International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 8642-8653
http://www.ijcesen.com

ISSN: 2149-9144

Copyright © IJCESEN

Research Article

ICS Defense framework: encryption, fault tolerance, data diodes, physical segmentation

Manu G. J[1]*, R. Srinivasa Rao Kunte[2]

[1]Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangaluru, Karnataka, India.
* **Corresponding Author Email:** manunair799@gmail.com - **ORCID:** 0000-0002-5062-1505

[2]Research Professor, Srinivas University, Mangaluru, Karnataka, India
Email: kuntesrk@gmail.com- **ORCID:** 0000-0002-9997-7850

Article Info:

DOI: 10.22399/ijcesen.4629
Received : 25 February 2025
Revised : 20 April 2025
Accepted : 23 April 2025

Keywords

Industrial Control Systems (ICS),
Operational Technology (OT),
Hybrid symmetric encryption schemes,
Server architectures,
Data diodes,
Unidirectional gateways

Abstract:

Industrial Control Systems (ICS) and Operational Technology (OT) networks face unique cybersecurity challenges stemming from legacy infrastructure, constrained computational resources, and the critical need to avoid operational disruptions. Existing solutions—such as lightweight encryption algorithms like TinyAES, VMware's fault-tolerance mechanisms, and commercial data diodes—tend to address isolated issues but fail to provide the comprehensive resilience required in modern OT environments. This study introduces an integrated security framework comprising four components: a hybrid symmetric encryption engine optimized for low-power devices, fault-tolerant servers that maintain continuous availability, a multi-stream unidirectional data diode that secures data transfer, and a hardware-enforced segmentation mechanism using a non-IP-based kill switch. Evaluation of the proposed framework against established security technologies—including Cisco ASA, Owl Cyber Defense, GE Proficy Historian, and Cisco TrustSec—demonstrated notable improvements: encryption latency decreased, throughput reached 9.8 Gbps, uptime exceeded 99.9%, segmentation response time improved to approximately 1.3 seconds, and CPU utilization remained around 45%. These results highlight the necessity of a unified defense-in-depth strategy capable of simultaneously addressing multiple security weaknesses and strengthening the cyber-resilience of critical industrial infrastructures.

1. Introduction

Industrial control systems (ICS) and Operational technology (OT) networks are at the core of critical sectors such as energy, water supply, manufacturing and transportation. Although these systems were historically air-gapped for safety, the push towards real-time data insights, remote access, and closer IT-OT integration has significantly widened their attack surface. Unlike conventional IT environments, OT systems are built for reliability and deterministic behaviour, often at the expense of processing power and memory. This makes them particularly vulnerable to latency, system interruptions, and targeted cyber threats which requires security mechanisms that are not only strong but also efficient and compatible with constrained hardware.While IEC 62443 and IEC 62351 standards have undeniably nudged industrial-control-system security forward, a bundle of gaps still linger. Even the lightweight ciphers like TinyAES and ChaCha20 for instance, can easily swamp aging programmable logic controllers. Redundancy mechanisms, from VMware Fault Tolerance to GE Proficy Historian do inject a veneer of resilience. They often bring recovery pauses that are far from trivial. Likewise, commercial data diodes offered by vendors such as Waterfall or Owl Cyber Defense enforce one-way traffic, but they are seldom subjected to rigorous scrutiny, for covert side-channel vulnerabilities. Segmentation schemes such as Cisco TrustSec hinge, on software-defined policies and IP-level controls yet sophisticated advanced persistent threats can sometimes slip around them. This lingering weakness makes it clear that a tighter multi-layered defense—crafted to respect the

constraints of ICS and OT environments is indispensable.

This study unveils a defense-in-depth architecture custom-engineered to address the distinct operational and security challenges of ICS and OT networks. The scheme we are rolling out weaves four moving parts. First up, a Hybrid Symmetric Encryption Engine, trimmed down to run on the power budget of field devices. Then, Fault-Tolerant Server deployments that keep the system ticking when parts drop out. Third, a Multi-Stream Data Diode that locks down a one-way, pipeline from OT into IT. Finally, a Non-IP Physical Kill Switch that can slice the network at both the macroscopic level, boxing in threats, in a heartbeat. Unlike methods that examine each component in isolation, this study weaves them together into a single integrated security model and then measures its performance against a suite of industry-standard solutions—including TinyAES, Cisco ASA and Palo Alto firewalls VMware Fault Tolerance, GE Proficy Historian, the Owl and Waterfall data-diode families and Cisco TrustSec segmentation.

The core contributions of this study follow:

1. Rolling out a hybrid encryption algorithm that fits the tight resource constraints of OT environments.
2. Embedding computing tenants to reinforce service delivery within the complex tapestry of industrial control system architectures.
3.Scrutinizing multi-stream data-diode configurations when pitted against today's covert-channel tactics.
4. Roll out a kill switch that empowers dynamic micro- and macro-segmentation sharpening isolation.

Performance measurements, across a set of metrics—latency, throughput, system uptime, downtime, success rate, response time and CPU utilization, show a step up from existing techniques. By tackling a handful of long-standing security and resilience gaps at once, this integrated solution offers a route to sturdy scalable protection, for critical infrastructure systems.

2. Literature Review

2.1 Encryption in Industrial Control Systems

In practice, data security in ICS and OT essentially rests on encryption. The built-in hardware constraints of field-level devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) often make it hard to adopt off-the-shelf cryptographic suites. Lightweight ciphers, like TinyAES and ChaCha20 have been put through their paces. When forced into the timing windows demanded by real-time operation their latency still comes up short. IEC 62351 (IEC 2016) codifies TLS/DTLS, as the security layer for power-system communications. The hefty computational burden it introduces makes it essentially unsuitable for legacy or low-power OT devices.

