Engineering (ORE) framework provides a comprehensive methodology for integrating cybersecurity, engineering reliability, operational dependency analysis, quantitative risk assessment, and executive decision-making, several limitations should be recognized.

First, the proposed metrics, including the Operational Dependency Criticality Index (ODCI), Operational Reliability Index (ORI), and Return on Resilience Investment (RORI), require calibration using operational, engineering, and organizational data that may vary across industrial sectors. Consequently, the weighting factors and evaluation criteria should be adapted to the operational characteristics and risk tolerance of each organization.

Second, the proposed dependency and reliability models assume that operational relationships can be adequately represented through quantitative engineering parameters. In practice, industrial systems evolve continuously as equipment, architectures, operational procedures, and external dependencies

change over time. Periodic reassessment is therefore necessary to ensure that the Reference Critical Infrastructure Architecture (RCIA) and associated dependency models accurately reflect the current operational environment.

Finally, the framework presented in this paper establishes the theoretical and methodological foundations of Operational Resilience Engineering. Although the proposed methodology is grounded in established principles of systems engineering, engineering reliability, and quantitative risk management, additional validation through real-world industrial case studies will further strengthen its applicability across diverse critical infrastructure sectors.

These limitations do not diminish the value of the proposed framework; rather, they identify opportunities for refinement, sector-specific calibration, and continued advancement of Operational Resilience Engineering as an emerging engineering discipline.

E. Future Research

> *"Operational Resilience Engineering should be viewed as an evolving engineering discipline whose capabilities will expand through advances in artificial intelligence, Digital Twins, autonomous systems, and data-driven decision support."*

The methodology presented in this paper establishes the foundational principles of Operational Resilience Engineering (ORE); however, numerous opportunities exist for further research and industrial development. As critical infrastructure continues to evolve toward increasingly interconnected and autonomous cyber-physical systems, resilience assessment will require models capable of continuously adapting to dynamic operational environments.

Future research should investigate the integration of ORE with Digital Twins to enable real-time resilience assessment, continuous operational monitoring, and predictive evaluation of engineering assets. Such integration would provide decision makers with dynamic visibility into operational dependencies, engineering reliability, and evolving risk conditions.

Artificial Intelligence and machine learning likewise present significant opportunities for enhancing the proposed framework. Data-driven models may support automated calibration of the Operational Dependency Criticality Index (ODCI), Operational Reliability Index (ORI), and Return on Resilience Investment (RORI), while advanced optimization techniques may recommend resilience strategies under changing operational conditions.

Another promising direction involves the application of graph theory and network science to represent complex operational dependencies within large-scale critical infrastructure systems. Graph-based models may improve the identification of critical assets, cascading failure paths, and resilience optimization opportunities across interconnected industrial environments.

Collectively, these research directions demonstrate that Operational Resilience Engineering extends beyond a single analytical methodology and provides a foundation for future advances in quantitative resilience assessment, engineering optimization, and executive decision support for critical infrastructure.

VII. Conclusions

> *"The resilience of critical infrastructure is no longer solely a cybersecurity challenge; it is fundamentally an engineering problem requiring quantitative methodologies capable of measuring, optimizing, and sustaining mission-essential operations under continuously evolving cyber-physical conditions."*

This paper introduced Operational Resilience Engineering (ORE), a multidisciplinary engineering methodology that integrates systems engineering, cybersecurity, engineering reliability, quantitative risk management, and executive decision support into a unified framework for evaluating and improving the resilience of critical infrastructure. Unlike conventional approaches that primarily emphasize compliance or cybersecurity controls, the proposed methodology focuses on sustaining mission-essential operations through quantitative engineering analysis and resilience optimization.

The proposed framework introduced several complementary contributions, including the Reference Critical Infrastructure Architecture (RCIA), Operational Dependency Modeling, the Operational Dependency Criticality Index (ODCI), the Operational Reliability Index (ORI), quantitative operational risk assessment using Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), Monte Carlo simulation, and the Return on Resilience Investment (RORI). Collectively, these components establish an integrated methodology capable of supporting engineering analysis, resilience optimization, and strategic decision-making across complex cyber-physical environments.

The discussion demonstrated that the proposed methodology complements established cybersecurity, risk management, and business continuity frameworks while extending their capabilities through engineering-based dependency analysis, reliability assessment, and quantitative operational decision support. Furthermore, the framework was shown to be applicable across multiple critical infrastructure sectors, including electric power, manufacturing, oil and gas, food processing, healthcare, transportation, water systems, mining, and aerospace, illustrating its versatility as a general engineering methodology rather than a sector-specific solution.

As critical infrastructure becomes increasingly interconnected, autonomous, and data-driven, engineering decisions will require more than qualitative assessments of cyber risk. Future resilience strategies must incorporate quantitative models that continuously evaluate operational dependencies, engineering reliability, probabilistic risk, and investment priorities. The proposed Operational Resilience Engineering framework provides a foundation for achieving this objective while supporting the development of more resilient, adaptive, and sustainable industrial systems.

Ultimately, this work argues that operational resilience should be regarded as a measurable engineering property rather than an abstract organizational objective. By integrating engineering analysis with executive decision-making,

Operational Resilience Engineering establishes a systematic foundation for protecting critical infrastructure and sustaining mission-essential operations within an increasingly uncertain cyber-physical environment.

References

[1] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. Aldershot, U.K.: Ashgate, 2006.

[2] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, *Resilience Engineering in Practice*. Farnham, U.K.: Ashgate, 2011.

[3] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA, USA: MIT Press, 2011.

[4] INCOSE, *Systems Engineering Handbook*, 5th ed. Hoboken, NJ, USA: Wiley, 2023.

