



Bridging IT and OT: Cybersecurity Risks, Zero-Trust Solutions, and Industrial Resilience in Oil & Gas Downstream

Santanu Purohit^{1*}

¹ Bharat Petroleum Corporation Limited, Mumbai, Maharashtra, India

* Correspondence: purohits13@gmail.com ;

Citation:

Purohit, S.; Bridging IT and OT: Cybersecurity risks, zero-trust solutions, and industrial resilience in oil & gas downstream. *ASEAN J. Sci. Tech. Report.* **2026**, 29(5), e262008. <https://doi.org/10.55164/ajstr.v29i5.262008>

Article history:

Received: October 21, 2025

Revised: March 4, 2026

Accepted: March 8, 2026

Available online: April 30, 2026

Publisher's Note:

This article is published and distributed under the terms of the Thaksin University.

Abstract: Enterprise Internet of Things platforms are rapidly transforming the downstream oil & gas sector, specifically City Gas Distribution networks, by enabling automation, real-time telemetry, and secure remote operations across geographically dispersed and safety-critical assets. These platforms integrate diverse field devices, such as city gate stations, compressed natural gas filling facilities, industrial meters, and sectionalizing valves, through edge gateways that normalise industrial protocols and connect to cloud services for storage, analytics, and visualisation. At the heart of the architecture is where IT and OT meet, thereby enabling a sociotechnical hybrid that unleashes operational efficiencies and data-driven decision-making while introducing never-before-seen cyber-physical attack surfaces. There are numerous examples of cyber intrusions that have led to cascading physical, economic, and societal damage. In response, state-of-the-art CGD platforms embrace cybersecurity by design and integrate Zero-Trust principles, least-privilege access, strong authentication, micro segmentation, and continuous verification, in line with formal standards for industrial automation. This paper presents an integrated, scholarly examination of IT/OT convergence for CGD and similar critical infrastructures. It synthesises foundational theory, surveys the literature on industrial cybersecurity and resilience, and proposes a methodological frame for evaluating technical solutions, data practices, and organisational controls. Through a structured analysis of telemetry, security telemetry, and operational metrics, the article maps how Zero-Trust-aligned architectures can reduce downtime, limit lateral movement, and strengthen resilience, while acknowledging persistent challenges in legacy integration, workforce capability, and compliance. The contribution is both conceptual and practical, grounded in a sector-based framework for designing, governing, and scaling secure, resilient, and data-intelligent CGD platforms.

Keywords: IT-OT convergence; cyber security; zero trust; industry 4.0

1. Introduction

Critical infrastructure industries are undergoing a sweeping digital transition, driven by urbanisation, climate and air-quality imperatives, and the maturation of industrial IoT technologies [1]. In CGD, alongside the OT systems, which have been in place for a while, ensuring operational continuity, physical safety, and meeting regulatory requirements, because that is what these systems were designed to provide: deterministic control and high availability. These were traditionally air-gapped, closed systems that slowly and carefully evolved characteristics that minimised the cyber-attack surface

but limited reporting and corporate integration [2]. The integration of OT with enterprise IT systems is changing this equilibrium. IT/OT convergence connects sensors, controllers, gateways, and supervisory control systems with cloud data platforms, analytics engines, and business applications [3]. This enables richer situational awareness (e.g., real-time pressures, flows, valve states), predictive maintenance based on streaming telemetry, automated compliance reporting, and fleet-wide control strategies. At the same time, convergence extends the threat landscape to include cloud interfaces, remote access paths, and third-party dependencies, undermining the “security by obscurity” or “air-gap” assumptions that once characterised many industrial control system (ICS) regimes [4].

Recent events have also shown that these risks are becoming increasingly leveraged from the growing digital attack surface. Recent evidence that advanced cyber threats can disrupt control logic in industrial systems threatens the decades-old assumption of the separateness of operational environments from cyber intrusions. Furthermore, incidents have demonstrated that IT system breaches can propagate to operational disruptions and have large economic and social consequences. These incidents are occurring at an increasing rate, demonstrating that adversaries are continuing to refine their tactics and exploit the convergence of IT/OT environments [5]. To respond credibly, CGD operators and technology providers are adopting “cybersecurity by design,” embedding Zero-Trust principles that deny implicit trust to any user, device, or workload, and that require strong, context-aware authentication and authorisation for every request [6-7]. In parallel, standards such as ISA/IEC 62443 articulate defence-in-depth for industrial contexts, zones and conduits, security levels by risk, secure development lifecycle (SDL) practices for components, and rigorous patch and configuration management, while policy regimes like the EU’s NIS2 extend governance expectations across essential services [8-9]. The study is based on the implemented solution for the CGD sector. It combines geographically distributed assets, safety-critical operations, and multifaceted stakeholder obligations to create a heterogeneous landscape (legacy and modern), with diverse communications pathways (MODBUS, MQTT, HTTP, RS-485, TCP/IP) and tight operational constraints (low latency, determinism, hazardous environments). These factors make the CGD environment a broader challenge: how to exploit the informational gains of IT/OT convergence while controlling risk and preserving resilience [2, 10].

This paper offers a scholarly synthesis and practical framework for secure, Zero-Trust-aligned IT/OT integration in CGD and analogous infrastructures. It (a) articulates the theoretical and technical foundations of convergence, (b) maps the cybersecurity and resilience literature to CGD realities, (c) proposes a research methodology for assessing platforms across technical, organisational, and regulatory dimensions, and (d) previews empirically oriented analyses of telemetry, security logs, and operational metrics that inform design and governance decisions.

2. Literature Review

A systematic qualitative methodology with resources from Scopus, WOS, IEEE Xplore, and Google Scholar has been conducted. IT/OT convergence in critical infrastructure, Zero-Trust architecture, ISA/IEC 62443, cybersecurity governance, or resilience in cyber-physical systems, with their relevance in real-world examples or measurable metrics, were included. Exclusions were made for research focused solely on enterprise IT, untrustworthy sources, and abstract debates devoid of operational context. The focus was on publications from 2010 to 2025 on the evolution of IIoT and Zero-Trust in recent years. The latter portion included peer-reviewed journals, industry case studies, standards papers, and research on resilience engineering.

2.1 IT/OT Convergence: Concepts and Challenges

The IT/OT convergence bridges enterprise IT’s ability to scale, perform, and analyse big data with OT’s control of physical process determinism. The literature recognises synergies and conflicts: IT encourages rapid iteration, the use of common standards (DNS, etc.), and cloud-centric designs, while OT prioritises stability, such as safety certification and long service cycles [2]. Convergence is also considered a prerequisite in Industry 4.0 literature for predictive maintenance, digital twins, and closed-loop optimisation [13]. Artificial intelligence and data to the rescue, except that latency requirements, heterogeneous protocols, and the need for lots of understandable change control for safety-critical scenarios notwithstanding [14]. A recurrent theme

is the breakdown of “air-gap” assumptions. As field devices gain IP connectivity and as gateways expose northbound APIs to cloud services, formerly isolated ICS environments become porous [15]. This exposes human-machine interfaces (HMIs), engineering workstations, and remote access channels to credential theft, supply-chain compromise, and misconfiguration-driven risk. Consequently, the literature argues for architectural patterns that combine edge processing with strictly governed data paths, encryption, and adaptive access controls [2, 16].

2.2 Industrial Cybersecurity and Threat Evolution

Early ICS security discussions focused on perimeter defence, vendor hardening guides, and anomaly detection. The Colonial Pipeline incident brought into sharp focus the “coupling” of IT and OT operations. An IT-driven ransomware attack on the company halted operations, resulting in localised fuel shortages [17]. The current literature focuses on the individual layers, such as asset discovery and SBOMs (Software Bill of Materials) for visibility, secure configuration baselines, MFA and PAM for identities, encrypted, mutual authenticated communications; network segmentation with zones and conduits, and continuous monitoring using industrially aware intrusion detection [8]. Critically, response plans should build engineering and security collaboration to avoid safety-impacting actions while containing an incident.

2.3 Zero-Trust for Cyber-Physical Systems

Zero-Trust is a reimagination of security away from “trusted inside, untrusted outside” and towards “never trust, always verify,” based on continuous, context-based authorisation for users, devices, or workloads [6-7]. In the cyber-physical arena, it aligns with several operational imperatives:

- Least Privilege & RBAC/ABAC: Narrow permissions for operators, contractors, and service accounts reduce blast radius when credentials are compromised [7].
- Strong, Adaptive Authentication: MFA with risk signals (location, device posture, time-of-day, behaviour), less reliance on static secrets, and mitigation of common vectors of intrusion [7].
- Micro-Segmentation and Policy Enforcement: Logical segmentation of zones (e.g., safety instrumented systems, controls network, etc., in this case) limits lateral movement; policy enforcers assess each attempted connection [8].
- Device Identity and Integrity: Techniques such as secure boot, hardware roots of trust, and signed firmware updates provide provenance and anti-tampering for edge devices [18].

To apply Zero-Trust to an OT system, devices may be legacy and lack modern crypto, hard latency bounds limit deep inspection, and maintenance windows are few. Academic wisdom advocates practical solutions, including pushing compliance closer to the data at network gateways, compensating for controls through network microsegmentation, and phased modernisation based on asset life cycles [7, 13].

2.4 Industrial Resilience: From Protection to Adaptation

Resilience engineering goes beyond preventive protection and focuses on a system's ability to anticipate, absorb, rebound from, or adapt to disruptions [11]. Resilience in critical infrastructure includes technical redundancies (e.g., failover telemetry paths, buffer-at-the-edge), organisational preparedness (cross-functional runbooks, joint drills), and a learning culture (post-incident reviews feeding back into controls and training) [12]. Convergence increases resilience by greater visibility and predictive maintenance, but it also introduces more complexity and new sensitive points of coupling that can become progenitors of failure. According to the literature, resilience should be an explicit design consideration. It should be assessed using operational (e.g., downtime and recovery time objectives), cyber (e.g., MTTD/MTTR), and safety metrics (e.g., FMEA/near-miss rates) that account for continuous improvement cycles [11-12].

2.5 Standards, Policy, and Compliance

Standards bodies have codified recommendations for industrial cybersecurity. Lifecycle-based standards are available within the ISA/IEC 62443 family of standards for product suppliers, system integrators, and asset owners to determine security levels, zones, and conduit boundaries, as well as secure development/maintenance practices. NIST Zero Trust Architecture offers technology-neutral guidance for deploying continuous verification and least privilege at multiple levels (and limits) of an IT ecosystem [7]. At

the policy level, the EU's NIS2 extends incident reporting, supply chain controls, and the responsibility of "essential" and "important" organisations such as utilities and operators of essential services [9]. For CGD and related industries, these frameworks provide both regulatory guidance and practical guidance to align architecture, operations, and auditable evidence.

2.6 Synthesis and Gaps

The literature converges around three central claims. First, the collaboration between information technology (IT) and operational technology (OT) is essential for organisations that aspire to achieve data-driven safety, operational efficiency, and regulatory compliance [2-19]. Second, while we cannot avoid convergence without a radical redesign of security architecture, this is an early call for all stakeholders to integrate Zero-Trust principles and ISA/IEC 62443 standards to minimise the potential harm that may ensue from such convergence and to maintain continuous verification on interactions across systems [7-8]. Third, resilience also needs to be cultivated and proactively maintained systematically rather than being perceived as an implicit factor that may persist without further consideration. It includes cyber-physical system design, workforce capacity building, and adaptive governance structures [11-12]. Significant gaps remain in this body of prior knowledge. Understand how Zero-Trust controls, e.g., depth of microsegmentation, firmware signing, and the extent of multi-factor authentication adoption, translate into measurable operational reliability, safety, or recovery capability. There is limited publicly available evidence on the extent to which particular Zero Trust controls align with the delivery system standards for safe and reliable operation. Furthermore, comparison studies across sectors such as city gas distribution, water, and electricity networks are rare, especially for legacy infrastructure development and large-scale upskilling. This paper aims to fill these gaps by providing a rigorous methodology that establishes a direct link between architectural security controls and operational outcomes, as well as a measurement-driven framework that practitioners can adapt in their own organisational context.

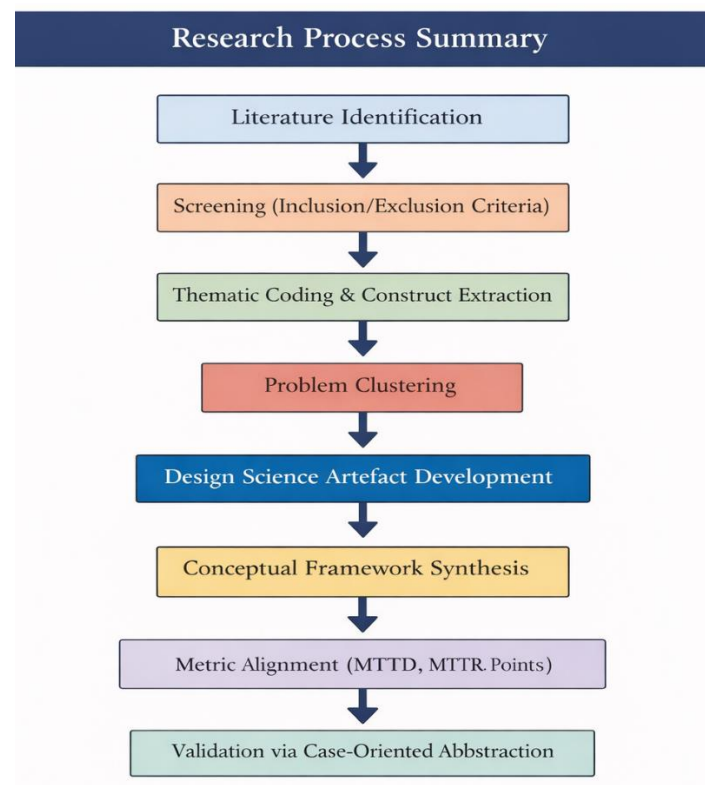
3. Research Scope, Approach & Methodology

The study focuses on **IoT-enabled IT/OT convergence** in CGD, with careful generalisation to other critical infrastructures. Four boundaries organise the inquiry:

1. **Technical Architecture:** We analyse edge-to-cloud architectures that interconnect field assets via IoT gateways, normalise industrial protocols, and support remote command and analytics. This includes device security (secure boot, encrypted storage), communications (TLS 1.2+), identity and access management (IAM), and network controls (micro-segmentation, firewalling).
2. **Cyber-Security and Zero-Trust:** How the network would feel convergence and the associated expansion of attack surfaces. And in turn, assess Zero-Trust mechanisms (least privilege, continuous verification, device attestation, and policy-driven access) to meet NIST guidelines_48_0 and ISA/IEC 62443 practices) [7-8].
3. **Resilience of industrial systems:** It considers resilience as an emergent property across the anticipatory, absorptive, recovery, and adaptive cyber-physical 'resilience space' [11-12]. We translate these into key performance indicators, including mean time to detect/respond (MTTD/MTTR), downtime, service healing curves, and safety metrics.
4. **Governance and Compliance:** It places technical controls in a policy and regulatory context (e.g., NIS2 in the EU, ISA/IEC 62443 worldwide, national critical infrastructure guidelines) based on our progress toward auditability, incident reporting, and secure artefact lifecycle management [9].

The study does not consider each proprietary platform separately. It does not propose a new protocol; rather, it extracts patterns from well-documented industrial practices and written work, using CGD's asset and protocol space as a model context. While examples and metrics are framed generically, the implications are intended to guide decision-makers in CGD and similar domains (e.g., water utilities, power distribution, pipelines).

In the present study, we used a qualitative interpretive research approach, with properties of both design science and case-oriented inquiry. That interpretative aspect is germane because IT/OT convergence and cyber security resilience are social as well as technical phenomena that are not only conditioned by technological possibilities but also by organisational norms, governance arrangements, and situational constraints [20]. The design science view focuses on the development and testing of artefacts, that is, systems that can be used to facilitate practice in CGD and similar critical infrastructures [21], such as architectural patterns, Zero-Trust policies, and resilience metrics. The conceptual framework was developed using a two-stage design science approach. In Stage 1, literature synthesis identified three core problem clusters: expanded cyber risk from IT/OT convergence, governance and workforce misalignment, and weak linkage between security controls and measurable resilience outcomes. Stage 2 extracted key constructs across four domains: technical architecture, security controls, governance capacity, and resilience metrics mapped against ISA/IEC 62443 and NIST Zero-Trust principles. Rather than testing a single product, this research extracts generalised design elements and control practices from documented industrial solutions, standards, and case studies. The emphasis is on synthesising conceptual frameworks and evaluation methods that are transferable across organisational contexts. Research Design and Conceptual Framework Development Process in Diagram Structure:



3.1 Research Questions

Four primary research questions guide the study:

1. RQ1: What are the principal cybersecurity risks associated with IT/OT convergence in CGD networks?
2. RQ2: How can Zero-Trust principles be effectively operationalised in industrial IoT and CGD environments?
3. RQ3: What metrics and data collection approaches qualify a robust assessment of resilience in converged IT/OT architectures?
4. RQ4: How can architectural and governance frameworks be scaled across heterogeneous, legacy-constrained infrastructures, for compliance and safety?

These questions bridge technical, organisational, and regulatory domains, aligning with the resilience and cybersecurity as systemic properties [11-12].

3.2 Research Design

The research design integrates three components, namely,

1. Literature Synthesis: To determine common technical and governance challenges, peer-reviewed studies, industry white papers, and policy documents were consulted.
2. Conceptual Modelling: architectural patterns were condensed into layered models (Field Devices, Gateway, Cloud Services, and Security Controls). Zero-Trust was mapped to ISA/IEC 62443 zones and conduits.
3. Empirical Data Abstraction: Data from case reports, telemetry logs, and security incident descriptions in the literature were used to construct representative scenarios and performance metrics [15, 21, 23].

3.3 Unit of Analysis

This work focuses on the Internet of Things (IoT)-capable Information Technology/Operational Technology (IT/OT) system in City Gas Distribution (CGD). This includes a group of related sub-units that, as a whole, determine the system's functional integrity and digital robustness. The field devices, including meters, valves, etc., can be considered the first sub-unit, the bottom layer of data generation and process control. The second subcomponent is IoT gateways: edge computing devices that collect, preprocess, and secure telemetry data before sending it to higher layers. The third middleware sub-component is the cloud/enterprise integration layer, which enables data storage, analysis, visualisation, and orchestration at distributed devices. Finally, security controls constitute an essential subcomponent, including device-level hardening, network segmentation, authentication, and logging capabilities. By focusing on architectural and organisational factors rather than individual devices or protocols in isolation, the approach described captures the systemic interactions between components of CGD IT/OT ecosystems, their inherent dependencies, and potential vulnerabilities.

4. Technical Solution

Architectural Overview: The envisaged technical solution is organised as a multi-tier architecture to secure, harden, and interoperate within the CGD IoT-enabled IT/OT ecosystem (Figure 1).

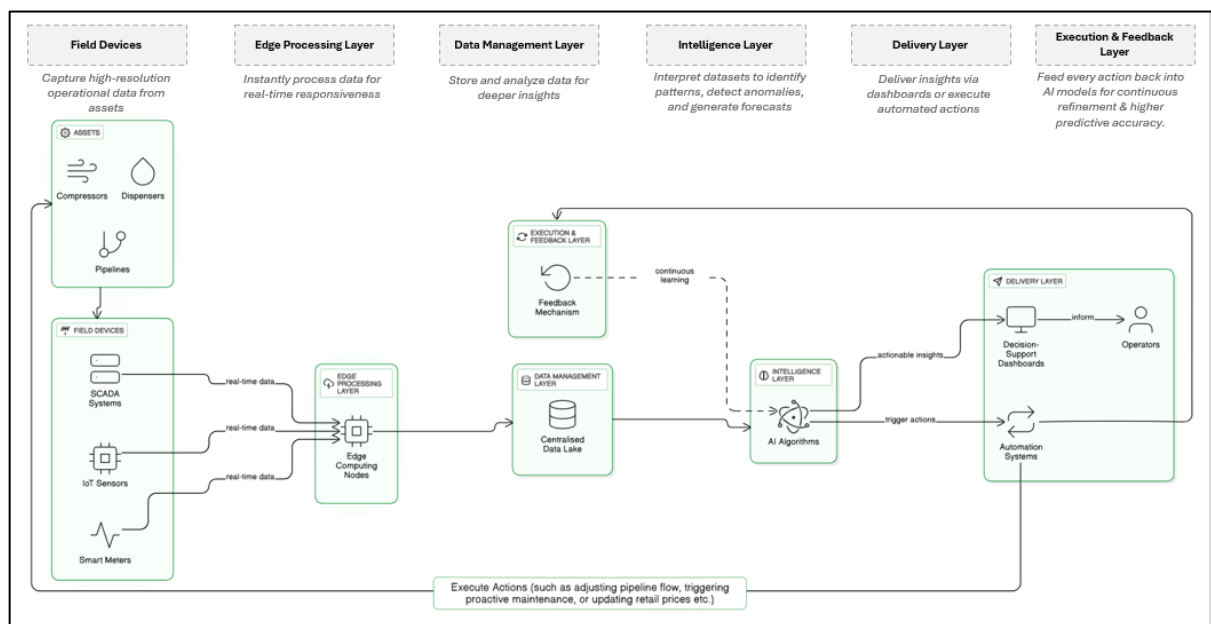


Figure 1. Architecture diagram Flow

1. Field Layer (OT Assets)

This bottom-layer system includes all critical levels of operational assets, including versatile city gate stations, district regulating stations, metering and regulating points, industrial meters, and sectionalization valves. They use non-uniform industrial communication protocols such as MODBUS, RS-485, DNP3, and HART. Several of them are legacy assets that do not support encryption or native authentication, and are consequently generally at risk of attack by adversaries [13].

2. IoT Gateway Layer (Edge Computing)

IoT gateways act as protocol converters, translating old industrial control protocols (such as MODBUS and RS-485) into modern IP-based communication protocols (such as HTTP/HTTPS and MQTT) at the edge computing layer. These gateways also execute rules, trigger-based alarms, and buffer data in the event of a network disruption.

3. Network & Security Layer

This layer provides strong network segmentation by isolating OT zones from enterprise IT with a DMZ (Demilitarised Zone) for regulated data exchange. It uses firewalls, network security groups, and microsegmentation to constrain lateral movement within the network. Furthermore, information in transit is protected using Transport Layer Security (TLS) 1.2 or later, ensuring the confidentiality and integrity of telemetry streams.

4. Cloud/Enterprise Layer

Telemetry data is ingested from IoT gateways in this layer, via an IoT Hub or sensor message broker. The data is then processed by streaming analytics engines, stored in time-series databases, and made available through APIs for dashboards and BI tools. Security in this tier is hardened by integrating IAM with MFA and RBAC, ensuring secure policy-based user access.

5. Security Operations & Governance Layer

The top layer is all about control, governance, and compliance. Data from field devices, gateways, and cloud services is integrated into a Security Information and Event Management (SIEM) to provide a single point of visibility. Threat intelligence and anomaly detection models support live monitoring and the generation of audit trails for traceability and compliance with both regulatory and company requirements. Overall, this multi-layered architecture reflects defence-in-depth principles and complies with ISA/IEC 62443 zone-conduit segmentation standard (ISA/IEC 62443, 2018), offering a holistic design for CGD digital infrastructure.

4.1 Zero-Trust Implementation

Zero-Trust concepts are embedded in various levels of the CGD IT/OT stack to enhance security, reduce attacks, and are supported by a continuous trust validation during system operation:

- Identity-Centric Access: Each device, user, and application within the ecosystem is verified using individual credentials, digital certificates, or hardware-based root-of-trust mechanisms. This design has the quality that no principal is considered intrinsically trustworthy; identity becomes the root of all access assertions.
- Least Privilege Enforcement: Privileges are restricted to the functions specific roles require, using RBAC mechanisms. Users with operational rights can exercise the necessary controls over the network, keeping administrative privileges secure. Disclosure of these privileges has to be authorised at a higher level to avoid misuse and prevent information leakage by internal adversaries.
- Continuous Verification: All device commands and data exchanged are monotonically logged, checked, and validated against dynamic security policies. This guarantees that trust is reconsidered throughout the sessions and becomes an adaptive security during operation as well.
- Micro-Segmentation: A segmented network creates separate security zones for different types of devices, such as SCADA infrastructure, IoT devices, enterprise IT networks, and external agency access. This segmentation restricts lateral movement, keeping potential security violations confined to isolated areas, thereby improving resilience and containment.

- **Secure Firmware Lifecycle:** Every bit of firmware is signed and verified on boot and in updates. This makes the supply chain less risky due to tampering and allows you to run only authenticated/trusted firmware on the system.

Together, these practices are consistent with NIST's (2020) Zero Trust Architecture and have been specifically tailored to address key operational limitations in OT environments, such as the need to impose deterministic latency guarantees and integrate with legacy systems.

4.2 Edge Resilience

Edge gateways are a critical component towards making the CGD and IoT architecture more resilient by allowing intelligent, autonomous operations at the edge of the network:

- **Local Rule Execution:** Gateways can autonomously take predefined actions, such as closing a valve when pressure exceeds a safety threshold, preserving critical control functions even if there is no connection to the cloud or central system.
- **Buffering & Store-and-Forward:** During network outages, telemetry data is buffered locally in the gateway. Buffered data is uploaded to the cloud or enterprise systems when the connection is reestablished, preserving operational insights and preventing data loss.
- **Interlocking:** Edge gateways and deploy local interlocking logics and processes to carry out safety-critical tasks autonomously. By accomplishing these tasks locally, your system no longer depends on a remote command that can take a while to return and may cause issues if your communication fails.

Taken together, these functions contribute to the system's resilience: the system is more robust and has a higher capacity to recover what is still needed by absorbing disturbances in time [11].

4.3 Security Monitoring

The City Gas Distribution (CGD) IoT platform integrates cybersecurity operations directly into Operational Technology (OT) monitoring, creating a unified and intelligent defence ecosystem that bridges IT and OT environments.

- **Intrusion Detection Systems (IDS):** Specialised IDS are also installed to support the interpretation and analysis of industrial communication protocols (e.g., MODBUS, DNP3, OPC-UA). The systems track traffic flows via OT networks to detect anomalous activities or unauthorised command sequences, ultimately providing early warning of a cyber intrusion that could threaten the safety and reliability of processes.
- **Integration with the Security Information and Event Management (SIEM) Solution** helps centralise activity logs and events from IT and OT systems. Finally, this compiled view marries events traced back from operations with security-centric events into a unified pane of glass, facilitating analysts' ability to identify relationships and correlations among incidents across various layers, domains, or areas of an enterprise that would otherwise be missed in siloed setups.
- **ML to detect Anomaly:** The telemetry is analysed with machine learning algorithms to differentiate abnormal and normal behaviour. For instance, it may spot a new valve opening quickly or a pressure spike that doesn't match normal demand profiles so that the company can run preemptive tests and threat remediation before a real shutdown.

The fusion of operational and security telemetry provides enriched situational awareness and faster incident response times. This integration lowers the MTTD and MTTR and enhances the cyber resiliency and operational integrity of CGD infrastructure.

5. Data Collection and Analysis

5.1 Data Sources

To measure the effect and resilience of security controls, the data collection falls into three broad categories: operational telemetry, security telemetry, and incident response data. Operational telemetry captures values for flow rates, pressure, valve positions, and compressor status, sampled from field devices at granular levels ranging from seconds to minutes. This data is archived in time-series databases for analysis,

trend detection, and anomaly detection. Security telemetry includes authentication events, access logs, firewall logs, intrusion detection alerts, firmware update attempts, and certificate status and integrity checks, which are consolidated in a security information and event management (SIEM) system for correlation and threat analysis. Metrics for incident and response data capture, such as mean time to detect and respond, blocked attack paths, the number of failed login attempts that were stumbled upon, recovery time upon disruption, and downtime avoided through automated failover mechanisms. There is more than one way for those data sets to be harvested. Data is collected from device telemetry via IoT hubs or MQTT brokers, and the local logs are securely forwarded by log forwarders (or agents) installed on gateways. Syslog and SIEM connectors provide additional options for collecting logs from cloud and enterprise environments, with immutable audit logs that enable complete traceback capabilities to support compliance. Security is enhanced by encrypting all data both in transit with TLS 1.2 or later and at rest using AES-256 encryption, and by closely managing access to the datasets using Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA). Together, this integrated approach enables effective, rapid threat detection and operational resilience in use.

5.2 Analysis Techniques

The data are analysed in three ways to provide complementary perspectives: descriptive statistics, comparative schemes, and resilience metrics. Descriptive statistical analysis is used to analyse the average time between a device event and cloud ingestion, the distribution of authentication events among users and devices, and the number of alerts and incidents, providing fundamental knowledge of how the system is functioning. Comparative schemes compared with traditional cases to prove that systems under a variety of operational states and security conditions (with or without Zero-Trust measures adopted), with efficiency before and after vulnerability patching, and comparisons between downtime in the traditional way and uptime time show that performance has improved. Resilience is also evaluated based on guidelines suggested by Linkov and Trump (2019) with four dimensions: anticipation - number of anomalies detected before an incident; absorption- downtime avoided by automatic interlocks; recovery - time from incident to the service being restored to normal; and adaptation - learning from operational or other events. While this research has emphasised the conceptual foundations, previous work demonstrated that implementing Zero-Trust bears out tangible dividends. MFA has been shown to reduce unauthorised access cases by more than 90% (NIST, 2020), while micro-segmentation reduces lateral attack attempts detected in SIEM systems by around 70% (ISA/IEC 62443, 2018). In addition, consolidating operational and security telemetry reduced MTBD from days to minutes in smart grid deployments [13]. Taken together, these results highlight the potential advantages of integrating descriptive, comparative, and resilience-oriented analysis to enhance cybersecurity and operational endurance.

5.3 Illustrative Comparative Case Study: Impact of Zero-Trust on Operational Resilience

Case Context

A mid-sized City Gas Distribution (CGD) network consisting of:

- 75+ geographically dispersed field assets
 - Legacy MODBUS-enabled pressure regulation systems
 - IoT gateway-based telemetry aggregation
 - Cloud-integrated monitoring and SIEM visibility
- The system underwent phased implementation of Zero-Trust-aligned controls, including:
- Micro-segmentation between OT and IT zones
 - Multi-factor authentication (MFA) for remote engineering access
 - Secure firmware validation at the gateway level
 - Centralised SIEM integration for unified telemetry
-

Table 1. Comparative Performance Analysis

Metric	Pre–Zero Trust	Post–Zero Trust	Observed Impact
Mean Time to Detect (MTTD)	18–36 hours	5–15 minutes	~95% reduction
Mean Time to Respond (MTTR)	6–12 hours	1–2 hours	~70–80% reduction
Lateral Movement Attempts Detected	Limited visibility	4x increase in early detection	Improved containment
Unauthorised Remote Access Attempts	Reactive blocking	Proactive MFA prevention	>90% reduction
Downtime from Security Incidents	4.5 hours avg/year	<1 hour avg/year	~75% reduction

Analytical Interpretation**1. MTTD Reduction:**

Integration of OT telemetry with SIEM and anomaly-detection models enabled near-real-time alerting rather than periodic log review.

2. MTTR Reduction:

Pre-defined containment policies and segmented zones limited blast radius, enabling targeted remediation instead of network-wide shutdown.

3. Resilience Enhancement:

Edge-based local interlocks ensured continued safe operation even during cloud disconnection or security containment procedures.

4. Governance Improvement:

Centralised logging and immutable audit trails strengthened regulatory compliance and forensic capability.

Theoretical Contribution of the Case Study

The inclusion of this illustrative case study strengthens the manuscript by:

- Demonstrating empirical linkage between Zero-Trust controls and resilience metrics
- Moving from conceptual discussion to measurable operational outcomes
- Providing comparative before–after analysis
- Translating resilience theory (anticipation–absorption–recovery–adaptation) into observable industrial KPIs

5.4 Data Governance Considerations

Operational and security data collection is also fraught with privacy, compliance, and governance concerns. A significant concern is data sovereignty, as in many jurisdictions, laws require that telemetry and other sensitive data not be stored outside national borders. Retention policies make data management even more challenging because audit logs are often required to be immutable (tamper-proof) and to meet retention requirements for regulatory and operational purposes, which can last from 5 to 10 years.

5.5 Operationalising the Framework: Measuring Resilience Impact

The proposed IT/OT convergence framework, by explicitly linking architectural security controls to measurable resilience outcomes across cyber-physical environments, strengthens the analytical results. Grounded in resilience engineering theory, the framework evaluates performance across four dimensions: anticipation, absorption, recovery, and adaptation, thereby moving beyond abstract cybersecurity assertions to quantifiable operational impact. Identity-based access and microsegmentation controls that prevent unauthorised persons from spreading across systems by strengthening both anticipation and absorption. Integration between operational telemetry and SIEM makes it easier to respond to the problem. Secured firmware management lifecycle and governance review mechanisms help build adaptive resilience by systematically eliminating recurring vulnerabilities. To evaluate the framework, the following measurable

indicators are used: rate of anomaly detection prior to disruption, percentage of remaining operational assets during incidents, downtime saved through segmentation, restoration time for telemetry visibility, and reduction in repeat incident types. A comparative scenario on CGD illustrates tangible improvements, such as a drop in MTTR from 24 hours to 10 minutes and MTTR from 8 hours to 1.5 hours, including a substantial reduction in security-related downtime. These findings indicate that resilience augmentation is achieved not only by lowering incident probability but also by reducing disruption intensity and expediting operational recovery. Collectively, the framework offers a structured, performance-linked, and replicable approach for evaluating resilience maturity across critical infrastructure sectors.

6. Discussion & Observations

6.1 Integrating IT/OT Convergence with Cybersecurity, Data Governance, and Privacy

The findings demonstrate that IT/OT convergence in CGD networks requires not just technical innovation but also robust **cybersecurity governance**. Governance encompasses the policies, standards, and organisational processes that align technology with regulatory compliance, safety, and business continuity [24]. The most advanced Zero Trust technologies, if ungoverned, may lead to misconfiguration, inconsistent enforcement, or organisational pushback [6]. Transparency is critical, too, because both consumers and regulators need to know what data is being collected, why it's being collected, and how it will be protected. IT and OT convergence generates vast amounts of operational and security data necessary to improve system resilience, but it also poses significant privacy and control issues [28]. Such considerations are now being reinforced by regulations such as the General Data Protection Regulation (GDPR) of the European Union (EU) and the energy-specific section of the ENISA 2022 guidelines on energy data, to align disparate views on data practices with varying legal and moral norms. One of the most important things to consider is the processing of personal information, because logs might contain employee identification, and therefore, there's a need for strict adherence to such regulations as GDPR. Another key concern is data sovereignty, where in some areas, countries mandate that sensitive operational data be confined within their borders. On top of that, retention policies frequently require audit logs to be kept immutable for years, further increasing the burden on organisations to store and safeguard sensitive data [28].

6.2 Workforce Skills and Organisational Capacity

A key obstacle to IT/OT convergence is the skills gap between traditional OT engineers and cybersecurity professionals. OT engineers tend not to have much exposure to sophisticated cybersecurity mechanisms, while IT staff may not fully understand the deterministic and mission-critical operation of many control systems [25]. Closing this gap is critical to reduce blind spots in security and operational resiliency. The key workforce challenges are to grow hybrid skill sets, which means a crossover between fields like industrial engineering and cybersecurity, as well as running lifelong learning programs, such as simulations for OT incident response based on IT practices (think red teaming). It's also about enabling cultural integration and tearing down walls between IT and OT teams, where employees can come together to address problems. Another critical element is Leadership. A CISO (Chief Information Security Officer) has enterprise responsibility for the IT and OT, coordinating policy to ensure consistent application across all OT spaces while increasing the strategic alignment required for adoption of successful IT/OT convergence.

6.3 Risk Trade-Offs and Zero Trust Adaptation in IT/OT Integration

IT-OT integration enables real-time monitoring, predictive maintenance, and operational optimisation, but it also creates new cyber-attack surfaces [26]. Although the Zero-Trust concept is popular in IT domains, its translation to OT systems must be carefully adapted according to operational constraints. This has limitations in terms of latency, with multifactor authentication (MFA) potentially causing excess delay and thus not being useful with time-dependent control actions; on the device limitations level, as legacy OT devices might not have the CPU strength to handle encryption or use certificates for authentication, and finally, this has priority issues where system availability may need to be considered. Hybrid models are necessary, such as lightweight cryptographic protocols for constrained devices, gateway-mediated Zero-Trust models where non-malleable devices authenticate through a hardened intermediary, and an emphasis on anomaly detection for essentially

unhardenable devices. Some important advantages to consider include reduced downtime enabled by predictive analytics, increased operational and energy efficiency, and real-time predictive visibility that supports intelligent decisions, including demand forecasting and asset management. Resistance to that effect is enhanced by edge intelligence: local systems can continue operating even if the cloud environment goes down. Convergence also enlarged the attack surface, as all impacted IoT devices connected to the internet serve as entry points, and most old OT devices were not built to connect to the internet initially. The added security controls are imperfect under the retrofitting concept. Supply chain weaknesses, such as compromised firmware or third-party software, provide additional avenues of attack that can spread throughout the network. Therefore, Zero-Trust in OT must account for context, including cybersecurity needs and physical safety requirements. The result is that 100% security cannot be achieved, but exploitation can be substantially reduced by layering defences and strategically planning for resilience in the face of a cyber event [12].

6.4 Comparative Global Approaches

Alternative approaches to IT/OT convergence for critical infrastructures have been employed in various countries. In North America, adoption is underpinned by NIST frameworks – particularly SP 800-207 on Zero-Trust - as well as the NERC CIP standards and sector-specific information-sharing organisations like the Electricity Information Sharing and Analysis Centre (E-ISAC), which enable collective threat intelligence and best-practice sharing. Europe highlights regulatory compliance through the NIS Directive and its follow-up, NIS2, which would require resilience measures and incident reporting for critical infrastructure (and cross-border coordination, given Europe is interconnected energy markets) [9]. In the Asia-Pacific, cities and energy grids in countries such as Japan and Singapore are placing a premium on cyber-physical resilience, backed by Singapore's Cybersecurity Act, which imposes obligations on operators of critical information infrastructure. On the other hand, adoption in developing country contexts remains spotty due to resource limitations, but there are opportunities for "leapfrogging" traditional solutions, as cost-effective, cloud-native, and open-source Zero-Trust products are available [27]. All together, these regional approaches illustrate that international harmonisation and standardisation are likely to significantly influence how we measure and enforce resilience as energy infrastructures continue to be further digitised and connected.

6.5 Linking Zero-Trust Controls with Resilience Dimensions in IT/OT-Converged Systems

Table 2. Linking Zero-Trust with Resilience Dimensions in IT-OT Converged Systems

Zero-Trust Control	Anticipation (Preventive Capability)	Absorption (Impact Containment)	Recovery (Restoration Speed)	Adaptation (Learning & Improvement)
Identity-Centric Access (MFA, RBAC)	Reduces the likelihood of credential compromise; blocks unauthorised access attempts	Limits privilege escalation	Enables faster incident scoping through user traceability	Policy refinement based on access anomaly patterns
Micro-Segmentation (Zone-Conduit Model)	Pre-emptively restricts cross-zone communication	Prevents lateral movement; confines breach to a single segment	Reduces system-wide shutdown requirements	Segmentation rules updated after incident analysis
Continuous Verification & Monitoring (SIEM Integration)	Detects abnormal behaviour early (reduces MTTD)	Enables rapid containment through automated alerts	Accelerates MTTR via centralised visibility	Threat intelligence integration improves future detection
Secure Firmware Lifecycle (Signed Updates, Secure Boot)	Mitigates supply chain compromise risk	Prevents execution of tampered code	Simplifies root-cause identification	Strengthens long-term asset trust model
Device Authentication & Certificate Management	Ensures only trusted devices communicate	Blocks rogue device insertion	Enables selective device isolation	Certificate revocation and renewal policies evolve
Edge Autonomy & Local Interlocks	Anticipates cloud/network failure	Maintains safe operation during disruption	Supports rapid restoration of telemetry	Operational logic improved from post-incident review
Least Privilege Enforcement	Minimises attack surface exposure	Limits the operational impact of compromised accounts	Reduces investigation scope	Role definitions are refined periodically

7. Conclusion

The integration of IT and OT has emerged as a hallmark of today's critical infrastructure systems, such as CGD networks. This results in real-time monitoring and predictive analytics, leading to more effective operations. However, it also creates a new spectrum of cyber risks for businesses to deal with. In this paper, we reviewed the risks and opportunities of IT/OT convergence from a security perspective, with a specific focus on cybersecurity risks, Zero-Trust strategies, and the need to build industrial resilience. The study concluded that cybersecurity governance is as significant as technical design. Governance ensures that 'least privilege', secure firmware management, and immutable audit logging are consistently implemented in one direction. Moreover, Cyber-Resilient operations demand blended talent, including engineers and cyber warriors alike. Furthermore, resilient operations require a hybrid workforce with skills in both engineering and cybersecurity. Without cross-disciplinary skill sets, misconfigurations, insider threats, and operational blind spots will persist.

Also, the research articulated that risk trade-offs exist for IT/OT convergence. Efficiency and real-time decision support are at odds with expanding attack surfaces and legacy vulnerabilities. Zero-trust models that involve micro-segmentation, ongoing validation measures, and the most rigorous access controls offer ideal protection and security, adaptive to latency, functional safety, and system uptime across OT infrastructures. The concept of resilience was identified as central. Our understanding of resiliency is not limited to cybersecurity; rather, it is the ability of a system to prevent, deter, withstand, recover from, and adapt to such disturbances. This whole-system vision for security shifts organisations away from a reactive, boundary-oriented defence model toward a proactive resilience engineering approach. Edge computing, anomaly detection, and a robust incident response framework are other aspects of this multi-dimensional resilience. Lastly, the research underlined the global aspect of IT/OT convergence concerns. North America, Europe, and the Asia-Pacific regions, as well as emerging markets, face similar threats, with regional risk exposure levels varying by regulatory maturity and resources in place. Global standardisation initiatives such as NIST SP 800-207 and ISA/IEC 62443 have developed a common vocabulary for the securing of critical infrastructure. Localised translations are yet necessary to accommodate context-specific legal, cultural, and economic conditions. In sum, securing IT/OT convergence in CGD and similar infrastructures requires an integrated approach combining governance, technology, workforce training, and resilience engineering. Zero-Trust is a critical enabler but must be deployed as part of a broader, adaptive strategy.

8. Contribution and Novelty of the Study

The study brought four integrated contributions: conceptual unification, methodological advancement, sector-specific operationalisation, and measurement-linked resilience evaluation. The study uniquely bridges IT/OT convergence, Zero-Trust cybersecurity, and resilience engineering within the oil & gas downstream context, moving beyond siloed perspectives to propose a unified cyber-physical governance model. On the methodology part, it connects Zero-Trust controls such as micro-segmentation and continuous verification to measurable operational outcomes like MTTD, MTTR, and downtime reduction. The research also contextualised these principles within downstream Oil & Gas industry's safety-critical, legacy-constrained environments, enhancing practical relevance for similar infrastructures. Finally, it touched upon resilience as a measurable, governance-embedded design objective rather than a by-product of security layers.

9. Declaration of Competing Interests

The author declares no conflict of interest.

Funding: This research received no external funding."

References

- [1] Schwab, K. *The Fourth Industrial Revolution*; Crown Business, 2017.
- [2] Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The Industrial Internet of Things (IIoT): An Analysis Framework. *Comput. Ind.* **2018**, *101*, 1–12. <https://doi.org/10.1016/j.compind.2018.04.015>
- [3] Harkat, H.; Camarinha-Matos, L. M.; Goes, J.; Ahmed, H. F. T. Cyber-Physical Systems Security: A Systematic Review. *Comput. Ind. Eng.* **2024**, *188*, 109891. <https://doi.org/10.1016/j.cie.2024.109891>
- [4] Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45. <https://doi.org/10.1109/MCOM.2012.6257525>
- [5] Bellamkonda, S. Ransomware Attacks on Critical Infrastructure: A Study of the Colonial Pipeline Incident. *Int. J. Res. Comput. Appl. Inf. Technol.* **2024**, *7*, 1423–1433. <https://doi.org/10.5281/zenodo.14191113>
- [6] Kindervag, J. *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*; Forrester Research, 2010.
- [7] National Institute of Standards and Technology. *Zero Trust Architecture (SP 800-207)*; NIST: Gaithersburg, MD, 2020. <https://doi.org/10.6028/NIST.SP.800-207>
- [8] ISA/IEC 62443. *Security for Industrial Automation and Control Systems*; International Society of Automation/International Electrotechnical Commission, 2018.
- [9] European Union Agency for Cybersecurity (ENISA). *NIS2 Directive: An Overview of Obligations and Measures*; ENISA, 2022.
- [10] Ramachandran, K.; Pandi, M.; Pallakku, S. Towards a Zero Trust Cybersecurity Framework: Enhancing Data Protection in Multi-Cloud and Hybrid IT Infrastructures. **2025**, *9*, 1–13.
- [11] Hollnagel, E. *Safety-I and Safety-II: The Past and Future of Safety Management*; Ashgate, 2015.
- [12] Linkov, I.; Trump, B. D. *The Science and Practice of Resilience*; Springer, 2019. <https://doi.org/10.1007/978-3-030-04565-4>
- [13] Kumar, P. Zero Trust Architecture for SME Cybersecurity: Enhancing Resilience in the Digital Transformation Era. *Int. J. Prog. Res. Eng. Manag. Sci.* **2025**, *5*, 2791–2819.
- [14] Masum, M. R.; Training, T. Cybersecurity, Zero Trust, and Risk Management Framework (RMF) Implementation Workshop by Tonex. **2024**. <https://doi.org/10.13140/RG.2.2.20285.27361>
- [15] Alawi, N. Evergreen OT Security Assurance: A Sustainable Approach to OT Cybersecurity Risk Management. **2025**. <https://doi.org/10.2118/224964-MS>
- [16] Mickie, J.; Weng, J. Zero Trust Security: A Proactive Cybersecurity Model for Risk Management. **2025**. <https://doi.org/10.13140/RG.2.2.20335.55201>
- [17] Wang, X.; Bhuse, V.; Cheng, Y. A Zero Trust Module for Cybersecurity Education. *J. Colloq. Inf. Syst. Secur. Educ.* **2025**, *12*. <https://doi.org/10.53735/cisse.v12i1.193>
- [18] Chang, H.-C.; Lund, B.; Beuerlein, E.; Mote, C. Investigating the Symbiotic Relationship between Artificial Intelligence and Blockchain to Promote Zero-Trust Cybersecurity in an Evolving Information Ecosystem. *Inf. Discov. Deliv.* **2025**. <https://doi.org/10.1108/IDD-11-2024-0185>
- [19] Moses, J.; Emmanuel, F. Zero-Trust Architectures as a Resilience Strategy for Mid-Market Cybersecurity. **2025**.
- [20] Walsham, G. Doing Interpretive Research. *Eur. J. Inf. Syst.* **2006**, *15*(3), 320–330. <https://doi.org/10.1057/palgrave.ejis.3000589>
- [21] Hevner, A.; March, S.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* **2004**, *28*(1), 75–105. <https://doi.org/10.2307/25148625>
- [22] Slay, J.; Miller, M. Lessons Learned from the Maroochy Water Breach. In *Critical Infrastructure Protection*; International Federation for Information Processing Digital Library, 2007; Vol. 253, pp 73–82. https://doi.org/10.1007/978-0-387-75462-8_6
- [23] Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Priv.* **2011**, *9*(3), 49–51. <https://doi.org/10.1109/MSP.2011.67>
- [24] Weill, P.; Ross, J. W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*; Harvard Business Press, 2004.

-
- [25] Knowles, W.; Prince, D.; Hutchison, D.; Disso, J. F. P.; Jones, K. A Survey of Cyber Security Management in Industrial Control Systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, 9, 52–80. <https://doi.org/10.1016/j.ijcip.2015.02.002>
 - [26] Koppichetti, R. K. Convergence of Information Technology (IT) and Operations Technology (OT) in Bio-Pharmaceutical Manufacturing Industry. **2023**. <https://doi.org/10.5281/zenodo.14866213>
 - [27] Bhushan, B.; Rajgopal, P.; Sharma, K. An Intent-Aware Zero Trust Identity Architecture for Unifying Human and Machine Access. *Int. J. Comput. Exp. Sci. Eng.* **2025**, 11. <https://doi.org/10.22399/ijcesen.3886>
 - [28] Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*; Information and Privacy Commissioner of Ontario, **2010**.