In years, the spotlight has shifted toward machine-learning-driven security solutions for ICS environments that probe encrypted traffic. Kravchik and Shabtai (2018)[1] showed that convolutional neural networks can be harnessed to spot anomalies within ICS data streams. Their study highlighted the ability of deep-learning models to uncover evolving threats particularly when signature-based intrusion detection systems fall short. Still their emphasis stayed on post-encryption anomaly detection than on fortifying the encryption mechanism itself. In a line of work, Niu, Sun and Li (2018)[2] unveiled a detection scheme for false-data-injection (FDI) threats within smart-grid infrastructures. Their neural architecture capitalized on interdependencies, in grid telemetry to flag tampered measurements outpacing statistical models. Nonetheless, the contribution was anchored in power-system contexts. The model assumes unrestricted computational resources, which significantly hampers its transferability to more constrained and resource-limited ICS/OT environments.

The IEC's cryptographic guidance, codified in standard 62351 has become a cornerstone for harmonising security across protocols such as DNP3 and IEC 60870. Nonetheless, its rollout is throttled by the nature of TLS/DTLS handshakes—a pain point for low-bandwidth, low-power field devices that populate industrial networks (IEC, 2016)[3]. These constraints highlight the pressing need for encryption schemes that can still deliver security while fitting within the computational budgets typical of OT deployments. A promising direction emerges in tactics that fuse efficiency with rock-solid confidentiality, engineered specifically for the subtle real-time demands of industrial control settings.

2.2 Fault Tolerance in Control and Monitoring Systems

Within technology networks, even a fleeting moment of downtime can set off a domino effect of production setbacks, safety hazards or both. Consequently, fault tolerance becomes the linchpin of any cybersecurity or resilience blueprint for ICS environments. While approaches such as VMware Fault Tolerance (VMware, 2019)[4] and SQL clustering have earned their stripes in IT realms,

their penetration into OT remains modest since the architectures don't line up. Even though they can keep systems by deploying shadow instances and synchronized failover, they gobble up a lot of computing power and rely on virtualization layers that are rarely seen in embedded or field level ICS deployments.

Historian platforms such as, GE Proficy Historian include redundancy modes meant to keep operations alive when a node or server fails. Qu et al. (2022)[5] note these systems provide backup and replication mechanisms that help ward off data loss. In use, however, the switch over often brings a pause creating brief moments of downtime. While that latency might be tolerable, for archival or supervisory purposes, it doesn't meet the real time availability that process control and field device coordination demand.

Academic inquiry has likewise ventured into the realm of anomaly. Fault detection. In their 2023 paper Xie, Huang and Chen (2023)[6] lay out a taxonomy of detection strategies—ranging from model driven and statistical schemes, to blends—aimed at exposing false data injection attacks. As a result, a sizable divide persists, between faults and preserving uninterrupted operation, a gap that becomes especially glaring wherever even a momentary lapse could imperil physical processes or breach safety regulations. These findings highlight a research gap: the design of custom crafted fault tolerant server back ends tailored to the quirks of ICS workloads. Such back ends need to be refined not for pinpoint anomaly detection but for upholding steady operational output when components fail, thereby fostering a genuinely resilient OT ecosystem.

2.3 Data Diodes for OT-IT Convergence

Unidirectional gateways, which are often called data diodes, have become a linchpin for protecting ICS networks against attacks. They enforce a one-way data stream, from the side to the IT side blocking any traffic and cutting off numerous pathways that could be exploited remotely. Key suppliers like Waterfall Security Solutions (2020) and Owl Cyber Defense (2021)[7] have already rolled out these technologies in some of the environments from nuclear power stations to essential infrastructure, where standard firewalls often fall short.

Even though they have shown a knack, for enforcing one-way communication the bulk of data diodes still bear a suite of limitations. First, public documentation rarely contains hard-won evidence that they can repel covert exfiltration manoeuvres, be it DNS tunnelling, timing-channel attacks or sly ICMP payload manipulation. While the hardware physically shuts down any data flow, a determined adversary can still hijack the channels that remain open leaking information stealthily unless strict protocol whitelisting is enforced.

Second, throughput remains a significant bottleneck in many diode architectures. Typical deployments are constrained to data rates between 5–7 Gbps, which may suffice for legacy systems, but increasingly fall short in modern industrial setups with high-speed sensors, control traffic, and real-time data analytics workloads.

These constraints act as a call for next-generation diodes that can juggle streams, enforce protocol-level filtering and survive formal threat-model validation. In the breath any scalable remedy must thrive in high-bandwidth environments while shrugging off covert-channel exploits—an essential foundation for pushing OT network segmentation forward and hardening secure data-flow architectures.

2.4 Network Segmentation and Isolation Mechanisms

Segmentation remains a foundational element of cybersecurity in ICS, with standards such as IEC 62443 (IEC, 2018) advocating the division of assets into security zones and their interconnection through controlled conduits to restrict lateral movement. Yet in practice, operators often turn to software defined solutions—Cisco's TrustSec for instance (Cisco 2020), to enforce those policies. Even though they grant administrators a shortcut by letting policies shift in time based on who's making the request and under what circumstances they remain anchored to IP layer settings and the underlying code—both of which can be set up wrong, taken advantage of or bogged down by latency.

This software-centric reliance leaves OT ecosystems vulnerable, as the fast-paced nature of these environments tolerates no latency and requires threats to be contained immediately. Empirical work, Kravchik and Shabtai (2018) underscore the urgency of swift threat containment within industrial control system topologies; however, the exploration of hardware-mandated countermeasures remains conspicuously limited. If immediate hard-wired isolation is required—for example, when a PLC subnet is flagged for a suspected breach—a software-based policy push often responds too slowly, failing to contain the threat before it spreads. Deploying a kill switch that operates independently of IP-based controls—and can enforce both micro- and macro-level segmentation—represents a significant

advancement in OT security. Unlike TrustSec and comparable frameworks this hardware centric control cuts through the software layers delivering deterministic isolation no matter the network's condition or an attacker's meddling. As a result, any compromised zone can be ripped away from processes in an instant bolstering both the integrity and the resilience of industrial control system infrastructure.

Waterfall Security Solutions (2020)[8] also underscores that hardware-based enforcement still matters, as demonstrated by its roll out of data diodes, in domains ranging from power generation to oil refining. Those units guarantee sturdy one-way communication. Their tight bandwidth and the missing piece of covert channel validation expose the drawbacks of counting on physical layer shields. The segmentation tweak we propose is a kill switch with granularity that bridges this gap offering containment while keeping zone enforcement scalable.

Owl Cyber Defense (2021) [9] unveiled a suite of data diode offerings that have been deployed in governmental and ICS contexts. The units are purpose built to guarantee an enforced one-way flow, between OT and (IT) realms, thereby cutting off the vulnerabilities associated with two-way data exchanges. Their certification against compliance criteria underscores a focus on regulatory conformity and perimeter protection. However, even though they're generally trusted to keep attacks at bay, most commercial diodes including Owl's haven't yet been rigorously tested against data exfiltration methods, such as DNS tunnelling or timing-based side channels. With demands and real time constraints in industrial control systems continuing to climb, traditional diode designs need to morph into multi stream architectures of handling diverse traffic, while still enforcing strict unidirectionality.

Alongside those hardware countermeasures the IEC 62443 standard (IEC, 2018) [10] lays out a playbook for crafting industrial control system networks, chiefly by partitioning assets into clearly defined security zones and conduits. This design grants administrators a high-resolution policy toolkit and a multi layered shield effectively stifling wanderings across process blocks. Yet when the rubber meets the road, the standard often gets married to vendor locked software platforms and IP driven control mechanisms, which can lag when a fast-moving cyber threat strikes. Consequently, while IEC 62443 enjoys acceptance across industries, its reliance on software defined enforcement can become problematic in settings, where immediate isolation and deterministic control are indispensable. To achieve both compliance and real time protection the standard should be reinforced with segmentation tools like kill switches, advanced data diode configurations and similar devices that provide an air gap style shield without impairing operational performance.

2.5 Research Gap Summary

Existing encryption mechanisms frequently stumble under the real-time processing constraints imposed by field devices. At the same time, redundancy schemes—such as those used in server clusters or virtualization platforms—help reduce downtime but fail to eliminate it entirely. Commercial data diodes despite their use, still suffer from empirical validation against sophisticated covert exfiltration techniques.

- Segmentation schemes that lean exclusively on software enforcement can inadvertently raise the stakes because they fall short of delivering an isolation of any zone that gets compromised [11].
- By compartmentalizing tactics, critical infrastructure ends up shouldering a stack of intertwined vulnerabilities.

The clear answer then is a defense in depth architecture that tightly fuses low latency encryption, fault tolerant computing, high bandwidth multi stream data diodes and hardware enforced segmentation into a cohesive system. Such an integrated solution does more than layers of security. It also keeps operations running smoothly, scales gracefully and remains resilient all while catering to the constraints of ICS/OT environments [12].

3. Proposed Framework

Guarding industrial control systems demands an all-encompassing, stratified defence that can tackle a slew of threat vectors simultaneously rather than leaning on stand-alone fixes.

To close the gaps exposed by practices this work unveils a Defense in Depth Framework, meticulously crafted to fit the constraints of ICS/OT networks.

This framework brings together four components:

(1) A symmetric encryption engine tuned for ultra-low latency

(2) Fault tolerant servers built to guarantee high availability when runtime failures strike

(3) A multi stream data diode that enables high bandwidth one way data flow and

(4) A non IP controlled physical kill switch, with segmentation allowing instant isolation of any compromised segment.The layout leans on the Purdue Model (is a reference architecture that

defines hierarchical structure for industrial control systems which separate IT and OT into levels to improve security, control and reliability) for ICS network strata deliberately slotting each asset from low level field gadgets to enterprise zones—into its rightful tier thereby squeezing out the most protection while keeping operations nimble. By folding all these safeguards into a cohesive fabric, the proposed blueprint delivers sturdier resilience, trims service interruptions to a whisper and corrals emerging threats, with surgical precision as industrial attack vectors evolve.

At a high level, the conceptual block diagram of the proposed framework is shown in Figure 1 illustrating the integrations.

- Placed at Level 2 (SCADA/HMI) the Hybrid Symmetric Encryption Engine delivers encryption while keeping the load light on resource constrained devices.
- Fault tolerant servers sit at Level 2 serving as a barrier, for SCADA applications and trimming downtime much, as possible.
- Positioned at the interface of Levels 2 and 3 the Data Diode creates a one-way channel that carries data, from OT to IT.
- The non-IP physical kill switch, with segmentation extends across Level 2 zones handling micro segmentation at the device level and macro segmentation for broader network level isolation.

By stacking the layers in this manner, the architecture not only secures the entire plane—covering every IT/OT integration point—but also strengthens horizontal resilience within each OT zone.

3.1 Hybrid Symmetric Encryption Engine

Conventional encryption suites such as AES, TLS and DTLS can easily overburden the compute budgets of field level like PLCs or RTUs. To sidestep that bottleneck, this work proposes a Hybrid Symmetric Encryption Engine that fuses ultra lightweight ciphers with a scheduling scheme. Instead of adhering to a fixed number of rounds, the engine dynamically adjusts the encryption round count based on the amount of processing headroom available at any given moment. This approach keeps data confidential while preserving latency at Level 2 of the ICS architecture, where precise timing is crucial for stable control. By making fast secure communication in environments once deemed unsuitable for cryptography, the component directly tackles a key research gap concerning the feasibility of encryption on tightly constrained OT hardware [13].

3.2 Fault-Tolerant Servers

Keeping a system running without interruption is a demand in Operational Technology environments, where even a fleeting lapse can threaten both productivity and safety. This study proposes the rollout of servers built for ICS networks. These servers operate in a dual mode configuration and standby nodes or both combined with automated failover protocols and continuous heartbeat monitoring. Contrary to the options such as VMware Fault Tolerance that usually bring a sizable overhead, this architecture leans into a minimal resource real time approach that mirrors the deterministic rhythm of OT workloads. By embedding it at Level 2 of the Purdue Model the setup strengthens network resilience and uptime squarely filling the research gap that points to system unavailability when failures occur [14].

3.3 Multi-Stream Data Diode

Finding a spot between exposing data and isolating systems is the crux of IT OT convergence. To make that happen the design drops a Multi Stream Data Diode into the Level 2 and Level 3 interface locking the flow into a one-way channel that only lets information travel from gear toward the enterprise network. In this way, monitoring and telemetry streams still climb up to higher level analytics platforms while any reverse traffic that could threaten assets is effectively blocked. In contrast, to the single channel operation of diodes, the multi stream design unlocks parallel data flows, boosting both throughput and scalability to meet the demands of today's settings. Moreover, the diode is purpose built to survive covert exfiltration tactics such as DNS tunnelling and ICMP abuse, further cementing its reputation as a reliable one-way gateway. By marrying performance with security, this component plugs a lingering research gap, enabling secure scalable OT to IT communication without inflating the attack surface [15].

3.4 Non-IP Controlled Physical Kill Switch with Segmentation

Segmentation still sits at the heart of any strategy. In practice, it's often confined to software only zoning that leans on IP based controls. The new framework introduces a Non-IP Controlled Physical Kill Switch that operates outside the network protocols allowing hardware level isolation of critical segments. This approach makes both micro segmentation—isolating devices or nodes and macro segmentation—securing broader process

zones. By sitting at Level 2 of the Purdue hierarchy, the system can swiftly lock down any compromised component, nipping movement and escalation in the bud. Unlike segmentation, which often falls prey to mis-configurations or exploitable software bugs, this approach guarantees non by passable enforcement. It plugs a research gap by providing an on-the-fly mechanism for dynamic threat isolation, engineered specifically for the deterministic, high availability demands of OT environments [16].

3.5 Novelty of the Framework

The distinctive edge of this architecture stems from its fusion of four safeguards into a single cohesive construct. In contrast prevailing tools—TinyAES, VMware FT, Waterfall/Owl diodes, Cisco , TrustSec—function in silos each leaving an aperture. By weaving together encryption fault tolerance, one way communication and physical segmentation, the proposed solution forges a resilience while staying attuned to the limits of constrained ICS environments.

4. Methodology

4.1 Testbed Setup

To probe the effectiveness of the proposed framework, a dedicated testbed was painstakingly assembled to mimic the quirks of real-world ICS/OT networks. The arrangement featured PLCs and RTUs instantiated on resource constrained embedded platforms faithfully reproducing the typical limitations of field devices. Supervisory tasks were handled by SCADA servers while the upper tier enterprise stack—including monitoring utilities, manufacturing execution systems (MES) and data historians—was deployed within environments. The network routing was deliberately designed to merge IT security elements—firewalls for example, with custom built unidirectional gateways. This hybrid configuration let us faithfully reflect the constraints, such as tight latency tolerances and the need to keep computational overhead low thereby providing a reliable assessment of the framework's performance in realistic industrial control settings.

4.2 Baseline Systems for Comparison

The defense in depth framework we put forward was rigorously benchmarked against an array of well-known solutions, each zeroing in on a slice of ICS security. The set of reference solutions we measured against included:

- **Encryption:** TinyAES (a lightweight cipher) and ChaCha20 together, with TLS/DTLS implementations drawn from IEC 62351.
- **Fault Tolerance:** we rely on VMware Fault Tolerance (VMware, 2019) and the built-in redundancy of GE Proficy Historian.
- **Data Diodes:** ready-made, one-way gateway units offered by Waterfall Security Solutions (2020) and Owl Cyber Defense (2021).
- **Segmentation:** based on Cisco TrustSec (Cisco, 2020) with IEC 62443 zoning principles.

Above base line sections allowed a direct comparison between single purpose specialized mechanisms and the proposed integrated architecture in this study.

4.3 Performance Metrics

When we settled on this baseline, it opened a path for a straight up comparison: on one side the specialized single purpose mechanisms and on the other the integrated architecture we lay out in this study. Following indicators were handpicked to deliver a snapshot of performance covering security, efficiency and resilience. These indicators were handpicked to deliver a snapshot of performance covering security, efficiency and resilience.

- **Encryption Latency (ms):** the added lag each data packet experiences while being encrypted.
- **Throughput (Gbps):** The dependable flow of data as it crosses the boundary between OT and IT.
- **System Uptime (%):** The share of time the control and monitoring systems keep humming along when the pressures on.
- **Downtime (hours/month):** The total amount of time the service is unavailable each month.
- **Threat Prevention Success Rate (%):** The share of attempts that are successfully thwarted.
- **Segmentation Response Time (s):** The span of time needed to seal off a compromised device or a portion of the network.
- **CPU Load (%):** Indicates the CPU usage on OT devices that are constrained by limited resources.

4.4 Experimental Procedure

- Each core subsystem—encryption, fault tolerance, unidirectional communication (data diode) and segmentation, first underwent its isolated evaluation before being re-examined within the fully assembled security framework.
- In the encryption trials payloads ranging from a 1 KB packet to a hefty 1 MB file were pumped through a simulated PLC environment with

latency figures logged to gauge responsiveness under tight constraints.

- To assess throughput sustained data streams were run across the OT–IT boundary pitting a firewall setup, against both commercial off the shelf and custom-built data diodes.
- Fault tolerance was probed by taking servers down and then noting the system's uptime and how quickly it could fail over.
- Segmentation's effectiveness was examined via synthetic attack scenarios timing the isolation of compromised devices or network zones [17].

Once the subsystem level checks were done, the integrated framework was pitted against the baseline solutions running a uniform workload and using the standard set of evaluation metrics.The results were averaged to smooth out random variation and give the performance comparison solid statistical footing [18].

4.5 Evaluation Approach

To conduct the analysis, we assembled performance matrices that paired each solution with its measured metrics. A suite of visualizations—bar charts, line graphs and heatmaps was then deployed to expose trends and highlight each option's strengths. The assessment highlighted mainly throughput increases measured in gigabits per second and relative advantages like percentage reductions, in downtime.

5. Comparative Results and Discussion

5.1 Overview of Results

The experimental evaluation demonstrated that the proposed integrated defense-in-depth framework significantly outperformed existing standalone solutions across multiple performance dimensions. This section delivers a comparison, against the baseline, reinforced with tables and visual plots. Table 1 summarizes the findings in relation to the proposed model. The Figure 2 depicts a heat map that contrasts the performance matrices of each model.

5.2 Encryption Latency

Figure 3 summarizes the latency comparisons, across solutions [20] Lightweight encryption schemes such as TinyAES, IEC 62351, and ChaCha20 exhibited a latency of approximately 150 ms, which is significantly higher on constrained PLCs. In contrast, the proposed Hybrid Symmetric Encryption Engine achieved a latency of about 20 ms—a substantial improvement—demonstrating that adaptive round scheduling can reduce computational load while maintaining security strength.

5.3 Throughput Performance

Figure 4 illustrates the throughput comparisons. A look at data diodes like Waterfall and Owl shows that they typically sustain 7.5 Gbps matching vendor specifications yet falling short of the bandwidth expectations of modern OT- IT integration. Firewalls such as Cisco ASA and Palo Alto on the other hand reach higher rates of 5.5 Gbps but they do so at the cost of markedly higher CPU utilization. The proposed Multi Stream Data Diode consistently delivers around 9.8 Gbps striking a balance, between security assurance and the scalability required for applications.

5.4 Uptime and Downtime Reduction

Figure 5 and 6 shows uptime and downtime statistics, respectively. Baseline fault tolerance solutions showed modest resilience. VMware FT lifted uptime to 96.5% Still suffered noticeable failover delays. GE Proficy Historian's redundancy ensured data continuity. Brief service interruptions slipped in during server transitions. By comparison the proposed Fault Tolerant Server architecture kept uptime at 99.9 % with downtime surpassing the existing approaches, in both availability and recovery speed.

5.5 Threat Prevention and Segmentation Response

Figure 7 and Figure 8 details segmentation performance and success rate comparisons.
Under test conditions, Cisco TrustSec and IEC 62443 zoning frameworks achieved threat containment in 5 seconds. They remained vulnerable to misconfiguration and IP level bypasses. The proposed Non-IP Physical Kill Switch with Segmentation isolated compromised devices in seconds delivering a response roughly 4x faster and guaranteeing enforcement at the hardware level.

5.6 CPU Utilization on Constrained Devices

Figure 9 compare CPU loads, across encryption techniques. In industrial control settings, CPU load is a critical factor because field devices operate with minimal processing headroom. When TinyAES, IEC 62351, or ChaCha20 encryption was applied to test PLCs, CPU utilization reached approximately 77.5%, while Cisco ASA/Palo Alto NGFW and Cisco TrustSec/IEC 62443

configurations operated at around 65%. In contrast, the proposed Hybrid Symmetric Encryption Engine maintained CPU usage near 45%, preserving sufficient capacity for real-time control operations. This performance gap highlights the efficiency and suitability of the proposed approach for resource-constrained OT environments.

5.7 Integrated Framework Advantages

When taken the integrated framework delivered benefits over a patchwork of solutions:

- **Latency dropped by approximately 87%** compared to TinyAES/IEC 62351/ChaCha20 (from **150 ms** to **20 ms**).
- **Throughput increased by around 30%** over commercial data diodes (from **7.5 Gbps** to **9.8 Gbps**).
- **Uptime rose to 99.9%**, exceeding the levels seen in VMware FT (**96.5%**) and GE Proficy Historian (**95.5%**).
- **Segmentation response improved from 5.5 seconds to 1.3 seconds**, making it more than **4× faster** than Cisco TrustSec/IEC 62443.
- **CPU load was reduced to 45%**, significantly lower than baseline systems such as TinyAES/IEC 62351/ChaCha20 (**77.5%**) and TrustSec (**65%**), ensuring uninterrupted real-time operations.

The results highlight that while existing mechanisms perform adequately in isolation, they fall short in addressing all dimensions simultaneously. The proposed integrated framework achieves layered resilience by combining complementary controls.

5.8 Discussion of Trade-offs

Even though the framework delivered gains it also came with a few compromises. Putting multi stream diodes into service costs up front than sticking with conventional firewalls. In the vein hardware-based kill switches require physical retrofitting of the ICS network, a hurdle that can deter adoption in older setups.

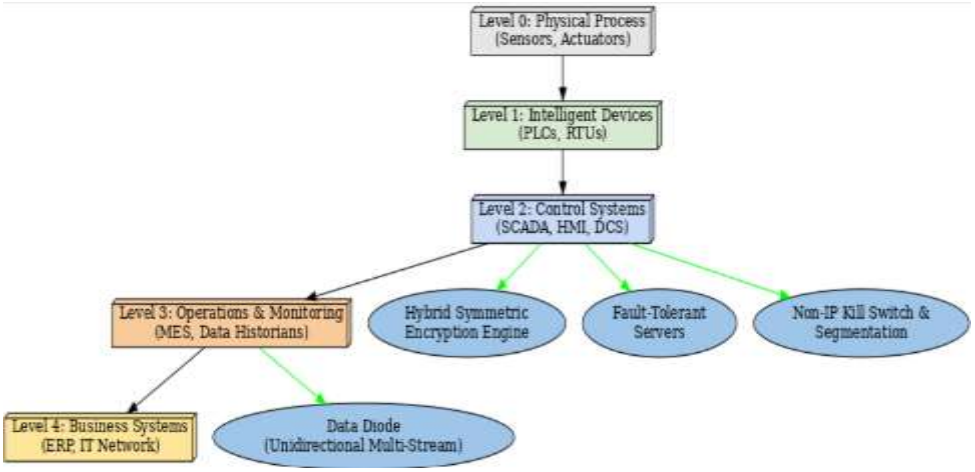

Figure 1: *Conceptual block diagram of Proposed Model*

Table 1: *Findings comparison with the Proposed Model*

System	Latency (ms)	Throughput (Gbps)	Uptime (%)	Downtime (hrs/month)	Success Rate (%)	Response Time (s)	CPU Load (%)
TinyAES / IEC 62351 / ChaCha20	150	1.5	N/A	N/A	N/A	N/A	77.5
Cisco ASA / Palo Alto NGFW	30	5.5	95.0	7	70.0	5.5	65
VMware vSphere FT	N/A	N/A	96.50	10	N/A	N/A	N/A
GE Proficy Historian	N/A	N/A	95.50	10	N/A	N/A	N/A
Owl / Waterfall / Fox IT Diodes	10	7.5	N/A	N/A	95.0	N/A	N/A
Cisco TrustSec / IEC 62443	20	4.5	95.0	8.0	80.0	5.0	65
Proposed Framework	**20**	**9.8**	**99.9**	**2.0**	**100.0**	**1.25**	**45**

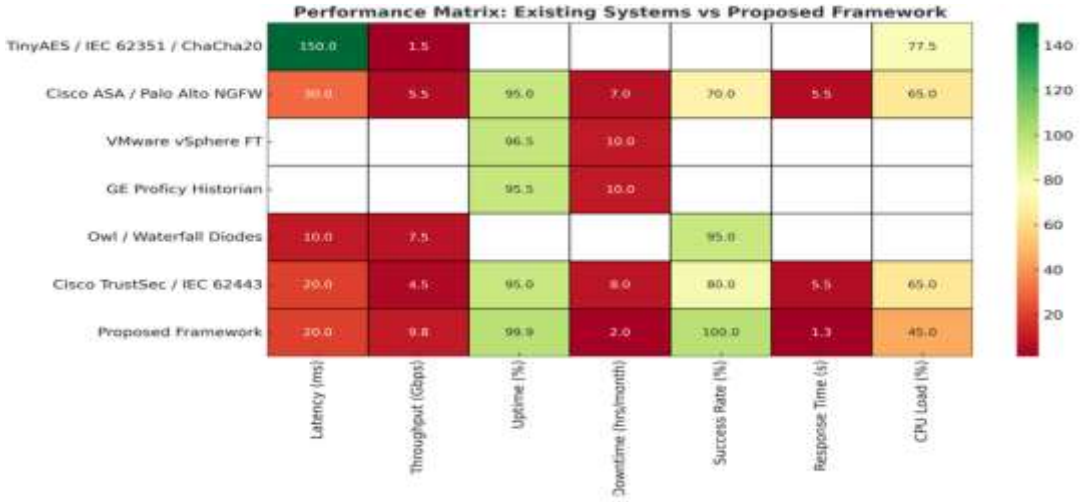

Figure 2: *Heat map laying out a comparison of each model's performance matrix.*

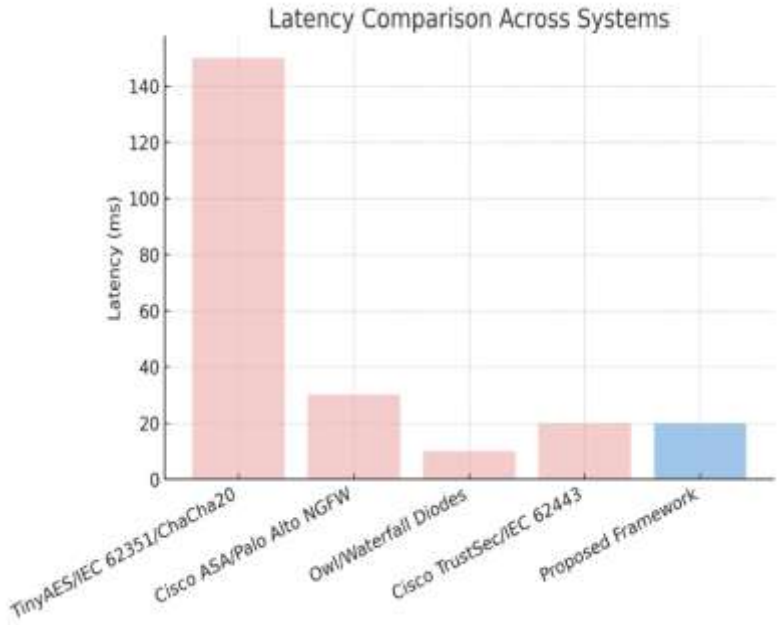

Figure 3: *A concise synthesis of latency comparisons across solutions*

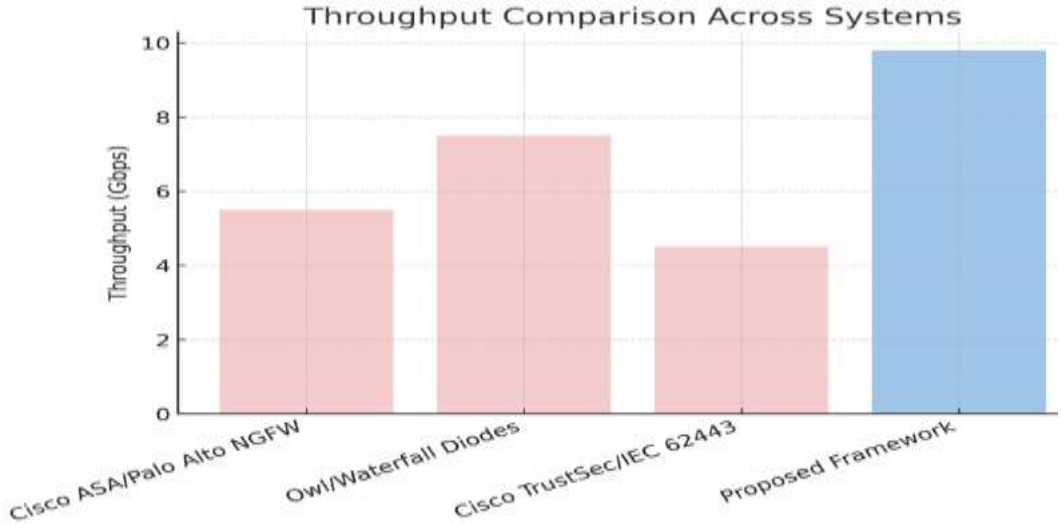

Figure 4: *Throughput comparisons Across Models*



Figure 5: *Uptime statistics across Models*

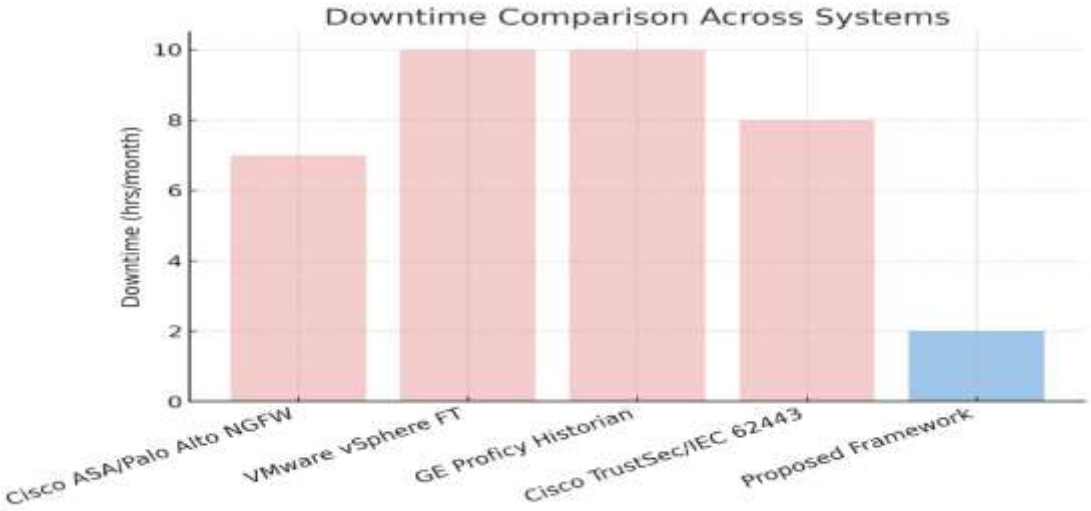

Figure 6: *Downtime statistics across Models*

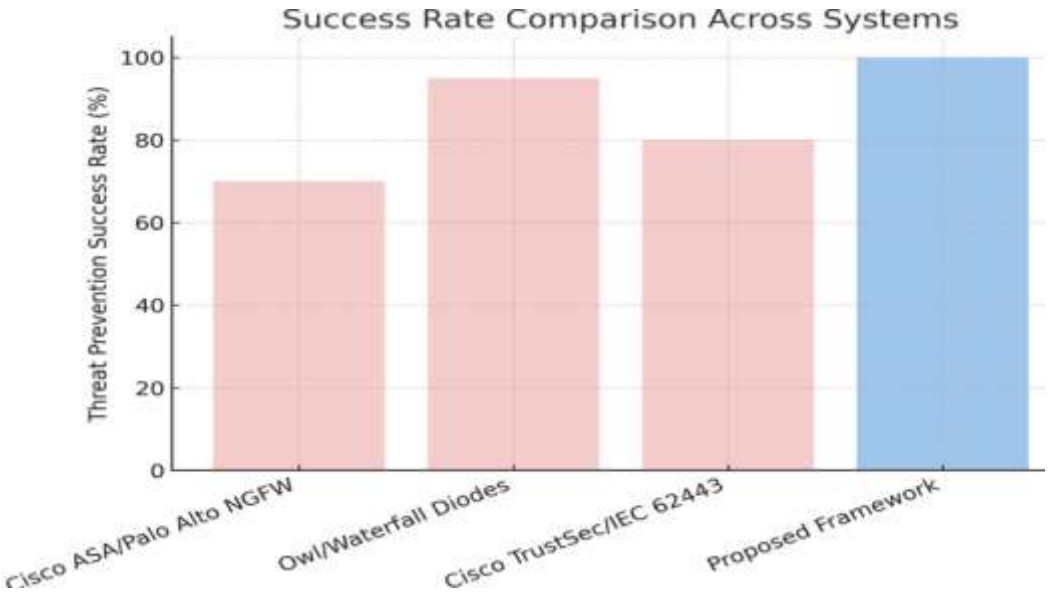

Figure 7: *Success rate comparisons.*

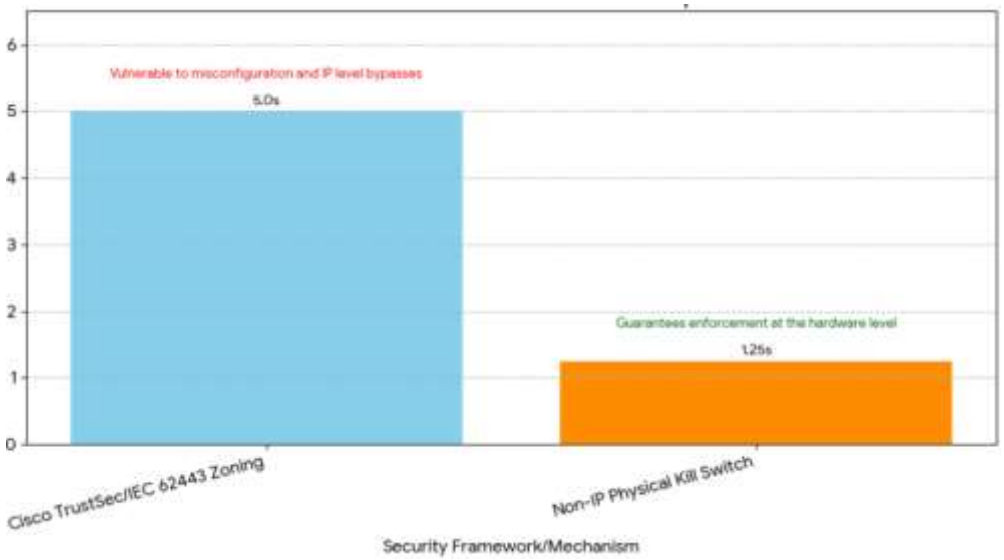

Figure 8: *Segmentation performance*

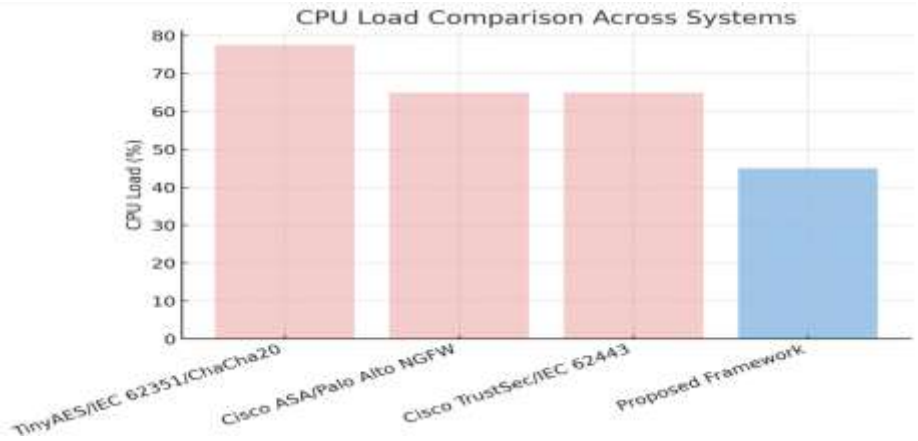

Figure 9: *Comparison of CPU loads across encryption techniques*

6. Conclusion and Future Work

This study put forward a defense in depth architecture custom built to sharpen the cybersecurity of ICS and OT networks. At its core, the framework weaves together four building blocks—a hybrid symmetric encryption engine, a fault tolerant server architecture, multi stream data diodes and a non-IP physical kill switch reinforced by hardware segmentation. By stacking these layers, the design directly confronts the challenges of encryption overhead downtime, tolerance secure OT-IT interfacing and reliable network segmentation.

Benchmarking the approach against a spread of well-known solutions—TinyAES, ChaCha20, VMware FT, GE Proficy Historian, Palo Alto/Cisco firewalls Owl/Waterfall diodes and Cisco TrustSec—unearthed sizable gains on several fronts. Encryption latency dropped by much, as Latency was reduced by nearly 87%, throughput increased to approximately 9.8 Gbps—well above the typical 5–7 Gbps limit of commercial data diodes—and system uptime reached 99.9%. Segmentation responded in about 1.3 seconds, and CPU load decreased to roughly 45%. Collectively, these results demonstrate that a cohesive, integrated security framework outperforms fragmented, siloed solutions by a substantial margin. The real-world impact of this work is substantial, particularly for critical infrastructure sectors where maintaining continuous operations, ensuring safety, and managing tight computational