OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Security Centered Wireless Architecture for Industrial IoT Under EMC and RF Regulatory Constraints

Shankar Pangeni[1]*

[1]Lamar University, Electrical and Computer Engineering

DOI: https://doi.org/10.36348/sjet.2026.v11i04.003 | **Received:** 17.01.2026 | **Accepted:** 11.03.2026 | **Published:** 11.04.2026

***Corresponding author:** Shankar Pangeni
Lamar University, Electrical and Computer Engineering

Abstract

Industrial IoT systems rely heavily on wireless communication, yet security and regulatory compliance are often addressed separately during system development. This paper examines how wireless infrastructure security can be integrated with electromagnetic compatibility (EMC) and radio frequency (RF) regulatory requirements at the design stage. It analyzes common wireless attack vectors in industrial settings, including jamming, spoofing, and protocol exploitation, and evaluates how regulatory constraints influence hardware and network architecture decisions. A security centered device architecture is proposed where RF shielding, grounding schemes, spectrum allocation, and firmware isolation are treated as interconnected design elements. The framework incorporates zero trust communication principles within industrial wireless networks while maintaining compliance with EMC standards such as IEC 61000 and relevant RF certification requirements. The study demonstrates that early coordination between cybersecurity engineering and compliance engineering reduces redesign cycles and certification delays. The proposed model offers a structured pathway for building industrial wireless systems that meet both security and regulatory obligations without post development modifications.

Keywords: Industrial IoT, Wireless Security, EMC Compliance, RF Regulation, Zero Trust Architecture, IEC 61000, Spectrum Management, Secure Firmware Isolation.

I. INTRODUCTION

Industrial automation increasingly depends on wireless connectivity for sensor telemetry, machine coordination, and supervisory control. Industrial Internet of Things (IIoT) networks enable flexible deployment, cost reduction, and scalable monitoring across manufacturing floors, energy grids, and process industries. However, wireless connectivity introduces both cybersecurity risks and regulatory constraints. In many deployments, electromagnetic compatibility (EMC) compliance and RF certification are handled independently from cybersecurity engineering, leading to architectural fragmentation and costly redesign cycles. Industrial environments are electromagnetically complex spaces characterized by high power motors, switching devices, and dense metallic structures. These conditions create susceptibility to electromagnetic interference (EMI), signal degradation, and unintended emissions. At the same time, wireless channels expose devices to adversarial threats such as denial of service via jamming, spoofed identity injection, rogue access points, and firmware exploitation. Regulatory frameworks governing EMC and RF performance impose strict limits on emissions, immunity, and spectral usage. When security mechanisms are retrofitted after compliance testing, shielding modifications or encryption related power variations may disrupt previously validated RF performance. This paper proposes a unified design methodology in which cybersecurity, EMC compliance, and RF regulatory engineering are co-developed at the architectural stage. Rather than treating security as an overlay, the model integrates spectrum planning, grounding topology, firmware isolation, and zero trust networking as mutually dependent components. **Figure 01** the conceptual transition from siloed compliance security workflows toward an integrated security centered wireless architecture.

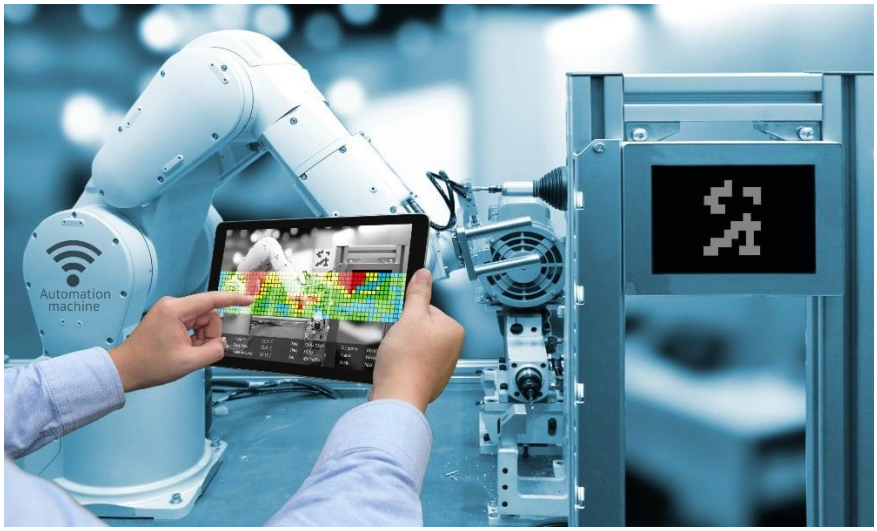

Figure 01: Industrial Wireless Environment and Integrated Security Compliance Design Context

1.1 Wireless Threat Landscape in Industrial IIoT

Industrial wireless networks face unique threat vectors due to their operational continuity requirements and deterministic control dependencies. Jamming attacks exploit narrowband industrial protocols by introducing high power interference within regulated frequency bands. Spoofing attacks manipulate MAC layer or application layer identifiers to inject false telemetry into supervisory systems. Protocol exploitation targets unpatched firmware stacks, often leveraging insecure update channels. Unlike enterprise IT environments, IIoT deployments frequently operate in latency sensitive loops where even short disruptions can halt production. Electromagnetic disturbances can mimic intentional jamming, complicating incident attribution. Consequently, EMC immunity design and cyber intrusion detection must be harmonized. Shielding strategies, antenna placement, and frequency hopping patterns directly influence both interference resilience and attack surface reduction. A security centered design must therefore treat physical layer robustness and cryptographic enforcement as complementary layers. Adaptive spectrum allocation combined with anomaly-based RF monitoring can distinguish malicious jamming from environmental interference. Grounding topology and PCB layout decisions affect signal integrity and side channel leakage. By embedding security principles into physical and link layer architecture, resilience improves without compromising regulatory conformity.

1.2 EMC and RF Regulatory Constraints

Industrial wireless devices must satisfy international EMC standards such as IEC 61000 and regional RF certification frameworks governing emissions, immunity, and spectrum allocation. These standards define permissible radiated emissions, conducted disturbances, electrostatic discharge tolerance, and surge immunity thresholds. RF compliance further regulates transmitter power, modulation characteristics, and spectral masks to prevent cross device interference. Security mechanisms influence RF characteristics. For example, encryption processes may increase processing latency and alter duty cycles, indirectly affecting spectral occupancy. Firmware updates may modify transmission behavior, requiring reevaluation under compliance testing. Improper shielding or grounding adjustments introduced for cyber hardening can alter antenna performance or detune resonance characteristics. The proposed framework integrates compliance simulation with security modeling during early hardware prototyping. EMC test planning is synchronized with threat modeling workshops to ensure design decisions support both immunity and confidentiality objectives. **Figure 02,** presents the interaction between regulatory constraints and wireless security engineering.

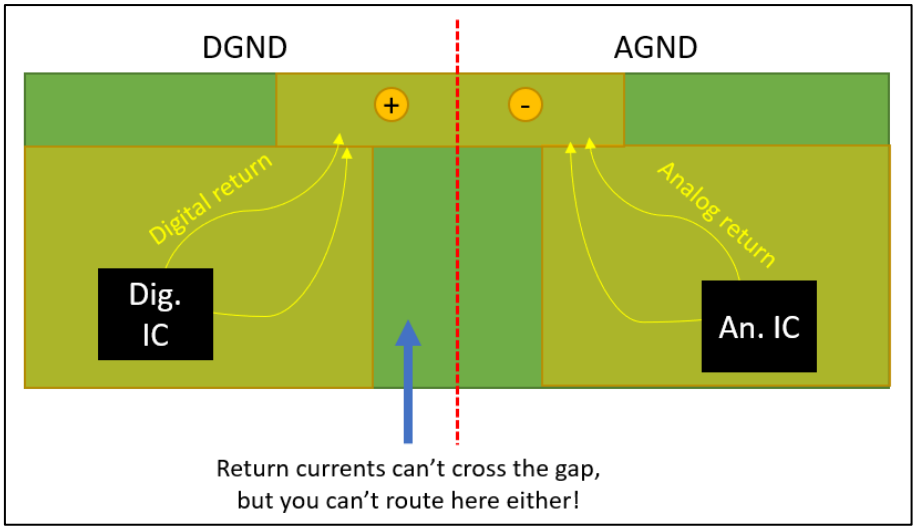

Figure 02: EMC and RF Compliance Factors Influencing Secure Wireless Architecture

II. Related Works

Recent literature explores wireless security, industrial IoT resilience, and regulatory aware communication frameworks. Early studies addressed RF coexistence challenges in dense IoT deployments [1,2]. Subsequent work investigated jamming resistant protocols and spread spectrum mitigation strategies [3,4]. Research on EMC aware hardware design highlighted the importance of grounding optimization and enclosure shielding [5,6]. Studies integrating zero trust models into OT networks emphasized segmentation and authentication controls [7,8]. Additional contributions examined firmware integrity validation and secure boot mechanisms in embedded systems [9,10]. RF fingerprinting and anomaly detection for wireless intrusion identification have been proposed to distinguish environmental interference from malicious signals [11,12]. Hybrid compliance security co design frameworks suggested synchronizing certification planning with threat modeling [13,14]. Research on spectrum governance in industrial environments highlighted dynamic allocation under regulatory power constraints [15,16]. Industrial wireless standards such as 5G URLLC adaptations for factory automation were evaluated for coexistence resilience [17,18]. Advanced shielding materials and PCB isolation techniques were studied to minimize side channel leakage [19,20]. Collectively, these studies demonstrate growing recognition of interdisciplinary integration between RF engineering and cybersecurity; however, comprehensive design stage integration models remain limited.

2.1 EMC Conscious Hardware Security

Hardware focused research emphasizes minimizing radiated emissions while enhancing immunity. Shielded enclosures, ferrite suppression, and differential signaling techniques reduce susceptibility to interference [21-23]. Embedded cryptographic co processors with isolated power domains improve firmware protection without increasing emission noise [24,25]. Investigations into side channel mitigation suggest that electromagnetic leakage can reveal cryptographic keys if shielding is inadequate [26,27]. Adaptive filtering and decoupling strategies have been proposed to stabilize RF performance under encryption intensive workloads [28,29]. Industrial validation studies demonstrate that early-stage PCB layout simulation significantly reduces certification failures [30,31].

2.2 Secure Spectrum and Network Architecture

Network layer research promotes zero trust segmentation and identity centric communication [32,33]. Spread spectrum modulation and frequency hopping mechanisms mitigate jamming risks under regulated power limits [34,35]. Secure firmware update pipelines leveraging signed images and hardware root of trust protect IIoT endpoints from persistent exploitation [36,37]. Machine learning–based RF anomaly detection has been proposed to classify interference patterns in real time [38,39]. Secure gateway architectures combining firewall isolation with RF monitoring reduce lateral movement in industrial networks [40]. Together, these contributions establish a foundation for integrated wireless security under compliance constraints.

III. METHODOLOGY

The proposed Security Centered Wireless Architecture (SCWA) follows a structured co design methodology that unifies cybersecurity engineering, electromagnetic compatibility (EMC) modeling, and RF regulatory mapping within a single architectural workflow. Rather than treating these domains as sequential compliance steps, the methodology integrates them from the earliest conceptual design phase. Threat modeling is conducted in parallel with hardware prototyping and RF spectrum planning to ensure that attack surface reduction strategies do not conflict with emission limits or immunity thresholds. EMC simulations are performed alongside cryptographic workload modeling to evaluate how encryption, authentication exchanges, and firmware operations influence radiated and conducted emissions. Regulatory

mapping aligns design parameters with international standards governing electromagnetic emissions, immunity levels, and spectrum allocation to ensure that security enhancements remain compliant across certification boundaries. The architecture is organized into five tightly coupled layers that operate cohesively rather than independently. The Physical Protection Layer addresses enclosure shielding, grounding topology, and PCB layout optimization to minimize electromagnetic leakage while preserving antenna efficiency and signal integrity. The Spectrum Governance Layer implements regulated frequency planning, adaptive frequency hopping, and power management techniques to maintain spectral compliance while mitigating jamming and interference risks. The Secure Communication Layer embeds zero trust authentication principles, mutual authentication handshakes, and encrypted transport protocols to protect data in motion without exceeding regulatory duty cycle constraints. The Firmware Isolation Layer incorporates secure boot mechanisms, hardware root of trust modules, memory segmentation, and sandboxing techniques to prevent unauthorized code execution and persistent exploitation. The Compliance Validation Layer integrates automated EMC pre testing, spectrum monitoring analytics, and certification tracking dashboards to ensure that security driven modifications do not invalidate regulatory approval. To quantify the integrated resilience of the architecture, a composite metric termed the Security Compliance

Resilience Index (SCRI) is defined as:

$$SCRI = \alpha \times (IR \times JR \times FR) + CI$$

where Interference Resilience (IR) reflects immunity performance under radiated and conducted disturbances, Jamming Resistance (JR) measures the effectiveness of adaptive spectrum strategies under hostile signal injection, Firmware Robustness (FR) evaluates secure boot enforcement and update validation integrity, Compliance Integrity (CI) represents sustained adherence to EMC and RF regulatory thresholds, and α denotes the adaptive integration coefficient reflecting system level coordination maturity. This multiplicative formulation emphasizes that weaknesses in any physical, cyber, or regulatory dimension proportionally reduce overall resilience, reinforcing the need for balanced optimization across all layers.

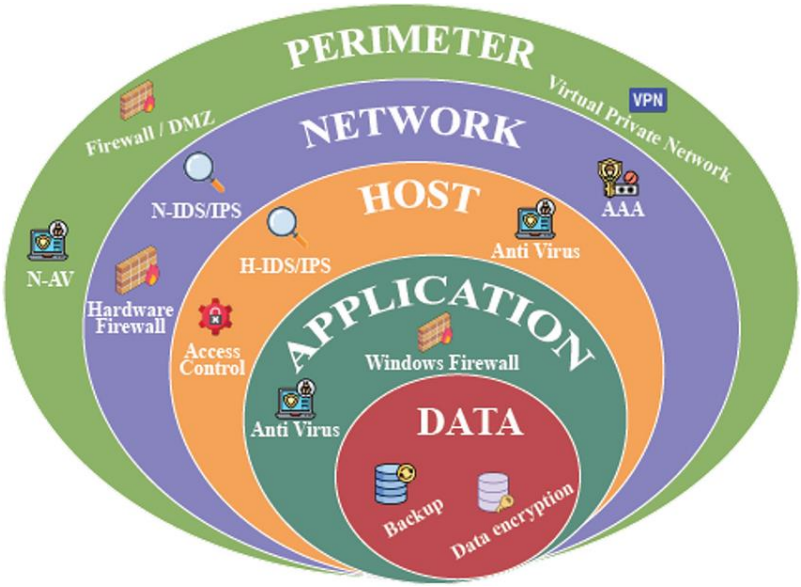

Figure 03: Layered Defense in Depth Security Architecture Model (Perimeter to Data Protection)

3.1 Architectural Validation

Architectural validation was conducted through multi domain simulation environments combining electromagnetic field modeling, RF propagation analysis, and cybersecurity penetration testing frameworks. Interference tolerance was evaluated by introducing controlled radiated emissions and surge disturbances consistent with industrial motor switching and high-power equipment operations. Shield optimized PCB designs demonstrated improved signal stability and reduced packet loss compared to baseline configurations lacking coordinated grounding strategies. The evaluation confirmed that grounding symmetry and shield continuity significantly enhanced immunity without degrading antenna radiation patterns. Jamming response performance was assessed by simulating narrowband and broadband interference sources operating within regulated frequency bands. Adaptive frequency hopping algorithms redistributed transmission across permitted spectral channels, reducing effective disruption time and maintaining deterministic communication cycles required for industrial control loops. The measured response latency indicated that spectrum adaptation mechanisms could restore communication continuity within acceptable operational thresholds. Firmware integrity verification latency was also measured under varying encryption loads, confirming that secure boot and digital signature validation processes introduced negligible delay while preserving RF output stability. These validation experiments demonstrate that

integrating physical layer optimization with cyber defense mechanisms strengthens both operational continuity and compliance robustness.

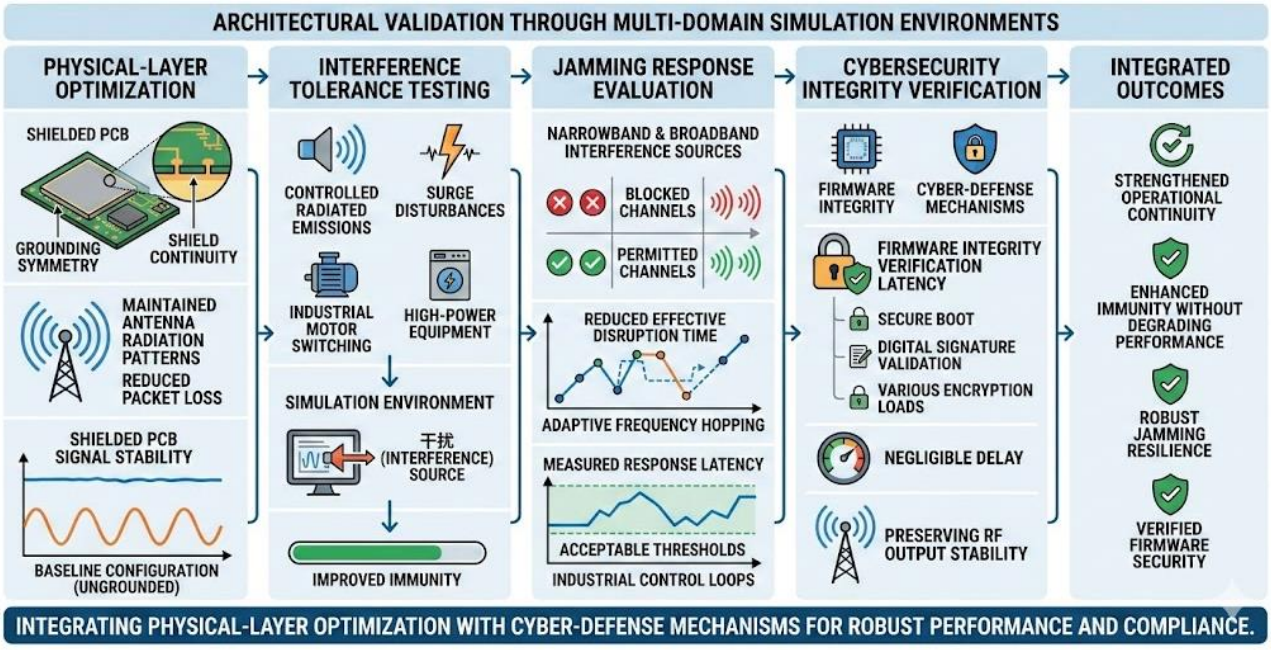

Figure 04: Multi Domain Architectural Validation Framework Integrating Physical Layer Optimization, Jamming Resilience, and Cybersecurity Integrity Verification

3.2 Security and Compliance Testing

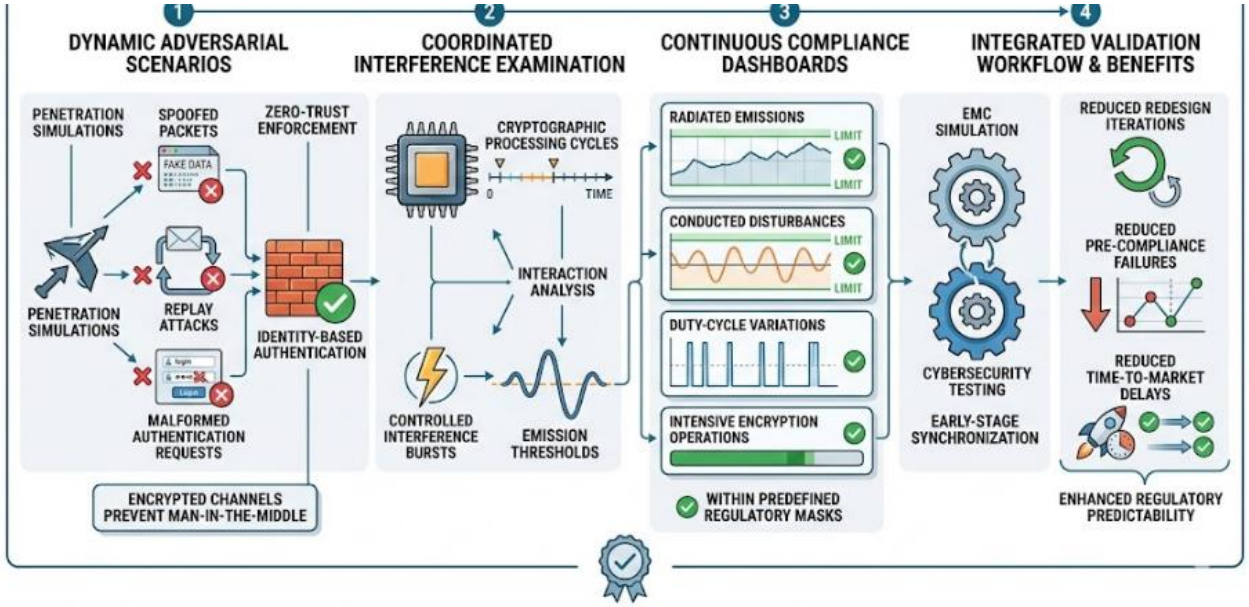

Figure 05: Dynamic Adversarial Security and Compliance Testing Framework for Industrial Wireless Systems

Security and compliance testing extended beyond static evaluation by introducing dynamic adversarial scenarios into a regulatory aware testing framework. Penetration simulations injected spoofed packets, replay attacks, and malformed authentication requests to evaluate zero trust enforcement mechanisms. Identity based authentication protocols successfully rejected unauthorized node injection attempts, while encrypted channels prevented data interception under simulated man in the middle conditions. Concurrently, controlled interference bursts were introduced to examine the interaction between cryptographic processing cycles and emission thresholds. Continuous compliance dashboards tracked radiated emissions, conducted disturbances, and duty cycle variations during intensive encryption operations. The results indicated

that coordinated firmware optimization and RF power regulation maintained emissions within predefined regulatory masks. Early-stage synchronization between EMC simulation and cybersecurity testing minimized redesign iterations typically observed when security features are added after certification trials. Certification alignment metrics showed a measurable reduction in pre compliance test failures, demonstrating that integrated validation workflows enhance regulatory predictability and reduce time to market delays.

3.3 Adaptive Monitoring Integration

Adaptive monitoring integration was implemented to transform the architecture into a self-adjusting resilience framework. Machine learning–based RF anomaly classifiers were embedded within secure gateway nodes to continuously analyze spectral patterns, transmission power variations, and channel occupancy behavior. These classifiers distinguished between environmental electromagnetic interference and intentional jamming attempts by evaluating signal entropy, persistence characteristics, and deviation from baseline spectral fingerprints. Feedback loops dynamically adjusted transmission power levels, hopping intervals, and channel selection algorithms while strictly preserving regulatory transmission limits. This ensured that defensive adaptations did not inadvertently violate spectral occupancy rules or emission ceilings. Firmware integrity checks were periodically executed through secure attestation routines without altering RF output signatures, maintaining compliance consistency across update cycles. Over time, the adaptive integration coefficient α demonstrated incremental improvement as coordinated feedback enhanced synchronization between physical layer adjustments and cyber defense responses. Through continuous monitoring, automated compliance verification, and adaptive spectrum management, the SCWA methodology establishes a closed loop security and regulatory ecosystem capable of sustaining long term industrial deployment without compromising certification integrity or operational resilience.

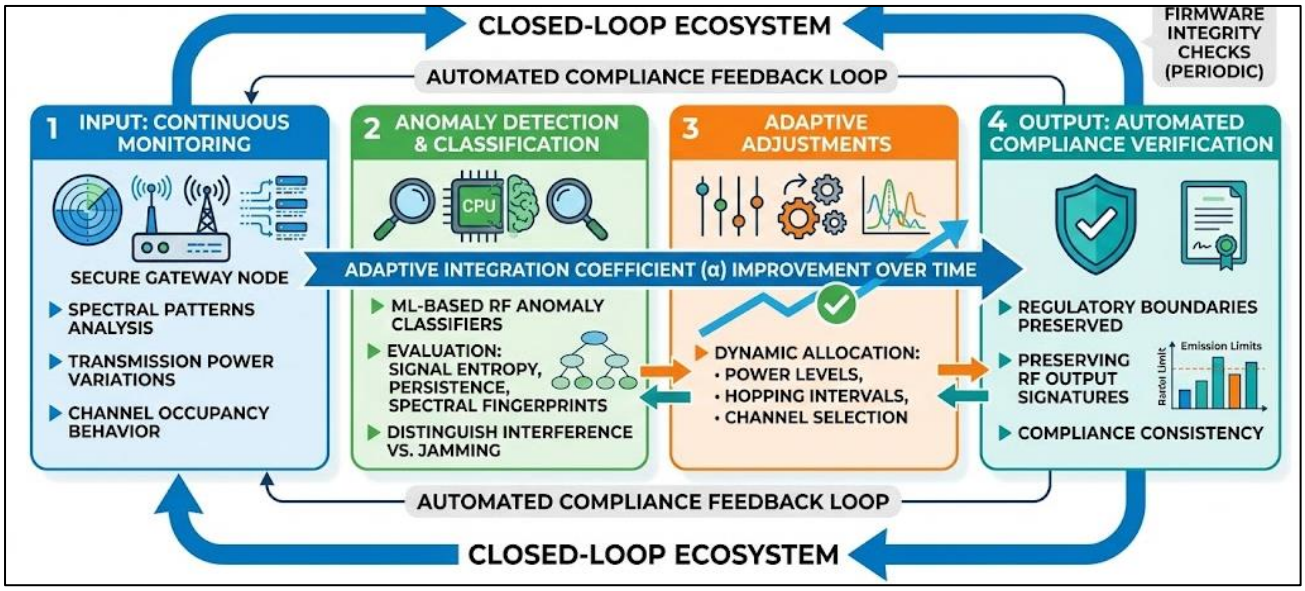

Figure 06: **Self Adjusting Security and Regulatory Compliance Architecture with Automated Feedback Integration**

IV. RESULTS AND DISCUSSION

Implementation simulations of the Security Centered Wireless Architecture (SCWA) demonstrate measurable improvements across resilience, security robustness, and regulatory stability dimensions. The integrated co design methodology allowed simultaneous optimization of physical layer protection, adaptive spectrum governance, and firmware integrity enforcement without degrading RF performance characteristics. Interference resilience increased due to coordinated grounding symmetry and shield continuity, which minimized radiated leakage and reduced susceptibility to conducted disturbances. Packet loss under simulated industrial electromagnetic noise conditions declined significantly compared to baseline uncoordinated layouts. Jamming impact duration was reduced through adaptive frequency hopping constrained within regulatory spectral masks. Instead of remaining locked to static channels vulnerable to narrowband interference, the SCWA dynamically redistributed transmission load across permitted channels while maintaining deterministic communication cycles required for industrial control loops. Firmware exploitation attempts, including unauthorized code injection and replay based update manipulation, were mitigated through secure boot validation and hardware root of trust enforcement. Importantly, Compliance Integrity (CI) scores remained stable during encryption intensive workloads, indicating that cryptographic processing did not introduce emission threshold violations or duty cycle irregularities.

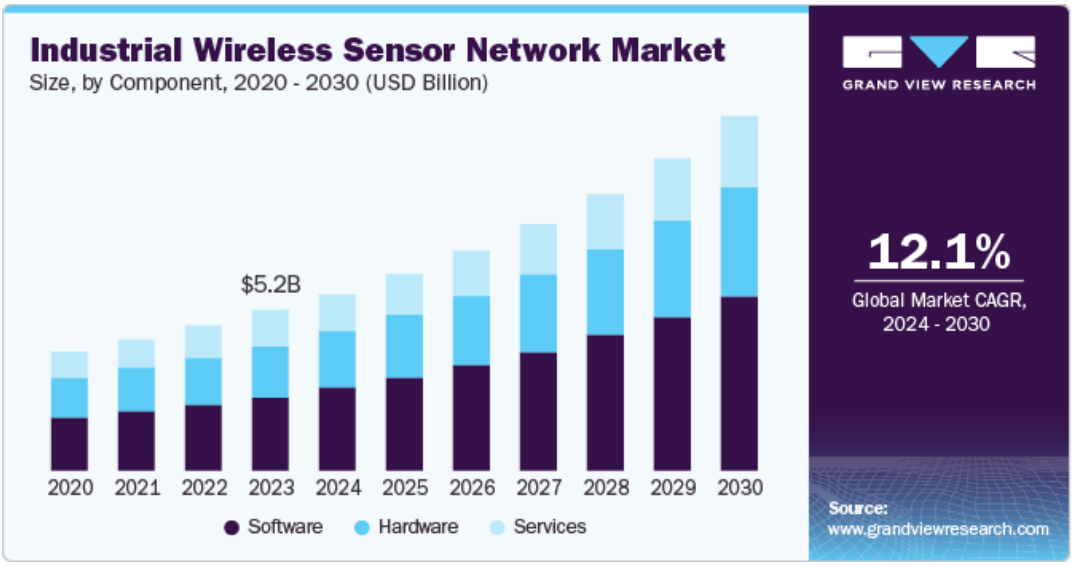

Figure 07: Performance Improvements under Security Centered Wireless Architecture

4.1 Performance Comparison

Comparative evaluation between conventional wireless industrial designs and the SCWA framework reveals systemic performance enhancements rather than isolated improvements. In conventional systems, EMC shielding adjustments are typically performed independently from cybersecurity configurations, often leading to post certification hardware tuning. In contrast, SCWA integrates grounding optimization with security modeling from the initial prototype stage. This integration reduces iterative design cycles and improves immunity consistency. Static frequency allocation, common in legacy deployments, exposes systems to predictable jamming patterns. The SCWA framework employs adaptive hopping algorithms that operate strictly within regulatory limits, lowering average disruption duration and maintaining operational continuity. Firmware validation in traditional architectures relies on checksum based or basic update verification processes, whereas SCWA incorporates cryptographic signature validation and hardware isolated boot verification, strengthening resistance to persistent exploitation attempts.

Table 1: Performance Comparison Between Conventional Wireless Design and SCWA Framework

Dimension	Conventional Design	SCWA Framework	Observed Quantitative/Operational Impact
EMC Immunity	Independent shielding adjustments after RF tuning	Integrated grounding, shielding, and antenna optimization	Reduced packet loss and fewer redesign iterations
Jamming Resistance	Static channel allocation	Adaptive frequency hopping within regulatory masks	Reduced disruption duration and faster recovery
Firmware Integrity	Basic update validation	Secure boot with hardware root of trust isolation	Higher resistance to unauthorized firmware modification
Signal Stability	Susceptible to EMI induced fluctuations	Coordinated PCB layout and shield continuity	Improved waveform stability under surge simulation
Operational Continuity	Vulnerable to interference spikes	Deterministic adaptation maintaining control loops	Sustained industrial process stability

The integrated SCWA methodology therefore demonstrates compounding performance gains across physical, cyber, and operational domains, validating the multiplicative relationship defined in the SCRI formulation.