[5] P. D. T. O'Connor and A. Kleyner, *Practical Reliability Engineering*, 5th ed. Hoboken, NJ, USA: Wiley, 2012.

[6] M. Rausand and A. Høyland, *System Reliability Theory*, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.

[7] E. Zio, *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. London, U.K.: Springer, 2013.

[8] ISO, *ISO 31000:2018 Risk Management—Guidelines*, Geneva, Switzerland, 2018.

[9] R. T. Rockafellar and S. Uryasev, "Optimization of Conditional Value-at-Risk," *Journal of Risk*, vol. 2, no. 3, pp. 21–42, 2000.

[10] P. Jorion, *Value at Risk*, 4th ed. New York, NY, USA: McGraw-Hill, 2007.

[11] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 2.0, Gaithersburg, MD, USA, 2024.

[12] International Society of Automation, *ANSI/ISA-62443 Series of Standards*, Research Triangle Park, NC, USA, 2023.

[13] International Electrotechnical Commission, *IEC 62443 Industrial Communication Networks – Network and System Security*, Geneva, Switzerland, 2023.

[14] Cybersecurity and Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals*, Washington, DC, USA, 2023.

[15] Cybersecurity and Infrastructure Security Agency, *Cross-Sector Risk Management Agency Guide*, Washington, DC, USA, 2024.

[16] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, Washington, DC, USA, 2013.

[17] M. Grieves and J. Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," in *Transdisciplinary Perspectives on Complex Systems*, Springer, 2017.

[18] F. Tao and M. Zhang, *Digital Twin Driven Smart Manufacturing*. London, U.K.: Academic Press, 2019.

[19] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2021.

[20] M. E. J. Newman, *Networks*, 3rd ed. Oxford, U.K.: Oxford University Press, 2018.

[21] A.-L. Barabási, *Network Science*. Cambridge, U.K.: Cambridge University Press, 2016.

[22] ISO, *ISO 22301:2019 Security and Resilience – Business Continuity Management Systems*, Geneva, Switzerland, 2019.

[23] E. D. Knapp and J. T. Langill, *Industrial Network Security*, 3rd ed. Elsevier, 2015.

[24] S. M. Ross, *Introduction to Probability Models*, 12th ed. Academic Press, 2019.

[25] D. P. Bertsekas, *Dynamic Programming and Optimal Control*, 4th ed. Belmont, MA, USA: Athena Scientific, 2017.

[26] D. Bertsimas and J. N. Tsitsiklis, *Introduction to Linear Optimization*. Belmont, MA, USA: Athena Scientific, 1997.

[27] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.

[28] Center for Chemical Process Safety, *Guidelines for Risk Based Process Safety*. New York, NY, USA: AIChE, 2007.

[29] International Electrotechnical Commission, *IEC 61511 Functional Safety – Safety Instrumented Systems*, Geneva, Switzerland, 2024.

About the Author

Israel Reyes is an executive advisor, researcher, and executive educator specializing in operational resilience, industrial cybersecurity, Artificial Intelligence, Digital Twins, and quantitative risk management. He has been invited by the Massachusetts Institute of Technology (MIT) to deliver executive lectures on crisis management, business continuity, operational resilience, and enterprise risk for industry leaders and senior executives.

Throughout his career, Mr. Reyes has advised organizations across critical infrastructure sectors, including energy, manufacturing, food processing, transportation, mining, and industrial operations. His work integrates engineering, cybersecurity, quantitative risk analytics, and executive decision-making to strengthen operational resilience, protect enterprise value, and support sustainable business growth.

His research focuses on the application of Artificial Intelligence, Digital Twins, reliability engineering, Expected Loss (EL), Value at Risk (VaR), Conditional Value at Risk (CVaR), Monte Carlo simulation, and stochastic risk modeling to optimize operational performance, prioritize capital investments, and reduce enterprise risk.

Mr. Reyes is the inventor of a patent-pending methodology for quantifying and optimizing operational resilience within industrial control systems and critical infrastructure environments (U.S. Patent Pending No. 2-01029619). His work bridges academic research with executive practice, helping organizations make data-driven decisions on digital transformation, AI adoption, operational resilience, and long-term infrastructure investment.

Chuck Russell is a Business Continuity and Crisis Management professional supporting a major natural gas transmission pipeline company with operations across Canada, the United States, and Mexico. His work focuses on strengthening enterprise resilience through business impact analysis, continuity planning, recovery strategy development, crisis management, exercise facilitation, and preparedness for cyber, technology, operational, and severe weather disruptions.

Prior to his current role, Mr. Russell held business continuity, crisis management, and operational resilience positions with Texas Children's Hospital and BP, where he supported enterprise continuity programs, incident response, disaster recovery alignment, alternate worksite strategies, and organizational preparedness for large, mission-critical operations.

His experience spans critical infrastructure, healthcare, and the energy sector, providing a broad perspective on operational resilience and executive readiness.

Mr. Russell earned a Bachelor of Science in Mechanical Engineering from the Georgia Institute of Technology and an MBA from the University of Texas at Austin. He is a Certified Business Continuity Professional (CBCP) and a former Project Management Professional (PMP), combining engineering expertise, operational risk management, and strategic program leadership to enhance organizational resilience.

His professional interests include business continuity, crisis management, critical infrastructure resilience, operational risk, emergency preparedness, and executive decision support. Through his work and collaborative research, he contributes to the development of practical strategies that enable organizations to strengthen resilience, improve continuity capabilities, and respond effectively to an evolving risk landscape.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Russell, C, Reyes, I (2026). Title. (Report No. 2026-1046). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/TJ6KC

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY