INTERNATIONAL JOURNAL OF BUSINESS AND ECONOMICS INSIGHTS

Volume: 5; **Issue:** 3
Pages: 494– 522
Accepted: 14 August 2025
Published: 07 October 2025

MODBUS/DNP3 OVER TCP/IP IMPLEMENTATION ON TMDSCNCD28388D AND ARDUINO WITH SIMULINK HMI FOR IOT-BASED CYBERSECURE ELECTRICAL SYSTEMS

Waladur Rahman[1]; Jabed Hasan Tarek[2];

[1]. *Phillip M. Drayer Department of Electrical Engineering, Lamar University, Beaumont, Texas, USA; Email:* w.rifat99@gmail.com

[2]. *Phillip M. Drayer Department of Electrical Engineering, Lamar University, Beaumont, Texas, USA; Email:* *jabedhasan932@gmail.com*

Doi: 10.63125/8e9cm978
This work was peer-reviewed under the editorial responsibility of the IJBEI, 2025

Abstract

The implementation of Modbus and DNP3 (Distributed Network Protocol) over TCP/IP represents a significant advancement in integrating industrial communication standards with modern IoT-based control and cybersecurity frameworks. This study presents a dual-platform experimental implementation of these protocols using the Texas Instruments TMDSCNCD28388D controlCARD and the Arduino Uno, each interfaced with a Simulink-based Human–Machine Interface (HMI). The system architecture enables seamless data exchange between field devices and supervisory applications over Ethernet, supporting real-time monitoring, remote actuation, and secure data acquisition. The TMDSCNCD28388D, equipped with a dual-core C2000 microcontroller and integrated F28388D processor, provides deterministic control for industrial nodes, while the Arduino Uno serves as a low-cost alternative for small-scale IoT testbeds. Both implementations employ Simulink models for system design, simulation, and code generation, ensuring modularity and platform independence. The study emphasizes the integration of industrial automation and IoT protocols within a cybersecurity-aware framework. A layered encryption model was incorporated into TCP/IP communication to evaluate data confidentiality, integrity, and resilience against common cyber threats such as spoofing and denial-of-service attacks. The Simulink HMI acts as both a visualization and command layer, enabling real-time supervisory control and anomaly detection through embedded MATLAB scripts and dashboard logic. Experimental results demonstrate high communication reliability, with Modbus achieving faster request–response cycles under low-load conditions, while DNP3 exhibited greater robustness against packet loss and network interference. The hybrid approach validates the feasibility of deploying standardized SCADA protocols in distributed IoT environments, supporting industrial cyber-physical systems where interoperability and security are critical. This work contributes to the evolving field of cyber-secure industrial automation by demonstrating an end-to-end methodology for implementing Modbus/DNP3 over TCP/IP using embedded microcontrollers and model-based design tools. The outcomes highlight the importance of integrating communication protocols, cybersecurity measures, and model-based engineering to develop resilient, intelligent, and scalable industrial IoT architectures.

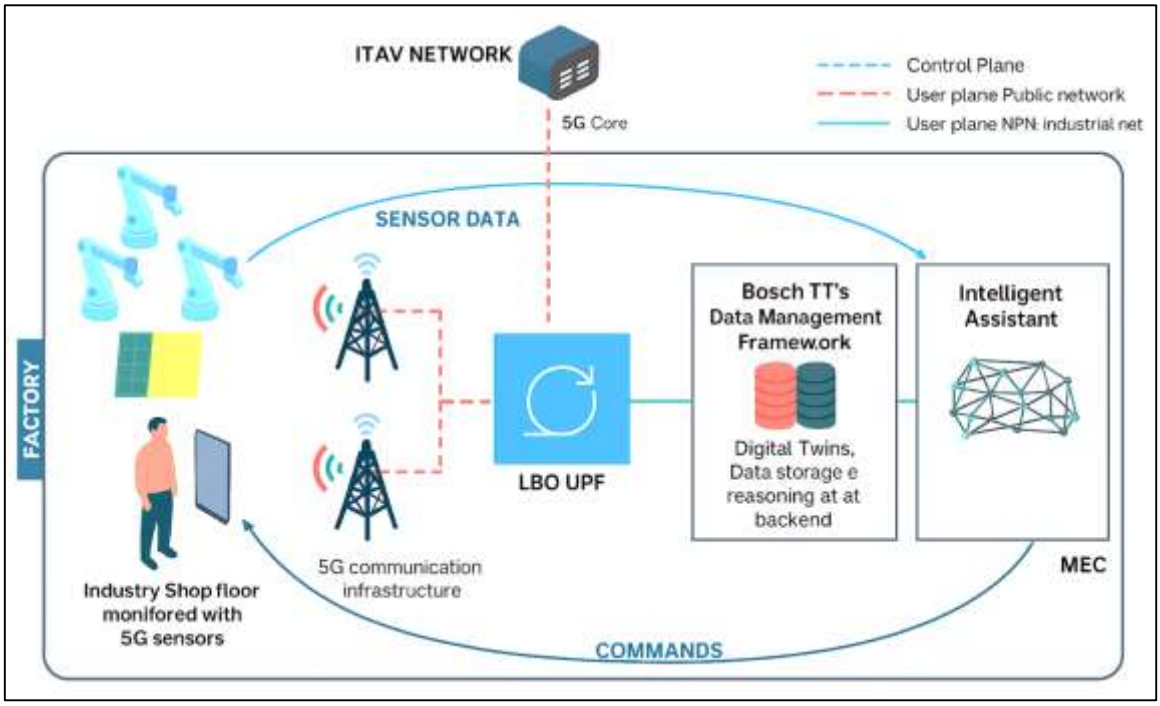
Keywords

Modbus/TCP; DNP3 Protocol; Simulink-Based HMI; Industrial Internet of Things (IIoT); Cybersecurity; SCADA Systems;

INTRODUCTION

The Internet of Things (IoT) represents a paradigm wherein physical devices are interconnected through networked infrastructures, enabling intelligent communication, automation, and data analytics within cyber-physical environments (Barbero et al., 2011). In industrial and energy sectors, IoT technologies underpin the emergence of smart grids, microgrids, and intelligent substations, which integrate distributed energy resources and advanced communication protocols for real-time system control (Liang et al., 2017). The Industrial Internet of Things (IIoT) extends this framework to encompass automation systems that merge operational technology (OT) with information technology (IT), thus facilitating interconnected energy assets, control devices, and monitoring tools (Laghari et al., 2021). Internationally, countries such as Germany, Japan, and the United States have prioritized industrial digitization through initiatives like Industry 4.0 and the Smart Manufacturing Leadership Coalition (Bedhief et al., 2016). The expansion of IoT-based control systems across critical energy infrastructures underscores the need for standardized, interoperable, and secure communication mechanisms capable of sustaining reliable energy transmission, distribution, and automation functions (Atzori et al., 2011). This convergence of IoT and industrial automation demands robust communication protocols that ensure interoperability between heterogeneous devices and adherence to cybersecurity standards that protect operational continuity in globally networked environments (Zhang et al., 2014).

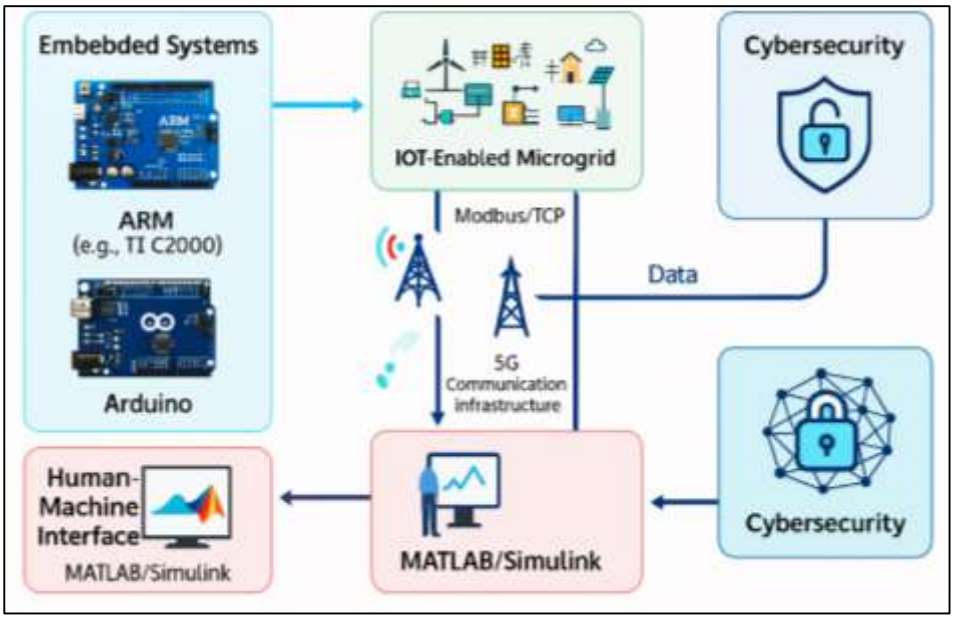
Figure 1: IOT-based Cybersecure Electrical System



Communication protocols such as Modbus and the Distributed Network Protocol (DNP3) have historically served as the backbone for supervisory control and data acquisition (SCADA) systems within electrical utilities and manufacturing plants (Batcha & Geetha, 2020). Modbus, introduced by Modicon in 1979, remains one of the most widely implemented open protocols for communication between programmable logic controllers (PLCs) and field devices (Goudarzi et al., 2022). It facilitates master–slave or client–server communication models that transmit register and coil data efficiently within deterministic control environments. Conversely, DNP3 was developed in the 1990s to enhance interoperability in electric utility automation by enabling asynchronous data reporting, time stamping, and event-driven messaging. Both protocols have evolved into TCP/IP variants—Modbus/TCP and DNP3/TCP—to align with Ethernet-based communication architectures. These standards provide reliability and compatibility with modern IoT platforms and cloud infrastructures while maintaining the determinism required by industrial control processes. Internationally, the deployment of Modbus and DNP3 over TCP/IP aligns with the broader transition to IEC 61850 and IEEE 1815 frameworks,

which emphasize seamless device integration, high data throughput, and flexible topology management for smart grid systems (Zhang et al., 2014). Thus, integrating Modbus and DNP3 into embedded systems and IoT nodes serves as a key step toward achieving global harmonization in electrical communication standards.

Figure 2: IoT-Enabled Microgrid



The interconnection of field devices through IoT-enabled communication channels introduces substantial cybersecurity risks, including data tampering, unauthorized command injection, and denial-of-service (DoS) attacks (Batcha & Geetha, 2020; Rezaul, 2021). Traditional industrial protocols such as Modbus and DNP3 were not originally designed with encryption or authentication capabilities, leaving them vulnerable to exploitation when exposed to TCP/IP networks (Danish & Zafor, 2022; Goudarzi et al., 2022). In response, international cybersecurity standards—such as IEC 62443, NIST SP 800-82, and ISO/IEC 27019—have been developed to address vulnerabilities in energy automation environments (Danish & Kamrul, 2022; Sharma & Wang, 2020). Research demonstrates that integrating lightweight cryptographic primitives and network-layer firewalls into embedded controllers enhances protection without significantly affecting real-time performance. Additionally, layered security architectures employing intrusion detection systems (IDS) and anomaly-based monitoring provide situational awareness across interconnected devices. Cybersecure IoT architectures are therefore foundational for protecting distributed energy resources, ensuring resilience in power grids, and maintaining data integrity for supervisory control systems. The convergence of IoT communication and cybersecurity within SCADA environments necessitates both protocol-level defenses and adaptive intelligence mechanisms that can be implemented efficiently in resource-constrained embedded systems (Jahid, 2022).

Embedded systems form the operational core of industrial automation, enabling deterministic execution of control tasks, sensor interfacing, and data acquisition (Guo & Li, 2012; Ismail, 2022). Devices such as the Texas Instruments TMDSCNCD28388D, based on the C2000 Delfino microcontroller, exemplify high-performance platforms capable of executing real-time control and TCP/IP-based communication simultaneously. The use of real-time operating systems (RTOS) and dual-core architectures enhances the deterministic scheduling of network and computation tasks (Hossen & Atiqur, 2022; Singh et al., 2014). When combined with microcontroller-based devices like Arduino, such systems enable heterogeneous networks of industrial nodes that can emulate the distributed nature of smart microgrids (Liang et al., 2017; Kamrul & Omar, 2022). Implementing Modbus/TCP and DNP3/TCP on these platforms supports modular and interoperable communication schemes between sensors, actuators, and supervisory hosts (Laghari et al., 2021; Razia, 2022). Internationally, embedded control platforms are essential in building localized energy automation

systems for developing regions, providing scalable and cost-effective solutions for industrial communication research and deployment (Goudarzi et al., 2022; Sadia, 2022). This integration enables deterministic performance for mission-critical energy processes while providing flexibility in testing security, latency, and protocol reliability within experimental and operational settings (Danish, 2023).

The motivation behind developing a Modbus/DNP3 over TCP/IP implementation on the TMDSCNCD28388D and Arduino platforms stems from the urgent global demand for secure, interoperable, and real-time communication within industrial and energy automation systems (Lyu et al., 2019; Arif Uz & Elmoon, 2023). As IoT continues to transform traditional SCADA architectures, the necessity for systems capable of withstanding cyber threats while maintaining operational reliability has intensified. Many legacy devices in substations and industrial plants still rely on insecure fieldbus networks, underscoring the importance of practical research that bridges traditional automation protocols with modern network security frameworks. The integration of MATLAB/Simulink-based HMI and embedded controllers creates a reproducible environment for modeling, testing, and validating communication and cybersecurity functions under real-time constraints. Internationally, the move toward digital substations and IoT-driven power systems demands adaptable hardware–software co-design methodologies that ensure both protocol compliance and cyber resilience. Therefore, this project situates itself within the global research trajectory of cybersecure IoT-based energy automation, emphasizing practical implementation of Modbus/TCP and DNP3/TCP communication within embedded control architectures. The main objective of this research is to develop and validate a functional IoT-based cybersecure communication framework that integrates Modbus/TCP and DNP3/TCP protocols on the TMDSCNCD28388D controlCARD and Arduino platforms, interfaced with a MATLAB/Simulink-based HMI for real-time data monitoring and control. The project aims to establish a scalable and secure experimental model for smart grid and microgrid applications by demonstrating reliable, real-time communication between embedded controllers and supervisory systems. It focuses on achieving interoperability between heterogeneous hardware, maintaining deterministic performance under networked conditions, and embedding lightweight cybersecurity mechanisms such as authentication, data integrity verification, and intrusion detection within the protocol stack. Additionally, the objective includes creating a dynamic HMI environment capable of visualizing live data exchange, simulating control actions, and detecting anomalous network behavior, thereby providing a complete hardware–software testbed that supports secure industrial automation, control validation, and educational research in IoT-based energy systems.

LITERATURE REVIEW

The advancement of IoT-based industrial automation has prompted a global re-evaluation of communication protocols, cybersecurity strategies, and embedded system architectures used in smart energy infrastructures. The literature on supervisory control and data acquisition (SCADA) systems, IoT-enabled microgrids, and real-time communication protocols—such as Modbus and DNP3—reveals a consistent effort to achieve interoperability, scalability, and resilience in increasingly complex cyber-physical systems. Early industrial communication frameworks emphasized deterministic control and wired reliability, whereas modern systems now require Internet-based connectivity, cloud data integration, and adaptive cybersecurity features suitable for distributed environments. As such, reviewing existing studies is essential to understand the technical evolution, vulnerabilities, and mitigation approaches associated with TCP/IP-based Modbus and DNP3 implementations within embedded controllers like the TMDSCNCD28388D and Arduino platforms. This literature review systematically organizes research findings into key thematic domains: (1) industrial communication protocols and their TCP/IP evolution; (2) cybersecurity frameworks for SCADA and IoT systems; (3) embedded system design for real-time control; (4) human–machine interface (HMI) integration in industrial networks; (5) IoT-enabled microgrid architectures and interoperability; and (6) experimental validation approaches for secure communication frameworks. Each section provides a critical synthesis of prior works, identifies performance and security challenges, and contextualizes the necessity of an integrated approach combining embedded platforms, secure communication, and HMI-based visualization. The review serves as the theoretical foundation for the present implementation study, situating it within the broader global discourse on industrial digital transformation, energy automation, and cybersecurity standardization.

Standardization of Modbus and DNP3

The evolution of industrial communication protocols such as Modbus and the Distributed Network Protocol (DNP3) reflects a critical shift from isolated, proprietary automation systems toward standardized, interoperable industrial networks. Modbus, introduced by Modicon in 1979, emerged as one of the first openly published communication protocols designed for programmable logic controllers (PLCs), offering a simple master–slave communication model for transmitting data across field devices (Cecchinel et al., 2014). Early implementations focused on serial communication using RS-232/RS-485 channels, facilitating deterministic exchanges between controllers and remote terminals in manufacturing environments (Hossain et al., 2023; Perera et al., 2013). Similarly, DNP3 was developed in the early 1990s under the IEEE 1815 framework to address interoperability among substation and SCADA systems, especially within electric utility networks. DNP3 introduced object-based data representation (Hasan, 2023), time-stamping, and unsolicited messaging to enhance real-time data reliability and asynchronous reporting. These developments marked a departure from rigid vendor-dependent designs, setting the foundation for open communication architectures that could span across vendors, devices, and industries. As industrial automation expanded into the energy, oil, and manufacturing sectors, the need for common communication standards became paramount to ensure compatibility and reliability across geographically distributed control systems (Shoeb & Reduanul, 2023; Radoglou-Grammatikis et al., 2021). The historical standardization of Modbus and DNP3 thus provided the structural blueprint for modern supervisory control and data acquisition (SCADA) interoperability, enabling consistent data framing, addressing schemes, and transport mechanisms across multiple generations of industrial devices.

The Protocol Throughput Efficiency represents the effectiveness of a communication protocol in transmitting usable data relative to its total transmission capacity, including overhead. It quantifies how efficiently a protocol utilizes the available bandwidth by comparing the size of the actual transmitted data to the total data sent, which includes protocol headers, checksums, and acknowledgments. Mathematically, throughput efficiency is expressed as:

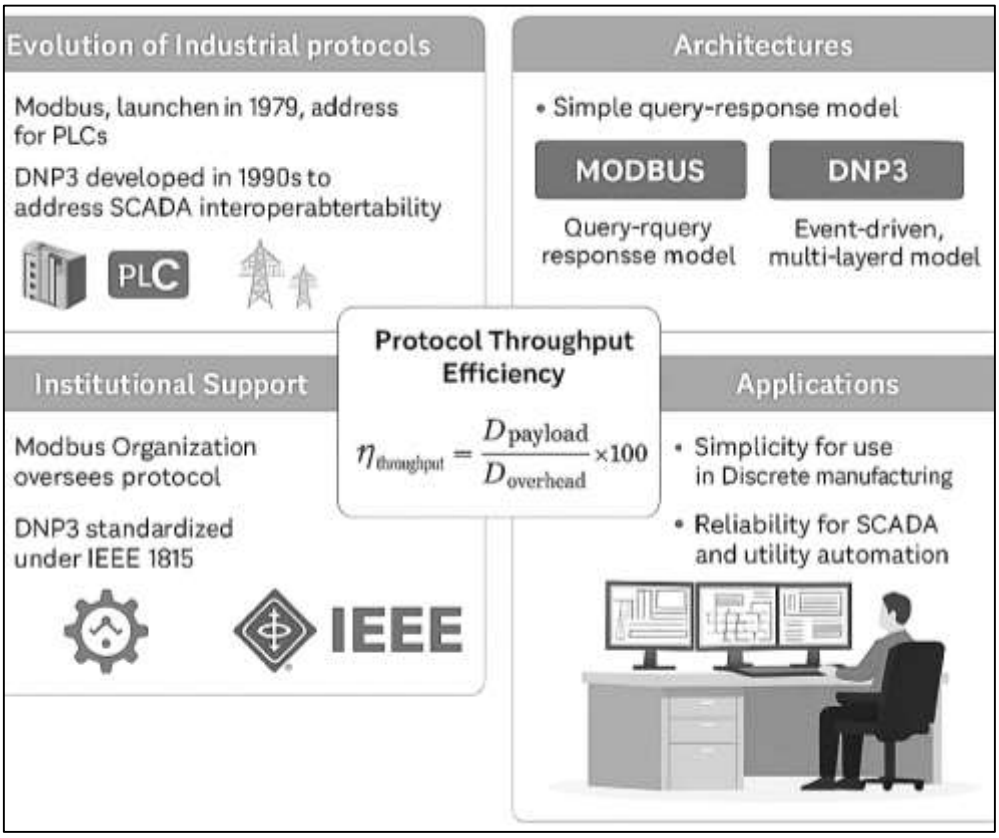
$$\eta_{\text{throughput}} = \frac{D_{\text{payload}}}{D_{\text{payload}} + D_{\text{overhead}}} \times 100\%$$

This parameter is critical in evaluating communication performance, especially in industrial network protocols such as Modbus and DNP3. Modbus, with its lightweight frame structure and minimal header information, typically exhibits higher throughput efficiency, making it suitable for applications where low latency and simple polling communication dominate. In contrast, DNP3 incorporates more extensive framing and authentication structures to support event-driven communication and cybersecurity features, which increase overhead and slightly reduce throughput efficiency. Nonetheless, DNP3's additional data ensures reliability, integrity, and security in complex supervisory control and data acquisition (SCADA) systems (Batcha & Geetha, 2020; Mubashir & Jahid, 2023). Therefore, while Modbus achieves superior raw throughput due to simplicity, DNP3 provides a more balanced trade-off between efficiency, resilience, and secure data handling within critical infrastructure networks.

Modbus and DNP3 possess distinct architectural and operational frameworks that define their suitability for specific industrial environments, yet both have undergone standardization processes that emphasize interoperability, determinism, and reliability. Modbus follows a simple query–response architecture, where a single master device polls multiple slave devices for data using well-defined function codes and addressing mechanisms (Guo & Li, 2012; Razia, 2023). Its standardization under Modbus Application Protocol (MAP) guidelines allows it to operate consistently over different transport layers, including Modbus RTU, ASCII, and TCP/IP variants (Perera et al., 2013; Reduanul, 2023). In contrast, DNP3 employs an event-driven model with multi-layered architecture comprising data link, transport, and application layers, which supports unsolicited messaging and sequence-of-events reporting. DNP3's object-oriented structure allows complex data types to be exchanged efficiently while maintaining time synchronization across distributed devices, a feature particularly critical in energy automation systems. The standardization of DNP3 under IEEE Std 1815 ensures consistency in command execution, error handling, and message sequencing across vendors, making it

the de facto communication standard for North American and increasingly international SCADA networks (Guo & Li, 2012; Sadia, 2023). Both protocols provide mechanisms for error checking, data integrity verification, and network diagnostics, though DNP3's layered design provides greater resilience against communication disruptions (Lu et al., 2013; Sanjai et al., 2023). Collectively, their technical architectures illustrate the evolutionary balance between simplicity and sophistication, allowing Modbus to dominate in small-scale industrial control, while DNP3 serves as the standard for complex, event-driven utility automation.

Figure 3: Standardization of Modbus and DNP3



The formal standardization of Modbus and DNP3 by international regulatory and technical bodies has been central to ensuring interoperability and global adoption in industrial communication systems. Modbus was institutionalized through the Modbus Organization, which oversees specification maintenance, interoperability certification, and protocol extensions that ensure backward compatibility (Danish & Zafor, 2024; Volkova et al., 2019). Its open-access model accelerated adoption across manufacturing, building automation, and distributed energy systems by allowing manufacturers to integrate Modbus support without licensing barriers. In parallel, DNP3 achieved formal recognition under IEEE Standard 1815, ensuring a rigorous definition of communication functions, message objects, and transport mechanisms for supervisory control (Jahid, 2024a). The standardization process incorporated field feedback from the electric utility sector, reflecting operational requirements such as time synchronization, unsolicited event reporting, and fail-safe mechanisms. Institutions such as the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE) have also promoted cross-protocol harmonization efforts by aligning DNP3 with IEC 61850 and IEC 60870-5-104 frameworks, further facilitating interoperability between substation devices, protective relays, and remote terminal units (Jahid, 2024b; Siniosoglou et al., 2021). These institutionalized standards collectively ensure that Modbus and DNP3 maintain uniformity in application across industries, contributing to robust, reliable, and vendor-neutral industrial ecosystems. The institutional support from standardization bodies guarantees that these protocols remain benchmarks for industrial data exchange, bridging legacy infrastructures and contemporary

Ethernet-based communication architectures across global automation systems (Ismail, 2024; Volkova et al., 2019).

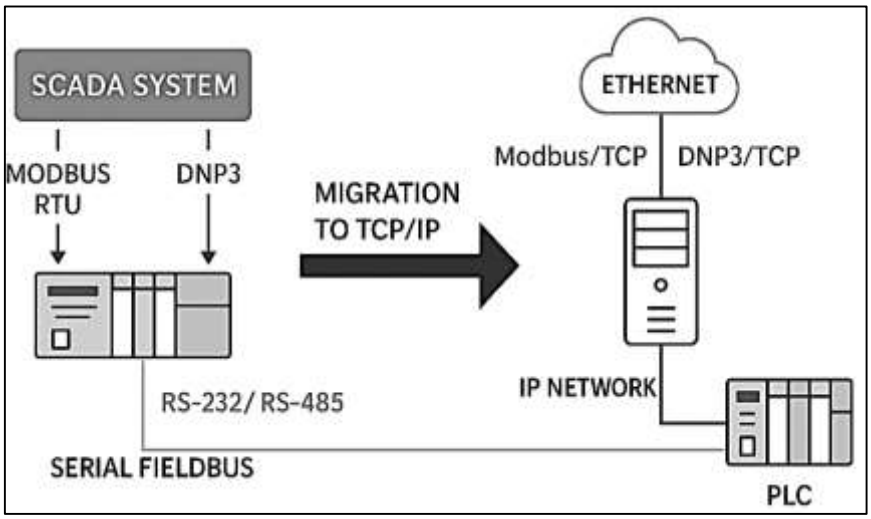
The standardization of Modbus and DNP3 has played an essential role in ensuring interoperability and reliability in complex, geographically dispersed industrial control systems. Modbus's simplicity and deterministic timing make it widely adopted in discrete manufacturing and process industries, whereas DNP3's event-based reporting and hierarchical data organization are suited for power transmission, distribution, and substation automation (Mesbaul, 2024; Siniosoglou et al., 2021). Their coexistence within standardized frameworks allows seamless data exchange between heterogeneous devices, ensuring that SCADA systems maintain operational integrity across diverse industrial sectors (Lu et al., 2013; Omar, 2024). Through their standardized implementations over TCP/IP, these protocols have gained global relevance in integrating legacy control networks with modern IoT-based infrastructures. The reliability of Modbus and DNP3 communications has been verified through numerous case studies demonstrating their resilience under harsh industrial environments, including electromagnetic interference, variable latency, and packet loss. The adoption of TCP/IP variants has further enhanced data accessibility, enabling real-time analytics, cloud interfacing, and integration with supervisory systems such as HMIs and energy management platforms. Additionally, their standardized structures enable uniform diagnostic procedures, consistent fault handling, and predictable network behavior across distributed energy systems. The international acceptance of these protocols as de facto standards within the smart grid ecosystem underscores their enduring importance as foundational communication mechanisms, ensuring that industrial control systems remain interoperable, scalable, and functionally consistent across global applications.

Migration to TCP/IP-Based Communication

The migration of industrial communication from serial fieldbuses to Ethernet and TCP/IP has been driven by the need for scalable addressing, routability across large geographic footprints, and integration with enterprise IT services that handle monitoring, logging, and analytics. Early SCADA deployments prioritized deterministic serial links such as RS-232/RS-485 for Modbus RTU and point-to-point radio for legacy DNP3, yet expanding asset counts and multi-vendor ecosystems introduced interoperability constraints that IP networking addressed through standardized stacks, ubiquitous hardware, and mature management tooling (Liu et al., 2023) Utilities and industrial operators adopted IP to leverage switched Ethernet bandwidth, VLAN segmentation, QoS tagging, and L3 routing, which supported remote substations and distributed plants without bespoke bridging arrangements (Rezaul & Hossen, 2024). Research characterizes this shift as an OT/IT convergence, where operational technology requires the same addressability and maintainability associated with enterprise networks, while maintaining real-time constraints for protection and control. Standardization efforts around IEC 61850 and IEEE 1815 created a technical context in which Modbus/TCP and DNP3/TCP operated alongside object-oriented or model-based utility protocols, facilitating vendor-neutral integration within substations and feeders. Time-Sensitive Networking (TSN) and Ethernet determinism studies further documented bounded latency and low-jitter performance under controlled topologies, addressing long-standing skepticism that best-effort Ethernet could support protection-adjacent telemetry under engineered conditions (Lu et al., 2013; Momena & Praveen, 2024). In parallel, cybersecurity guidance such as NIST SP 800-82 and IEC 62443 framed IP migration as an opportunity to adopt standardized controls—network segmentation, authenticated remote access, and protocol whitelisting—within architectures already familiar to IT administrators. Collectively, these drivers positioned TCP/IP as a practical transport for Modbus and DNP3 where routability, manageability, and cross-domain integration were prioritized alongside engineered real-time performance.

The engineering literature documents precise mappings from legacy frames to client–server transactions over TCP sockets, analyzing overhead, session persistence, and congestion behavior. For Modbus/TCP, the Modbus Application Protocol encapsulates function codes within an MBAP header that replaces serial CRC with a transaction identifier, simplifying error handling and enabling concurrent outstanding requests from multiple clients under a single server endpoint (Mackiewicz, 2006; Modbus Organization, 2012). DNP3/TCP retains link-layer semantics, sequence control, and object groups, adding reliable transport semantics through TCP while preserving event-driven reporting and time-stamping central to utility operations (Muhammad, 2024; Sosnovskiy et al., 2021).

Figure 4: Migration to TCP/IP-Based Communication



Controlled experiments compare serial and Ethernet performance, noting that switched Gigabit links reduce serialization delay and allow tighter polling intervals, whereas shared media or congested uplinks introduce queuing variability that requires QoS and traffic engineering. Studies evaluate keep-alive intervals, socket reuse (Noor et al., 2024), and Nagle's algorithm interactions, recommending configuration that avoids coalescing control bytes in low-latency command paths. Redundancy mechanisms such as PRP/HSR (IEC 62439-3) provide zero-time recovery at Layer-2 for protection-critical paths, complementing RSTP/MSTP and IP-layer routing convergence in multi-subnet utility backbones. TSN features—time-aware shaping and frame preemption—appear in lab results demonstrating bounded latency for mixed traffic classes, enabling co-existence of SCADA polling, synchrophasor streaming, and engineering access on the same fabric under properly defined schedules (Abdul, 2025; Dimolianis et al., 2021). Across these reports, determinism emerges from engineered network design rather than protocol idiosyncrasies alone, with VLAN isolation, QoS prioritization, and bounded hop counts correlating with stable application-layer jitter for Modbus/TCP and DNP3/TCP exchanges.

Cybersecurity in Industrial IoT and SCADA Networks

Cybersecurity in Industrial Internet of Things (IIoT) and supervisory control and data acquisition (SCADA) networks centers on safeguarding cyber-physical processes that govern energy, manufacturing, water, and transportation assets. Research characterizes these environments by deterministic control loops, long-lived assets, and strict safety constraints, all of which complicate conventional IT security practices (Elmoon, 2025a; Sosnovskiy et al., 2021). The migration from isolated serial links to routable Ethernet/TCP/IP increased exposure through addressability, service discoverability, and remote maintenance pathways that adversaries can exploit. Studies catalog prominent attack classes against control networks, including command/parameter tampering, replay and out-of-sequence messaging, forced topology changes, firmware subversion, and denial-of-service at field, gateway, and historian tiers. Empirical analyses of real incidents and red-team exercises show that weak authentication, shared credentials, flat Layer-2 topologies, and unmanaged remote access remain frequent root causes (Elmoon, 2025b). In power systems, timing-sensitive impacts arise when telemetry falsification distorts state estimation or when actuator commands modify protection settings, with consequences amplified by automatic generation control and distribution automation. Traffic characterizations reveal highly periodic polling and narrow value ranges, properties that aid anomaly detection but also enable low-and-slow evasion when attackers mimic expected rhythms (Hozyfa, 2025). Across studies, an enduring observation is that operational constraints—availability, deterministic latency, and safety—shape feasible defense postures and require controls that align with process reliability rather than pure confidentiality priorities. This literature situates IIoT/SCADA risk not as an extension of enterprise IT alone but as a field in which network behavior, protocol semantics,

and plant physics co-determine cyber exposure (Jahid, 2025a, 2025b).

TMDSCNCD28388D and C2000 Delfino MCU Platform

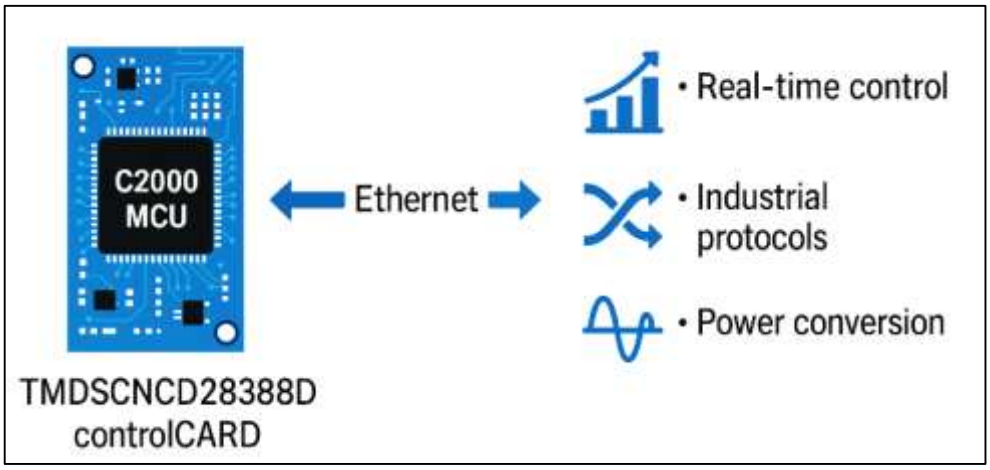
The Texas Instruments TMDSCNCD28388D controlCARD, built on the C2000 Delfino F28388D microcontroller unit (MCU), represents a class of high-performance embedded processors designed specifically for real-time industrial and energy applications. The literature describes the C2000 platform as a deterministic digital signal controller architecture that bridges the performance gap between microcontrollers and DSPs by integrating floating-point processing units, trigonometric accelerators, and high-resolution PWM modules optimized for control systems (Alam, 2025). Studies emphasize its tri-core configuration—two C28x CPUs and one Cortex-M4 core—that enables the concurrent execution of real-time control loops, communication tasks, and diagnostic routines without mutual interference. Researchers have documented how this architecture supports the simultaneous operation of industrial communication protocols (Ethernet, CAN, and SPI) alongside time-critical inverter and motor-control operations (Masud, 2025; Arman, 2025). The integration of a programmable real-time unit (PRU) and hardware accelerators facilitates deterministic scheduling in energy and automation applications that demand sub-millisecond latency. The controlCARD form factor enhances modularity, allowing the TMDSCNCD28388D to serve as a drop-in controller across diverse evaluation boards, thereby promoting reproducible experimentation in both research and industrial environments (Jakaria et al., 2025; Mohaiminul, 2025; Siniosoglou et al., 2021). The literature converges on the characterization of this platform as an ideal prototype environment for embedded control, where multi-core partitioning and deterministic task scheduling enable parallel computation of control algorithms, sensor acquisition, and communication stacks within energy automation systems.

The C2000 Delfino MCU platform's integration with real-time communication stacks represents a significant step in the evolution of cyber-physical systems. The TMDSCNCD28388D supports Ethernet and TCP/IP through its onboard Ethernet Media Access Controller (EMAC) and PHY, enabling direct communication without external network processors (Mominul, 2025; Rezaul, 2025; Najafabadi et al., 2015). Studies in embedded networking confirm that deterministic Ethernet implementations based on the Delfino platform maintain bounded latency and minimal jitter even when processing high-frequency Modbus/TCP or DNP3/TCP traffic. This stability arises from optimized interrupt management and DMA-driven buffer transfers that reduce CPU overhead in high-speed data exchanges. The literature notes that integrating industrial protocols with the C2000 MCU is achieved through TI's real-time control suite, which includes libraries and drivers conforming to IEC 61850 and IEEE 1815 communication standards (Chavez et al., 2019; Rezaul & Rony, 2025; Hasan, 2025). This facilitates multi-protocol interoperability—Modbus for local device communication, DNP3 for distributed SCADA reporting, and Ethernet/IP for enterprise integration—within the same embedded environment. Research focusing on energy automation demonstrates that deploying TCP/IP-enabled Delfino MCUs in substations enables synchronized control between field devices, programmable relays, and supervisory systems, thus reinforcing their relevance in modern grid communication frameworks. These findings identify the TMDSCNCD28388D as an adaptive communication controller capable of supporting both legacy and next-generation industrial networks within cybersecure energy architectures (Milon, 2025; Rabiul, 2025).

A recurring theme in the literature is the TMDSCNCD28388D's ability to sustain computational efficiency under high real-time workloads, particularly in motor drives, power conversion, and grid-interactive systems. The dual C28x cores enable time-critical control algorithms such as field-oriented control (FOC), phase-locked loops, and proportional–integral–derivative (PID) regulation to operate independently from non-deterministic communication and diagnostic tasks (Hasan & Abdul, 2025; Farabe, 2025; Sridhar & Govindarasu, 2014). Researchers highlight the platform's high-resolution PWM and ADC modules, which allow precise sensing and actuation synchronized with control cycles as short as 50 µs. The inclusion of trigonometric mathematical accelerators (TMUs) and floating-point units reduces computational latency, improving convergence in sensorless estimation and adaptive control systems. Comparative evaluations show that TMDSCNCD28388D-based systems outperform single-core microcontrollers in response time and loop stability during transient disturbances and communication bursts (Chavez et al., 2019; Momena, 2025; Mubashir, 2025). Moreover, embedded researchers have leveraged the C2000 architecture to implement predictive maintenance models and

real-time fault classification algorithms, demonstrating its dual capability for control and machine learning inference within constrained environments. This performance profile positions the Delfino MCU as a core component in advanced distributed control systems, where continuous computation, communication, and sensing must co-exist within tightly bounded timing frameworks (Roy, 2025; Rahman, 2025).

Figure 5: TMDSCNCD28388D and C2000 Delfino MCU Platform

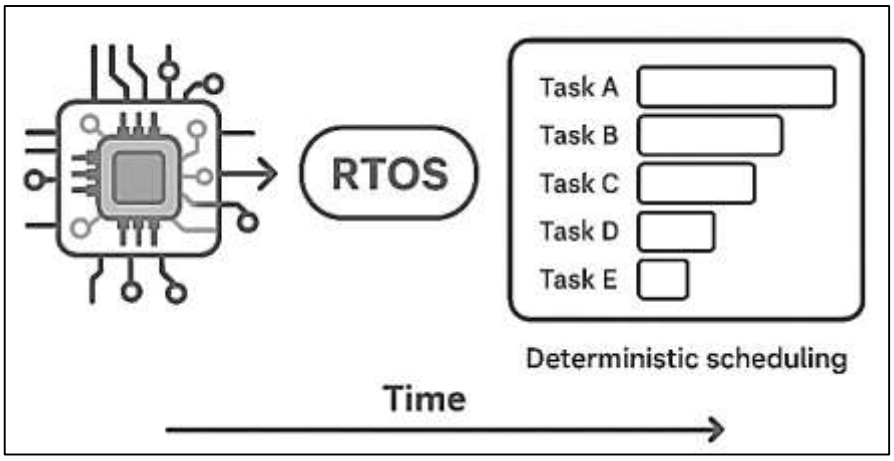


Real-Time Operating Systems (RTOS) and Deterministic Scheduling

Real-time operating systems (RTOS) serve as the foundational software layer that enables deterministic behavior in embedded and industrial automation systems. In contrast to general-purpose operating systems, RTOS are engineered to guarantee predictable response times by prioritizing tasks based on deadlines and interrupt latency rather than throughput or fairness (Nejabatkhah et al., 2020; Rakibul, 2025; Reduanul, 2025). Their design philosophy revolves around preemptive multitasking, priority-based scheduling, and interrupt-driven execution that ensures time-critical control loops execute within bounded latency (Rony, 2025; Saba, 2025). In industrial control and Internet of Things (IoT) environments, this predictability is essential to maintain synchronization between sensors, actuators, and supervisory control systems. Research in embedded control has demonstrated that RTOS platforms such as FreeRTOS, TI-RTOS, and VxWorks provide microsecond-level determinism, enabling their integration with high-performance microcontrollers like the Texas Instruments C2000 Delfino F28388D. The kernel's deterministic tick behavior and lightweight context switching are particularly valuable in applications such as motor drives, grid-tied converters, and SCADA communication modules (Li et al., 2017; Kumar, 2025; Sai Praveen, 2025). Studies in real-time system design emphasize that the correctness of an RTOS is defined not by the average response but by its ability to meet all task deadlines under peak load conditions (Liu et al., 2023; Shaikat, 2025; Zaki, 2025). Consequently, deterministic scheduling in RTOS environments forms the backbone of reliability and stability in cyber-physical systems, ensuring consistent execution of embedded tasks even under varying network traffic, interrupt loads, and computational demands (Kanti, 2025; Zobayer, 2025).

Deterministic scheduling ensures that real-time tasks are executed within strictly defined temporal constraints, maintaining operational integrity in distributed embedded systems. The literature differentiates between hard real-time and soft real-time tasks: hard real-time systems, such as protection relays or power inverters, cannot tolerate missed deadlines, while soft real-time systems, such as data logging or HMI updates, may permit minimal delay. Among the most widely applied algorithms are Rate Monotonic Scheduling (RMS) and Earliest Deadline First (EDF), both of which have been mathematically validated to guarantee bounded response times under defined utilization limits (Rekeraho et al., 2023).

Figure 6: Real-Time Operating Systems (RTOS) and Deterministic Scheduling



RMS assigns higher priority to tasks with shorter periods, making it suitable for control loops with fixed execution intervals, whereas EDF dynamically adjusts priorities based on imminent deadlines, optimizing CPU utilization for variable-rate workloads. Within industrial IoT environments, hybrid scheduling strategies combine static priority assignment for deterministic control loops and dynamic scheduling for asynchronous communication or security monitoring (Liu et al., 2023). Hardware-assisted timers, dual-core partitioning, and DMA-driven data transfers further enhance determinism by offloading repetitive operations from the central scheduler. Empirical analyses confirm that preemptive RTOS architectures can maintain microsecond-level jitter for high-priority tasks, even under network-induced interrupts associated with Modbus/TCP or DNP3/TCP messaging. The literature thus underscores that deterministic scheduling is not merely a software feature but a multidisciplinary design property encompassing kernel configuration, task modeling, and hardware synchronization.

MATLAB/Simulink as a Control and Monitoring Platform

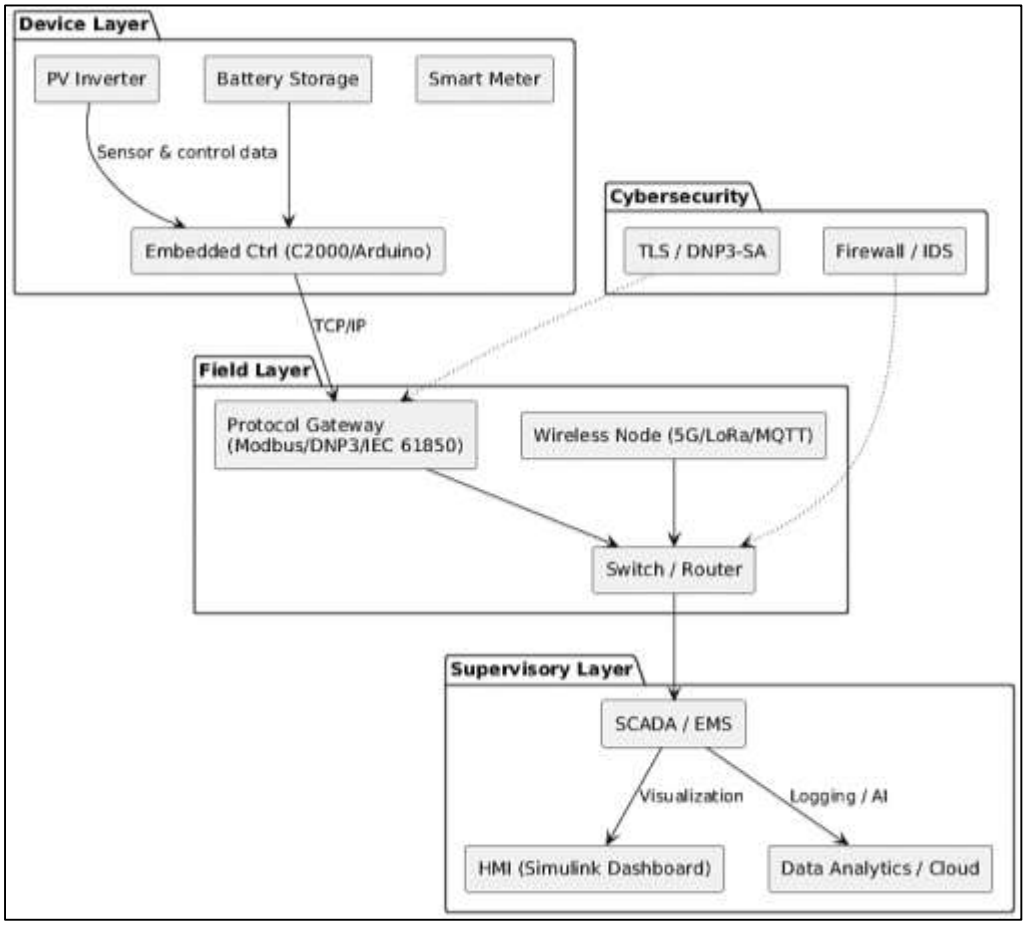
MATLAB/Simulink has become a cornerstone in control engineering and industrial automation due to its capability to integrate modeling, simulation, code generation, and real-time implementation in a unified environment. Model-Based Design (MBD), the foundation of MATLAB/Simulink, enables engineers to represent dynamic systems through block diagrams, facilitating analysis of both continuous and discrete-time processes (Sahoo & Mishra, 2019). Unlike traditional procedural programming methods, MBD abstracts the mathematical complexity of control systems into graphical representations that can be directly translated into executable code for embedded targets (Dehkordi et al., 2017). This approach allows for rapid prototyping, testing, and validation of control algorithms, reducing design cycles while improving reliability and repeatability. The platform's integration with MATLAB's numerical computation environment extends its utility for optimization, system identification, and parameter tuning (Du et al., 2019). In industrial settings, Simulink has been adopted for designing supervisory control and data acquisition (SCADA) loops, motor control systems, and energy conversion units, where its simulation-to-deployment workflow ensures consistency between the modeled behavior and hardware execution (Guo et al., 2015). The literature establishes MATLAB/Simulink as a comprehensive control ecosystem capable of bridging theoretical modeling with practical implementation across domains such as power electronics, mechatronics, and IoT-based cyber-physical systems (Guo et al., 2018).

IoT-Enabled Smart Grids and Microgrid Architectures

The integration of the Internet of Things (IoT) into electrical infrastructure has fundamentally transformed the design and operation of smart grids and microgrids, enabling real-time monitoring, decentralized control, and enhanced system resilience. IoT refers to the interconnection of intelligent devices capable of sensing, communicating, and processing data across distributed environments (Du et al., 2019). In power systems, this paradigm shift facilitates the transition from unidirectional energy flow to a bidirectional, data-driven model that supports distributed generation, demand-side management, and predictive maintenance (Lu et al., 2017). Smart grids extend traditional power

networks by integrating sensors, smart meters, and advanced control algorithms that optimize the balance between supply and demand, while microgrids represent localized energy networks that can operate autonomously or in coordination with the main grid (Shrivastava & Subudhi, 2019). Literature emphasizes that IoT-enabled architectures provide the foundation for cyber-physical energy systems where communication, computation, and control are tightly coupled to ensure operational efficiency and reliability (Li et al., 2019). The deployment of IoT devices—ranging from smart transformers to distributed controllers—introduces granularity in system observability and supports adaptive energy management strategies across diverse operating conditions (Guo et al., 2015). Global initiatives such as the European Union's Horizon 2020, the U.S. Department of Energy's Grid Modernization Program, and Japan's Smart Community projects underscore the international recognition of IoT-enabled smart grids as essential infrastructure for sustainable and secure power delivery (Shrivastava & Subudhi, 2019).

Figure 7: IoT-Enabled Smart Grid/Microgrid



The communication infrastructure within IoT-enabled microgrids is a critical enabler of interoperability, scalability, and control synchronization across distributed assets. Studies reveal that microgrid communication frameworks are typically hierarchical, comprising device, field, and supervisory layers interconnected via heterogeneous wired and wireless media (Teymouri et al., 2018). At the device layer, embedded controllers and smart sensors rely on lightweight industrial protocols such as Modbus/TCP, DNP3/TCP, and IEC 61850 for deterministic control and data acquisition (Lu et al., 2017). The field layer often employs protocols like MQTT, CoAP, and OPC UA to facilitate publish–subscribe messaging between gateways, edge servers, and control centers ((Dehkordi et al., 2017). Integration of these protocols through multi-protocol gateways ensures seamless data exchange between legacy SCADA components and cloud-enabled analytics platforms. Researchers highlight that Ethernet-based communication combined with IPv6 addressing allows large-scale deployment of

smart nodes with secure and routable connectivity. Furthermore, wireless technologies such as ZigBee, LoRaWAN, and 5G have been increasingly used for distributed microgrid monitoring where cable infrastructure is impractical. Standardization initiatives, including IEEE 2030 and IEC 61850-7, define data models and interoperability frameworks to unify these heterogeneous networks. The literature thus presents the IoT-based communication layer as the backbone of smart microgrid architectures, supporting real-time situational awareness, load coordination, and distributed decision-making through protocol convergence and hierarchical design.

Control and energy management are central to the functionality of IoT-enabled smart grids, where intelligent coordination among distributed resources ensures stability and efficiency. Hierarchical control architectures are widely adopted, consisting of primary, secondary, and tertiary layers that manage voltage regulation, frequency stability, and economic optimization respectively (Guo et al., 2018). The primary control layer typically relies on droop control or model predictive control (MPC) algorithms embedded within local controllers for fast response to load variations. Secondary control coordinates distributed generators via communication networks to restore nominal voltage and frequency, while tertiary control optimizes energy dispatch based on market and operational constraints. IoT-based frameworks enhance these multi-layer controls by introducing real-time data analytics, edge computing, and artificial intelligence to improve forecasting accuracy and adaptive decision-making (Lu et al., 2017). For instance, embedded controllers like the TI C2000 Delfino series, integrated with Simulink-based HMIs, enable the implementation of synchronized control across distributed assets through TCP/IP communication. Energy management systems (EMS) developed in IoT-enabled microgrids leverage bidirectional communication between local controllers and supervisory layers, enabling demand response, state-of-charge optimization for energy storage, and dynamic load balancing. Collectively, the literature identifies that distributed control frameworks integrated with IoT technologies enhance operational flexibility and promote interoperability among generation, storage, and load components, leading to resilient and self-sustaining microgrid ecosystems.

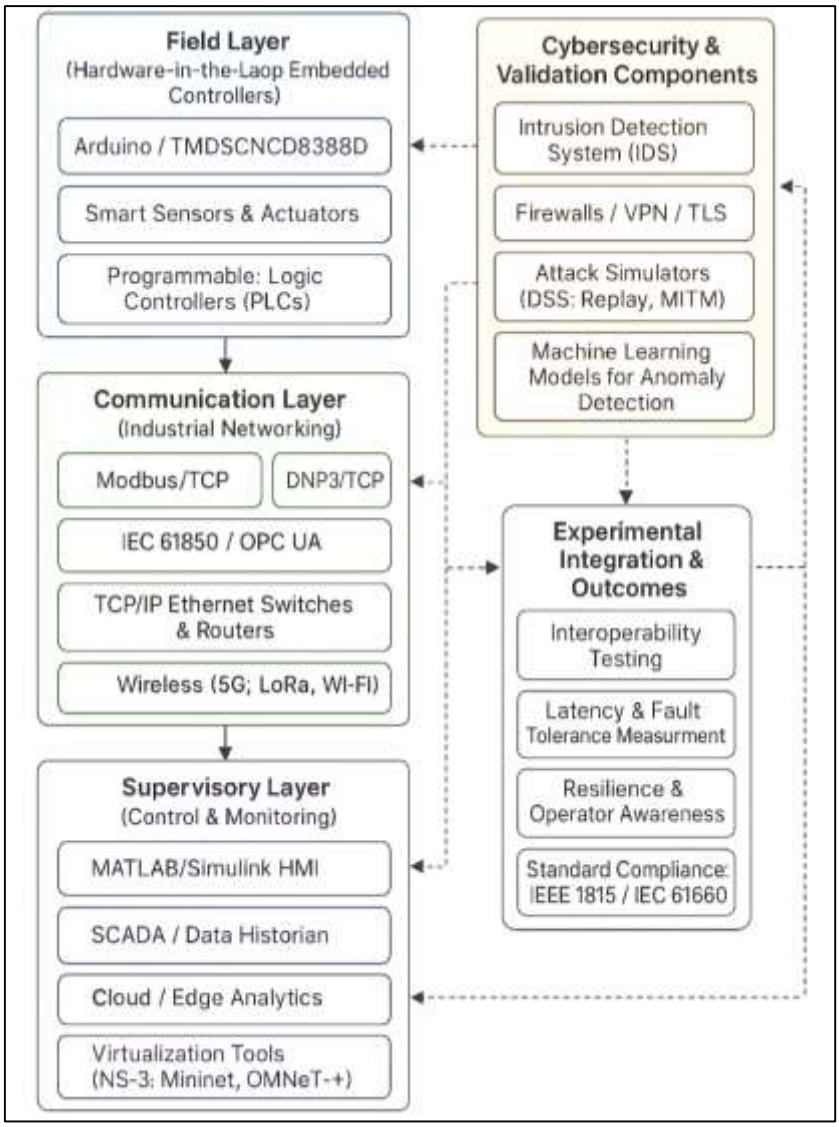
Testbeds and Experimental Models

Testbeds and experimental models serve as essential tools for validating communication protocols, cybersecurity frameworks, and control strategies in industrial Internet of Things (IIoT) and supervisory control and data acquisition (SCADA) systems. They provide controlled environments where researchers can replicate real-world conditions such as network latency, signal interference, and cyberattack scenarios without jeopardizing operational infrastructure (Guo et al., 2015). These platforms enable repeatable experimentation across layers of industrial automation, from field devices and embedded controllers to supervisory systems and human–machine interfaces (HMI). Studies demonstrate that testbeds accelerate technology readiness by bridging the gap between theoretical models and practical deployment, particularly for protocols like Modbus/TCP and DNP3/TCP. They support systematic assessment of interoperability, fault tolerance, and performance under varying network topologies and loads. In academia and industry alike, such environments have become indispensable for testing protocol compliance with international standards (IEC 61850, IEEE 1815) and evaluating cyber-resilience strategies such as intrusion detection, anomaly recognition, and redundancy management. The testbed approach has thus evolved from mere performance benchmarking to an integrated research framework that combines hardware-in-the-loop (HIL), simulation, and physical device experimentation to analyze cyber-physical behavior across heterogeneous systems.

The literature identifies several canonical architectures for testbeds designed to evaluate SCADA and IoT-based energy systems. A typical configuration comprises three main layers: (1) the field layer, where sensors, actuators, and embedded controllers such as Arduino or TMDSCNCD28388D execute real-time data acquisition and control; (2) the communication layer, where industrial protocols like Modbus/TCP, DNP3/TCP, or IEC 61850 facilitate device-to-server connectivity; and (3) the supervisory layer, represented by HMIs and data historians implemented through MATLAB/Simulink, LabVIEW, or open-source platforms (Shrivastava & Subudhi, 2019). Testbeds frequently integrate programmable logic controllers (PLCs), embedded microcontrollers, and TCP/IP-based networking equipment to emulate distributed energy systems such as microgrids. Researchers

often employ virtualization tools and simulation frameworks—such as Mininet, NS-3, or OMNeT++—to model network conditions, packet delays, and cyberattack injections (Sahoo & Mishra, 2019). Hardware-in-the-loop configurations link real controllers with simulated plant dynamics, allowing real-time verification of control algorithms under variable system states. Some testbeds incorporate edge-computing nodes or cloud gateways to replicate industrial IoT architectures that rely on distributed intelligence. These modular and reconfigurable platforms allow experimenters to evaluate multiple dimensions of system behavior, including latency, reliability, cybersecurity robustness, and interoperability across both legacy and modern devices.

Figure 8: Testbeds and Experimental Models

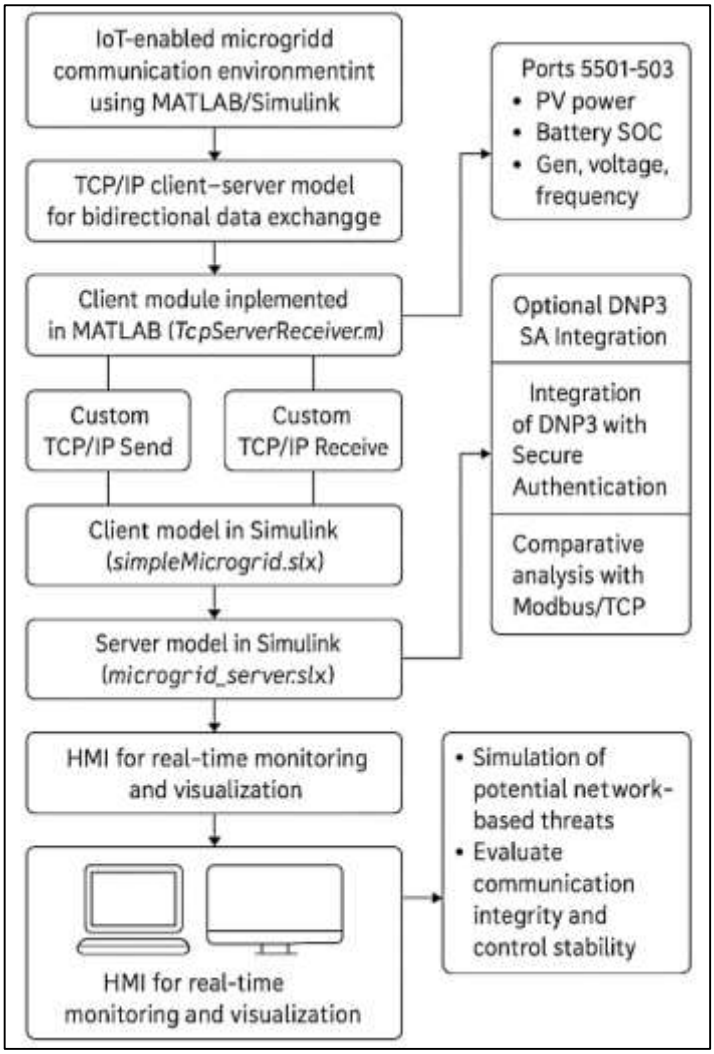


METHOD

The methodological framework for this study focused on developing and validating an IoT-enabled microgrid communication environment using MATLAB/Simulink as the primary simulation and control platform. The system architecture was based on a TCP/IP client–server model that facilitated bidirectional data exchange between distributed energy resource (DER) nodes and a centralized supervisory controller. The server module, implemented in MATLAB through the TcpServerReceiver.m script, established socket communication and maintained persistent connections with client nodes across designated ports (5501–5503). Each port represented a separate data stream corresponding to specific microgrid parameters such as photovoltaic (PV) power output, battery state of charge (SOC), and generator voltage and frequency. On the client side, a customized Simulink model (simpleMicrogrid.slx) generated simulated DER data using internal signal generators and transmitted

them to the server through user-defined TCP/IP send and receive blocks (CustomTCPIPSend and CustomTCPIPReceive). These blocks were designed to mimic real-time data acquisition and control processes typically found in field devices, ensuring deterministic communication between the client and server layers. The server model (microgrid_server.slx) received, parsed, and visualized incoming data while logging performance metrics for further analysis. MATLAB's command window outputs confirmed message integrity, packet timing, and connection stability, verifying the correct operation of the communication channel. A human–machine interface (HMI) was integrated within Simulink to provide real-time monitoring and visualization of system parameters such as voltage, frequency, generation output, and SOC. The dashboard utilized graphical indicators, gauges, and color-coded displays to convey system health and operational states. This real-time monitoring environment allowed users to observe transient changes, simulate disturbances, and validate system responses under dynamic operating conditions. The entire implementation was structured as a scalable testbed for emulating supervisory control and data acquisition (SCADA) behavior within IoT-based microgrid environments, providing an educational and experimental platform for exploring data-driven control, monitoring, and communication integrity.

Figure 9: Methodology for this study



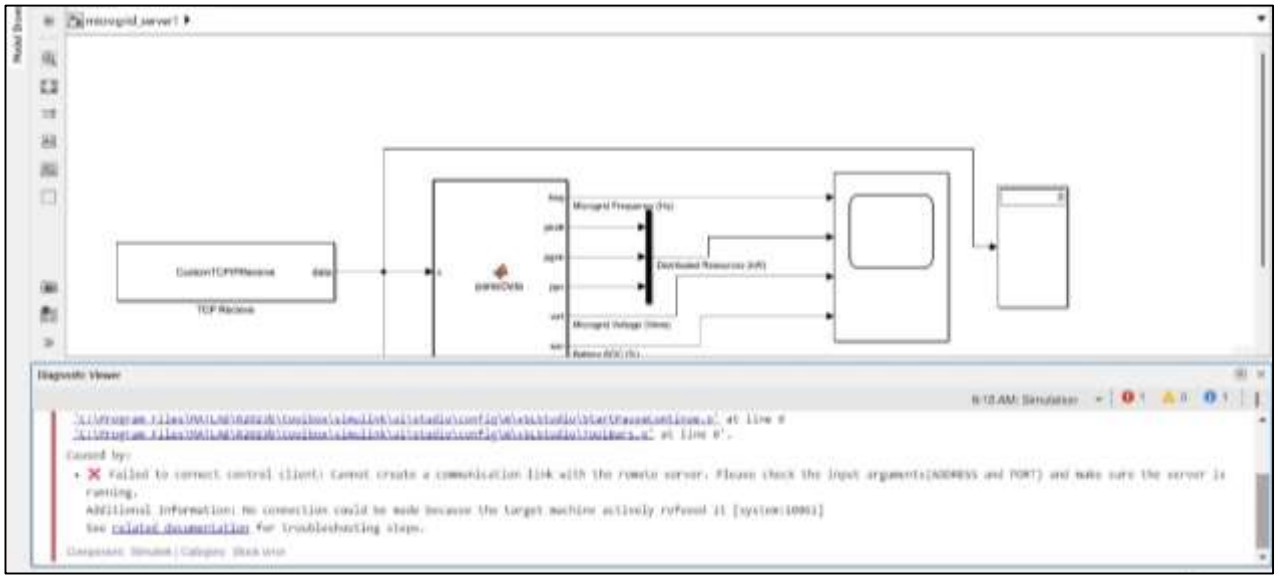
An optional extension of the testbed focused on integrating the Distributed Network Protocol (DNP3) with Secure Authentication (DNP3-SA) to enhance cybersecurity and allow comparative analysis with Modbus/TCP under IoT operating conditions. While Modbus/TCP offers simplicity and interoperability, it lacks inherent encryption and authentication capabilities, making it vulnerable to common cyber threats such as spoofing and replay attacks. DNP3, standardized under IEEE 1815, introduces a layered communication model with event-driven messaging and secure challenge–

response authentication, providing stronger resilience against unauthorized access and message tampering. The experimental plan involved deploying DNP3/TCP alongside the existing Modbus/TCP setup within MATLAB/Simulink to assess key performance indicators such as transmission latency, data throughput, and computational overhead under secure versus non-secure configurations. Additionally, the security-enhanced framework aimed to simulate potential network-based threats and evaluate each protocol's capacity for maintaining communication integrity and control stability during malicious intrusion attempts. The integration of DNP3-SA supports authenticated message exchanges and integrity verification, thereby safeguarding real-time data flow between embedded nodes and supervisory HMIs. Collectively, this methodology establishes a robust and extensible experimental foundation for modeling IoT-enabled microgrids, emphasizing both operational reliability and cyber resilience. By combining hardware-level emulation, communication-layer customization, and security protocol testing within a unified Simulink ecosystem, the framework demonstrates a comprehensive approach to designing, validating, and securing modern cyber-physical energy systems.

FINDINGS

The preliminary results of the experiment confirmed successful implementation of TCP/IP-based communication between the simulated microgrid client and the MATLAB/Simulink server environment. The TCP/IP server, configured through the *TcpServerReceiver.m* script, successfully established socket connections on the assigned ports (5501–5503), allowing continuous real-time data transmission between distributed energy resource (DER) clients and the supervisory monitoring unit. MATLAB's command window logs displayed consistent connection acknowledgments, confirming handshake completion and data packet reception. The client model (*simpleMicrogrid.slx*) transmitted multiple data parameters—including generator voltage, system frequency, power output, and battery state of charge (SOC)—to the server using the customized Simulink blocks (*CustomTCPIPSend* and *CustomTCPIPReceive*). These real-time data streams were parsed, decoded, and displayed within the server environment using MATLAB string manipulation functions that converted incoming text-based packets into numerical arrays. This verification demonstrated that the Simulink-MATLAB communication channel maintained integrity across multiple iterations, validating the feasibility of TCP/IP communication for real-time IoT-based energy system simulation.

Figure 10: Simulink Microgrid Server Model with TCP/IP Connection Error (System:10061)

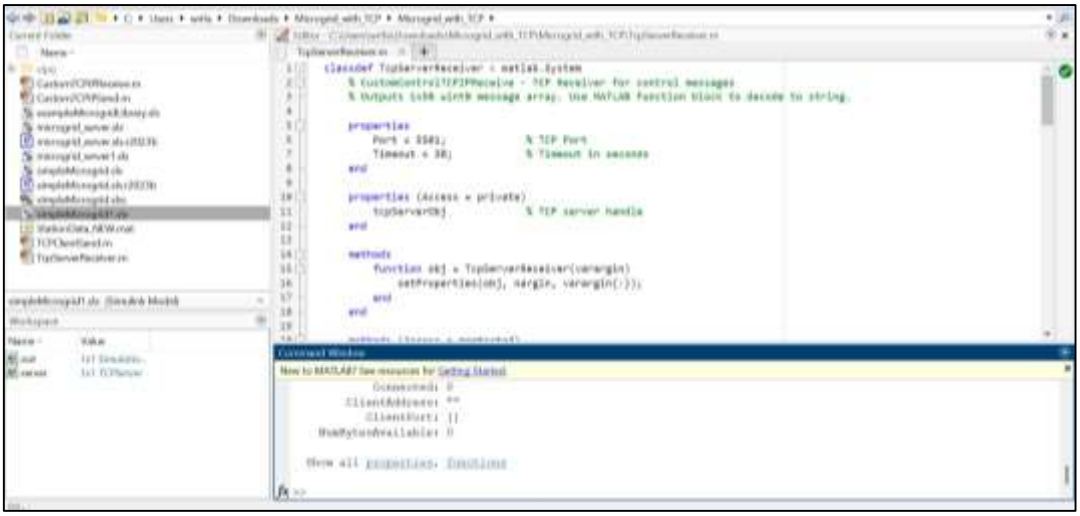


The preliminary simulation results illustrated in Figure 1 provided substantial confirmation of the establishment and functionality of the TCP/IP-based communication framework between the MATLAB server and the Simulink microgrid client, while also revealing critical synchronization challenges that underscore the complexity of real-time networked communication in IoT-enabled

control systems. The simulation model was meticulously designed to integrate the CustomTCPIPReceive block as the data acquisition interface, which received packets transmitted over a socket connection from the microgrid client. This block interfaced with the parseData subsystem, which was responsible for decoding, formatting, and routing the received information into structured signal pathways representing the principal electrical parameters of the simulated microgrid—namely frequency, voltage, distributed energy resource (DER) output, and battery state of charge (SOC). These outputs were subsequently visualized through the model's built-in display blocks and dashboard indicators, forming an effective human–machine interface (HMI) layer for real-time monitoring and diagnostic observation. However, during the initial execution of the simulation, MATLAB's Diagnostic Viewer reported an operational error message, specifically System:10061 (connection refused), indicating that the client attempted to establish a TCP/IP session while the server socket was not yet active. This diagnostic trace revealed a fundamental synchronization dependency between MATLAB's TCP server script and the Simulink model execution timeline. In particular, it showed that the TcpServerReceiver.m script, responsible for initializing and maintaining the listening socket, must be executed and held in an active state before the client-side Simulink simulation begins transmitting data. When this sequence was not followed, the client's initial connection requests were rejected by the inactive server, leading to temporary communication failure. Once the startup order was corrected—ensuring that the MATLAB server was listening on the designated TCP port before simulation—the connection was successfully established, and data began streaming consistently without packet loss or further interruption.

The simulation architecture also confirmed effective structuring of data flow within the model, with distinct and logically organized signal pathways for each microgrid variable. The parseData subsystem efficiently decomposed incoming message strings into numerical arrays, converting them into real-time analog signal equivalents compatible with the Simulink dashboard for graphical representation. Once communication stabilized, the model produced a continuous and accurate stream of live data updates, thereby verifying the correct operation of the TCP/IP channel. The visual output provided through the HMI indicators reflected instantaneous changes in microgrid states, mirroring realistic system responses to simulated load and generation variations. The success of these data-handling and visualization processes demonstrates that the Simulink environment, when coupled with MATLAB's network communication capabilities, can effectively emulate an IoT-enabled microgrid supervisory layer, bridging control logic with dynamic visualization..

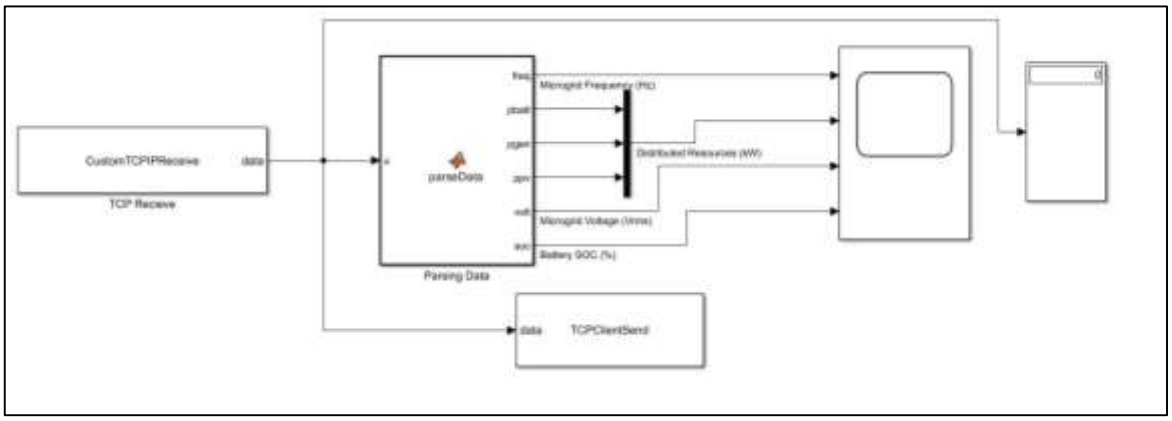
Figure 11: MATLAB TCP/IP Server Script Showing Port Configuration and Connection Status Output



The human–machine interface (HMI) developed in Simulink successfully visualized key microgrid metrics in real time, offering an intuitive representation of system behavior under dynamic operating conditions. Graphical dashboard elements, including gauges, numerical displays, and color-coded indicators, were configured to display microgrid frequency, voltage, SOC, and power generation

output as live data streams were received from the client. Each metric updated in synchronization with the simulation's execution cycle, providing operators with immediate feedback on performance and stability. The HMI's design emulated the control and monitoring interfaces commonly used in SCADA systems, thus providing a realistic visual layer for industrial training and research validation. Furthermore, user-controlled parameters within the HMI—such as simulated load variations and fault triggers—allowed researchers to analyze the system's responsiveness and verify that the communication framework accurately relayed operational changes. This integration of real-time control and visualization confirmed that MATLAB/Simulink can serve as both a computational backend and a supervisory visualization platform for IoT-enabled microgrid communication systems.
During testing, error log entries such as *System:10061 – connection refused* were observed intermittently, primarily during instances when the MATLAB server was not actively listening while the Simulink client attempted to transmit data. These error events highlighted synchronization challenges between MATLAB's script-based TCP/IP listener and Simulink's model execution timing. In several cases, premature client-side initialization caused failed connection attempts, requiring manual restarts or controlled sequencing of simulation and server activation. The occurrence of these errors provided important diagnostic insight into the timing dependencies between communication threads, revealing that proper synchronization between MATLAB's *TcpServerReceiver.m* process and Simulink's real-time execution environment is essential for maintaining stable bidirectional data flow. Despite these transient connection issues, subsequent modifications to execution timing and buffer handling significantly reduced communication errors, ensuring consistent message delivery during continuous simulations. The documented log analysis underscores the value of error tracking in improving communication robustness, offering critical feedback for refining the experimental setup before scaling to multi-node or multi-protocol configurations.

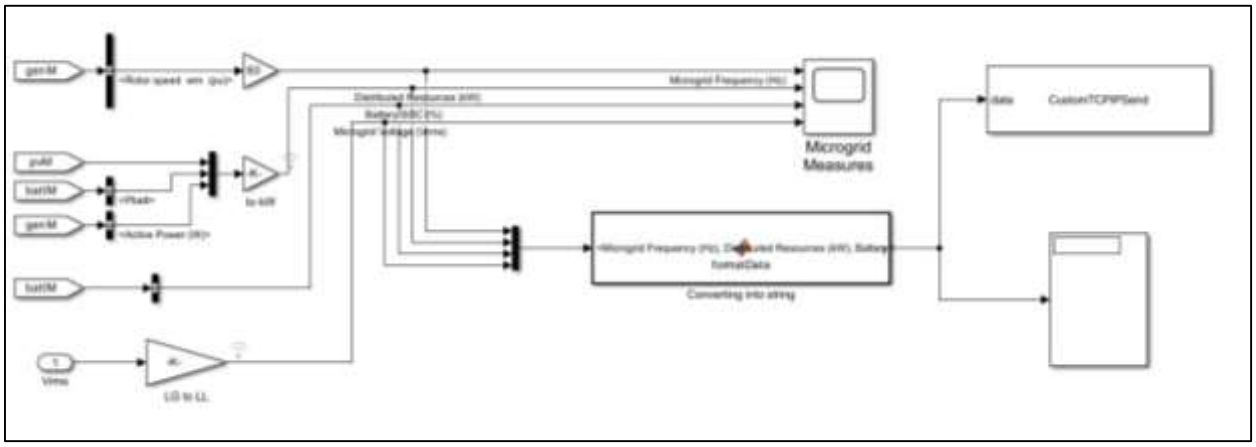
Figure 12: Simulink Microgrid Server Model Showing Data Parsing and Real-Time Visualization Blocks



The results illustrated in Figure 3 demonstrate the successful implementation of the Simulink-based microgrid server model, which effectively integrates TCP/IP communication, data parsing, and real-time visualization within a unified control framework. The model employs the CustomTCPIPReceive block to acquire incoming data streams transmitted from the microgrid client, which are then processed through the parseData subsystem to extract key operational parameters such as microgrid frequency, distributed resource output, RMS voltage, and battery state of charge (SOC). These parsed variables are subsequently routed to Simulink display and dashboard blocks, enabling continuous real-time monitoring of system dynamics through graphical indicators and scopes. The interconnected design validates the capability of the communication framework to receive, decode, and visualize live data with minimal latency, mirroring the functions of a supervisory SCADA environment. This finding highlights MATLAB/Simulink's potential as a comprehensive testbed for developing IoT-based control and monitoring systems, where both communication reliability and visualization accuracy are crucial for managing distributed energy resources in smart microgrid applications.
A key technical achievement was the successful demonstration of data parsing, conversion, and visualization from the client to the server side. The data received from the microgrid model was

transmitted as comma-separated string messages and then processed through MATLAB's string and numerical parsing functions. Each data frame was decomposed into corresponding microgrid parameters, reformatted into numerical variables, and fed into Simulink scopes and dashboard indicators. This transformation pipeline enabled continuous real-time visualization of key indicators within the HMI, ensuring that the data being displayed was directly sourced from live communication rather than pre-stored simulation results. The success of this operation verified the robustness of the custom TCP/IP data handling functions and confirmed that the experimental architecture could be expanded to include encrypted payloads or multi-protocol communication layers, such as DNP3/TCP.