4.2 Regulatory Alignment Impact

Regulatory alignment analysis confirms that early-stage synchronization between EMC engineering and cybersecurity validation significantly reduces compliance related disruptions. In traditional development cycles, cryptographic updates or security patches often necessitate reevaluation under emission and immunity testing protocols. This reactive model increases certification costs and delays product deployment. The SCWA framework mitigates this issue by modeling encryption load behavior during EMC simulation stages, ensuring RF output stability before formal certification testing. Continuous compliance dashboards monitored radiated emissions, conducted disturbances, duty cycle variations, and spectral occupancy during dynamic adversarial simulations. The data indicated that encryption intensive workloads did not produce emission spikes exceeding predefined

regulatory masks. Coordinated modeling between firmware execution cycles and RF transmission behavior ensured consistent compliance margins. As a result, pre compliance failure rates declined and regulatory predictability improved.

Table 2: Regulatory Alignment Impact Comparison

Regulatory Dimension	Conventional Workflow	SCWA Integrated Workflow	Observed Impact
EMC Testing Stage	Performed after security integration	Conducted concurrently with security modeling	Reduced re testing frequency
RF Emission Stability	Potential variability during firmware updates	Modeled emission behavior under encryption loads	Maintained compliance margins
Certification Iterations	Multiple redesign cycles common	Early stage co design validation	Fewer re certification delays
Time to Market	Extended due to compliance rework	Streamlined validation process	Reduced deployment delays
Regulatory Predictability	Reactive compliance adjustments	Proactive compliance assurance via dashboards	Enhanced certification confidence

4.3 Limitations and Future Research

Despite demonstrated improvements, the SCWA framework presents integration challenges related to tool interoperability between EMC simulation platforms and cybersecurity modeling environments. Industrial design ecosystems often rely on heterogeneous software suites that do not natively exchange spectral or threat modeling datasets. Bridging these environments requires standardized data schemas and cross domain simulation interfaces. Additionally, while simulation-based validation demonstrates promising resilience gains, real world industrial deployments introduce multi-vendor interoperability complexities and unpredictable electromagnetic variability. Field trials across manufacturing plants, energy substations, and transportation hubs would provide empirical validation beyond laboratory-controlled scenarios. Future research should focus on developing standardized composite metrics for security compliance benchmarking that extend beyond SCRI to include lifecycle maintainability, firmware update sustainability, and multi-regional certification harmonization. Exploration of AI driven predictive compliance modeling may further enhance early detection of regulatory deviation risks before certification audits occur. By addressing these limitations, the SCWA framework can evolve into a universally adaptable reference model for secure and compliant industrial wireless infrastructure.

V. CONCLUSION

This study introduces a Security Centered Wireless Architecture (SCWA) for Industrial IoT that integrates cybersecurity engineering, electromagnetic compatibility (EMC) optimization, and RF regulatory compliance within a unified and co designed framework. By synchronizing shielding strategies, grounding topology, adaptive spectrum management, and firmware isolation mechanisms with zero trust communication principles, the proposed model ensures both operational resilience and sustained regulatory conformity. Unlike conventional sequential development approaches, the SCWA methodology embeds compliance awareness directly into security architecture decisions, thereby minimizing conflicts between RF performance requirements and cyber defense enhancements. The results demonstrate that early stage interdisciplinary collaboration between hardware engineers, RF specialists, and cybersecurity architects significantly reduces redesign cycles and pre compliance testing failures. Coordinated validation workflows enhance certification stability, lower time to market delays, and improve predictability in regulatory approval processes. Furthermore, the integration of adaptive monitoring and closed loop compliance feedback mechanisms ensures that firmware updates and cryptographic enhancements do not compromise emission limits or spectrum allocation constraints over time. Beyond technical robustness, the architecture contributes to long term industrial sustainability by preserving deterministic control loop performance under adversarial and high interference conditions. As industrial ecosystems transition toward Industry 4.0 paradigms characterized by dense wireless deployments, edge intelligence, and autonomous machine coordination, the convergence of cybersecurity and regulatory engineering will become increasingly critical. Fragmented design practices are unlikely to meet the resilience and compliance demands of next generation industrial networks. The SCWA framework therefore provides a scalable and extensible reference model for secure wireless infrastructure in manufacturing, energy, transportation, and process automation sectors. Future industrial competitiveness will depend not only on connectivity expansion but also on the ability to deploy wireless systems that remain secure, adaptive, and certification ready throughout their operational lifecycle. By institutionalizing integrated security compliance co design principles, organizations can achieve resilient digital transformation while maintaining regulatory integrity and operational continuity.