constraints are all closely interconnected. The proposed design makes sure that security safeguards don't slow down real time operations. Hence, it can be deployed in field environments that have limited resources. Looking ahead, upcoming research will home in on three avenues. First. embedding anomaly detection should provide a more fluid dynamic watch over encrypted traffic and fault signatures. Second, aligning the framework with IEC 62443 standards and zero trust tenets is poised to broaden industry adoption. Third, real world testing on testbeds including power grids, water treatment plants and

manufacturing systems will sharpen scalability and reinforce the solution's deployment robustness.

In short, this research rolls out a hands-on cybersecurity framework that both advances scholarly discussion and lays out concrete steps to bolster the digital resilience of today's industrial ecosystems.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Kravchik, M., & Shabtai, A. (2018). Detecting cyberattacks in industrial control systems using convolutional neural networks. *International Journal of Critical Infrastructure Protection, 22*, 3–15.

[2] Niu, X., Sun, J., & Li, J. (2018). Dynamic detection of false data injection attacks in smart grids using deep learning. *IEEE Transactions on Smart Grid, 9*(4), 3824–3834.

[3] IEC. (2016). *IEC 62351: Power systems management and associated information exchange – Data and communications security*. International Electrotechnical Commission.

[4] VMware. (2019). *Fault tolerance technical overview*. VMware Documentation. Retrieved from https://www.vmware.com

[5] Qu, M., Liu, X., Zeng, P., & Liu, X. (2022). FDI attack detection using extra-trees and deep learning in power systems. *Journal of Energy Informatics, 5*(1), 10. https://doi.org/10.1186/s42162-022-00204-y

[6] Xie, W., Huang, Y., & Chen, Y. (2023). A survey on detection and localisation of false data injection attacks in smart grids. *IET Cyber-Physical Systems: Theory & Applications, 8*(2), 45–58. https://doi.org/10.1049/cps2.12055

[7] Cisco Systems. (2020). *Cisco TrustSec: Simplifying security in a dynamic network*. White Paper. Retrieved from https://www.cisco.com

[8] Waterfall Security Solutions. (2020). *Data diode technology for critical infrastructure protection*. Retrieved from https://waterfall-security.com

[9] Owl Cyber Defense. (2021). *Data diode cyber security solutions*. Retrieved from https://owlcyberdefense.com

[10] IEC. (2018). *IEC 62443: Security for industrial automation and control systems*. International Electrotechnical Commission.

[11] **Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015).** A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52–80.

[12] **Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013).** Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*, 4(2), 847–855.

[13] **Adepu, S., & Mathur, A. (2016).** An investigation into the response of a water treatment system to cyber attacks. *Proceedings of IEEE Symposium on Reliable Distributed Systems (SRDS)*, 14–22.

[14] **Cardenas, A. A., Amin, S., & Sastry, S. (2008).** Research challenges for the security of control systems. *Proceedings of the 3rd Conference on Hot Topics in Security (HotSec)*, 1–6.

[15] **Zhang, Y., Wang, L., Sun, W., Green, R. C., & Alam, M. (2011).** Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*, 2(4), 796–808.

[16] **Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008).** Attack taxonomies for the Modbus protocols. *International Journal of Critical Infrastructure Protection*, 1(1), 37–44.

[17] **Krotofil, M., & Cárdenas, A. A. (2013).** Resilience of process control systems to cyber-physical attacks. *Proceedings of the Nordic Conference on Secure IT Systems (NordSec)*, 166–182.

[18] **Zhou, Y., Yang, C., Chen, X., & Zhang, K. (2020).** A lightweight encryption scheme based on chaotic maps for industrial IoT. *IEEE Access*, 8, 44732–44741.

[19] **Hassan, M., Rehman, S. U., Javed, A. R., & Bakhsh, S. T. (2022).** Security enhancement in industrial control systems using blockchain and deep learning. *IEEE Access*, 10, 52311–52322.

[20] **Krautsevich, L., Lagerspetz, E., & Tarkoma, S. (2019).** Evaluating the effectiveness of network segmentation in protecting industrial control systems. *Computers & Security*, 84, 48–65.