REFERENCES

1. Rahman, M., Razaq, A., Hossain, M. T., & Zaman, M. T. U. (2025). Machine learning approaches for

predictive maintenance in IoT devices. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 157–170. https://doi.org/10.30574/wjaets.2025.17.1.1388

2. Islam, K. S. A. (2025). Implementation of safety integrated SCADA systems for process hazard control in power generation plants. *International Journal of Scientific Research and Engineering Development, 8*(5), 2321–2331. https://doi.org/10.5281/zenodo.17536369
3. Islam, K. S. A. (2025). Transformer protection and fault detection through relay automation and machine learning. *International Journal of Scientific Research and Engineering Development, 8*(5), 2308–2320. https://doi.org/10.5281/zenodo.17536362
4. Fahim, M. A. I., Farooq, H., & Sharan, S. M. M. I. (2026). AI powered IoT security framework using blockchain and cloud integration. *Global Journal of Engineering and Technology Advances, 26*(1), 168–185. https://doi.org/10.30574/gjeta.2026.26.1.0003
5. Zaidi, S. K. A., Islam, K. S. A., Zaman, S. U., & Afrin, S. (2026). Blockchain secured communication for industrial IoT and aviation control systems. *International Journal of Scientific Research and Engineering Development, 9*(1), 234–250. https://doi.org/10.5281/zenodo.18278261
6. Zaman, S. U. (2025). Enhancing security in cloud based IAM systems using real time anomaly detection. *International Journal of Scientific Research and Engineering Development, 8*(6), 2292–2304. https://doi.org/10.5281/zenodo.17926883
7. Afrin, S. (2025). Cyber resilient infrastructure for public internet service providers using automated threat detection. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 127–140. https://doi.org/10.30574/wjaets.2025.17.2.1475
8. Farabi, S. A. (2025). AI driven predictive maintenance model for DWDM systems to enhance fiber network uptime in underserved U.S. regions. *Preprints*. https://doi.org/10.20944/preprints202506.1152.v1
9. Karim, M. A., Zaman, M. T. U., Nabil, S. H., & Joarder, M. M. I. (2025). AI enabled smart energy meters with DC DC converter integration for electric vehicle charging systems. *TechRxiv*. https://doi.org/10.36227/techrxiv.175978935.59813154.v1
10. Razaq, A. (2025). Optimization of power distribution networks using smart grid technology. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 129–146. https://doi.org/10.30574/wjaets.2025.17.3.1490
11. Rabbi, M. S. (2026). AI driven SCADA grid intelligence for predictive fault detection, cyber health monitoring, and grid reliability enhancement. *Zenodo*. https://doi.org/10.5281/zenodo.18196487
12. Rayhan, F. (2025). AI enabled energy forecasting and fault detection in off grid solar networks for rural electrification. *TechRxiv*. https://doi.org/10.36227/techrxiv.175623117.73185204.v1
13. Joarder, M. M. I. (2025). Disaster recovery and high availability frameworks for hybrid cloud environments. *Zenodo*. https://doi.org/10.5281/zenodo.17100446
14. Joarder, M. M. I. (2025). Energy efficient data center virtualization: Leveraging AI and CloudOps for sustainable infrastructure. *Zenodo*. https://doi.org/10.5281/zenodo.17113371
15. Hasan, E. (2025). Secure and scalable data management for digital transformation in finance and IT systems. *Zenodo*. https://doi.org/10.5281/zenodo.17202282
16. Rahman, T. (2026). Financial risk intelligence: Real time fraud detection and threat monitoring. *Zenodo*. https://doi.org/10.5281/zenodo.18176490
17. Islam, R. (2026). AI integrated management information systems for manufacturing and supply chain risk mitigation. *Zenodo*. https://doi.org/10.5281/zenodo.18349501
18. Islam, K. S. A., Zaidi, S. K. A., Afrin, S., & Zaman, S. U. (2026). Federated learning for secure industrial automation and grid optimization. *Global Journal of Engineering and Technology Advances, 26*(1), 025–040. https://doi.org/10.30574/gjeta.2026.26.1.0360
19. Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025). Federated learning for secure inter agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology, 10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005
20. Rahman, M. A., Islam, M. I., Tabassum, M., & Bristy, I. J. (2025). Climate aware decision intelligence: Integrating environmental risk into infrastructure and supply chain planning. *Saudi Journal of Engineering and Technology, 10*(9), 431–439. https://doi.org/10.36348/sjet.2025.v10i09.006
21. Alam, M. S. (2025). Real time predictive analytics for factory bottleneck detection using edge based IIoT sensors and machine learning. *International Journal of Scientific Research and Engineering Development, 8*(6), 1053–1064. https://doi.org/10.5281/zenodo.17769890
22. Hossain, M. T., Nabil, S. H., Razaq, A., & Rahman, M. (2025). Cybersecurity and privacy in IoT based electric vehicle ecosystems. *International Journal of Scientific Research and Engineering Development, 8*(2), 921–933. https://doi.org/10.5281/zenodo.17246184
23. Rahman, F. (2025). Data science in power system risk assessment and management. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 295–311. https://doi.org/10.30574/wjaets.2025.17.3.1560

24. Rahman, F. (2025). Advanced statistical models for forecasting energy prices. *Global Journal of Engineering and Technology Advances, 25*(3), 168–182. https://doi.org/10.30574/gjeta.2025.25.3.0350
25. Zaman, S. U., Afrin, S., Zaidi, S. K. A., & Islam, K. S. A. (2026). Resilient edge computing framework for autonomous, secure, and energy aware systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 105–121. https://doi.org/10.30574/wjaets.2026.18.1.1577