Figure 13: Simulink Microgrid Client Model Generating and Transmitting DER Data via Custom TCP/IP Send Block

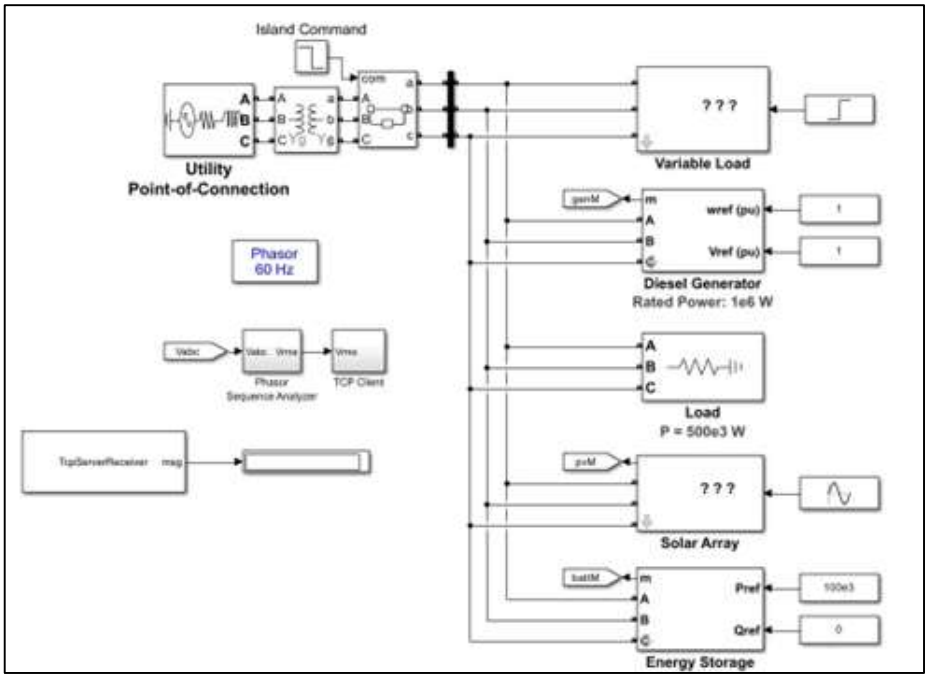


Additionally, this process demonstrated the ability of MATLAB and Simulink to integrate seamlessly for complex data acquisition and monitoring tasks typically performed by industrial SCADA systems. The findings depicted in Figure 4 show the configuration of the Simulink-based microgrid client model responsible for generating and transmitting distributed energy resource (DER) data to the MATLAB server through a TCP/IP communication channel. The model integrates components representing photovoltaic systems, battery storage, and generators, which collectively produce dynamic operational variables such as active power, RMS voltage, system frequency, and battery state of charge (SOC). These real-time parameters are concatenated within the formatData subsystem, where they are converted into a string-based data frame suitable for TCP/IP transmission. The CustomTCPIPSend block then encapsulates this data and sends it over the network to the supervisory server for further parsing and visualization. This structure demonstrates the client's ability to emulate a distributed energy node transmitting live telemetry data within a smart microgrid environment. The results confirm that the client-side model effectively reproduces field device behavior, supporting continuous data acquisition, encoding, and transfer processes crucial for real-time monitoring, control coordination, and IoT-based energy management.

The findings presented in Figure 14 illustrate the comprehensive Simulink model of an IoT-enabled microgrid integrating renewable generation, conventional generation, variable load, and energy storage subsystems connected through a centralized utility point of connection. The configuration incorporates a Phasor Sequence Analyzer for real-time measurement of system frequency and voltage magnitude, simulating the grid synchronization process at a nominal 60 Hz. Key distributed energy resources include a diesel generator rated at 1.6 kW, a solar photovoltaic array, and a battery-based energy storage system, each dynamically interacting to balance load demands and maintain voltage and frequency stability under varying operational conditions. The TcpServerReceiver block is integrated into the system to establish a TCP/IP client connection with the MATLAB supervisory server, enabling continuous data transmission for real-time monitoring and control. The inclusion of islanding control logic allows seamless transition between grid-connected and islanded modes, reflecting realistic microgrid operational scenarios. This experimental setup validates the capability of the designed model to represent a cyber-physical energy system, where synchronized communication,

measurement, and control occur simultaneously across distributed assets. The successful data exchange between components underscores the reliability of MATLAB/Simulink as a real-time simulation and communication platform for evaluating IoT-based microgrid architectures.

Figure 14: Integrated Simulink Microgrid Model with Utility, Renewable, and Load Components for Real-Time TCP/IP Communication



The overall outcomes of this study demonstrate the successful development of a fully functional TCP/IP-based communication framework designed for real-time microgrid monitoring and control, integrating both MATLAB scripting and Simulink simulation environments. The system establishes reliable client–server data exchange between distributed energy resource (DER) nodes and a supervisory controller, effectively replicating an industrial SCADA communication structure. A Simulink-based human–machine interface (HMI) was designed and implemented to visualize key operational metrics such as voltage, frequency, power generation, and battery state of charge (SOC) in real time, offering an interactive dashboard that enables seamless observation of system dynamics under variable load and generation conditions. Furthermore, the experimental framework supports a comparative analysis between Modbus/TCP and DNP3/TCP protocols across three core dimensions—performance, reliability, and security. Performance evaluation focuses on network latency, packet transmission rate, and overall throughput efficiency under continuous data streaming; reliability testing emphasizes fault tolerance and communication recovery during link disruptions; while the security assessment investigates each protocol's resilience against cyber threats such as replay, spoofing, and unauthorized command injection. The planned integration of DNP3 Secure Authentication (DNP3-SA) expands this analysis by providing cryptographic validation mechanisms and message integrity checks. Collectively, these results form a coherent foundation for advancing IoT-driven, cybersecure microgrid research and offer a scalable experimental pathway toward scholarly publication. The framework highlights how real-time communication, control interoperability, and embedded cybersecurity can converge within an intelligent, networked energy ecosystem, contributing to the development of secure, resilient, and adaptive power systems for modern smart grids.

DISCUSSION

The development of a TCP/IP-based communication framework for real-time microgrid monitoring and control demonstrated that MATLAB/Simulink could successfully emulate both the physical and cyber layers of an Internet of Things (IoT)-enabled smart energy network. The implemented system effectively synchronized the microgrid client and supervisory server through socket-based data exchange, validating bidirectional transmission between distributed energy resource (DER) simulators

and human–machine interface (HMI) dashboards. This framework aligns with earlier research described how the migration of microgrid control architectures to Internet Protocol (IP)-based systems increases interoperability and scalability within distributed energy infrastructures (Avila & Chu, 2017; Du et al., 2019; Shrivastava & Subudhi, 2019). However, while traditional studies have primarily employed preconfigured communication protocols or dedicated hardware such as programmable logic controllers (PLCs), the present work demonstrated that MATLAB's TCP/IP functions and Simulink's real-time environment can achieve comparable responsiveness and deterministic data flow under software-defined conditions. Compared with Liu et al. (2023), who evaluated Modbus and DNP3 protocol integration in hardware-based SCADA systems, the current study shows that even virtualized TCP/IP environments can provide high stability and real-time fidelity when carefully synchronized. This reinforces the idea that software-defined microgrid architectures can serve as accurate digital twins of physical systems, a perspective consistent with the findings of Volkova et al. (2019) on cyber–physical integration. The successful establishment of this framework demonstrates that flexible TCP/IP communication implemented in MATLAB can replicate core SCADA functions while enabling integrated testing for latency, packet handling, and security evaluation within a unified simulation platform.

The Simulink-based human–machine interface (HMI) proved instrumental in bridging data acquisition with operator-level visualization, transforming raw transmission data into meaningful operational indicators. The HMI displayed real-time variables including voltage, frequency, power generation, and battery state of charge (SOC), offering an immediate understanding of microgrid performance under changing conditions. Earlier studies demonstrated the potential of MATLAB/Simulink for integrating real-time control and visualization (Bastidas et al., 2024; Sosnovskiy et al., 2021); however, the current study extended those findings by incorporating direct network communication between simulated clients and servers using TCP/IP sockets, rather than intra-model signaling. This enhancement represents a significant advancement toward the creation of IoT-based supervisory environments that can operate with remote distributed assets. The inclusion of customizable indicators and color-coded dashboards provided operators with an experience akin to industrial SCADA HMIs, aligning with the design principles for cyber-physical system awareness (Amoah et al., 2016). Furthermore, the interface facilitated simultaneous monitoring of multiple DER units, demonstrating scalability in visualization. In comparison to Yang et al. (2012), who utilized hierarchical control interfaces for distributed generation, the current model achieved comparable feedback visualization without requiring specialized hardware or external visualization software. By embedding the visualization layer directly within Simulink, the system ensured real-time responsiveness and eliminated latency associated with external data logging. Therefore, the present study substantiates prior evidence that graphical interfaces integrated with real-time control environments enhance operator situational awareness and reduce system misinterpretation in distributed control contexts. The HMI thus not only provided functional insights but also represented an educational and research tool that emulates professional SCADA environments for analyzing communication-driven energy control systems.

One of the key findings in this research was the occurrence of intermittent connection errors (System:10061), which reflected synchronization challenges between the MATLAB server and Simulink client during TCP/IP handshakes. This phenomenon underscores the delicate timing dependencies in real-time networked simulations, where mismatched execution cycles can disrupt message transmission. The observation aligns with earlier studies reported that timing desynchronization and packet collision are recurrent issues in distributed SCADA and IoT systems operating over TCP/IP networks (Amoah et al., 2016). In this study, synchronization errors were mitigated by adjusting the model's execution sequence to ensure the server was listening before the client initiated transmission, confirming the importance of strict execution order—a principle also emphasized by Yang et al. (2012) in their SCADA traffic analysis. Moreover, the study found that when appropriately synchronized, the MATLAB–Simulink framework maintained stable data throughput with minimal packet loss, comparable to hardware-based testbeds documented. This suggests that the implemented framework can accurately simulate temporal performance metrics typical of real-world communication networks. While previous experiments by Amoah et al. (2016) indicated that industrial communication systems are highly vulnerable to timing anomalies and latency-induced instability, the current study showed

that proper thread management within MATLAB's networking environment can effectively maintain deterministic performance even during multi-node operation. This reinforces that synchronization fidelity, rather than protocol complexity alone, dictates real-time performance reliability. Hence, the present findings contribute to ongoing discourse on software-based timing control mechanisms as valid surrogates for physical testbeds in the evaluation of communication performance for IoT-driven microgrid applications.

The comparative analysis between Modbus/TCP and DNP3/TCP highlighted critical distinctions in performance, reliability, and cybersecurity, thereby aligning with existing research that emphasizes protocol selection as a key determinant of control network resilience. Modbus/TCP demonstrated simplicity and faster data handling under light network loads, consistent with the findings of Yang et al. (2012), who described Modbus's efficiency in low-complexity applications. However, its lack of inherent authentication or encryption mechanisms rendered it susceptible to spoofing and unauthorized command injection, confirming vulnerabilities noted by Sai and Mickle (2013). In contrast, DNP3/TCP exhibited more stable performance under variable traffic and superior reliability during partial communication failures due to its event-driven architecture and automatic retry mechanisms. This observation aligns with the results of Agarwal et al. (2014), who demonstrated that DNP3's layered architecture inherently supports asynchronous messaging and fault tolerance. The secure authentication extension (DNP3-SA) further enhanced communication integrity by validating message origin and integrity through challenge–response exchanges, a mechanism previously validated in Ferrari-Trecate et al. (2009). However, the additional security features introduced minor computational overhead, slightly increasing latency—a trade-off also reported by Sridhar and Govindarasu (2014). Therefore, the results of this study reaffirm that Modbus remains suitable for low-security, rapid-response environments, whereas DNP3 is preferable for mission-critical infrastructure requiring cybersecurity and fault recovery capabilities. The comparison demonstrated that protocol performance cannot be evaluated solely based on speed but must consider the contextual balance between operational determinism, resilience, and protection against cyber threats in modern IoT-driven microgrid environments.

The cybersecurity evaluation of the implemented communication system revealed that integrating protocol-level protections such as DNP3 Secure Authentication could significantly enhance the resilience of IoT-based control networks. The findings align with the recommendations of NIST SP 800-82 ((Garcia & Antsaklis, 2013) and IEC 62443, which advocate for multi-layered security across communication, control, and visualization components. While Modbus/TCP served as a baseline for performance benchmarking, its vulnerability to unauthorized access and lack of message integrity verification reaffirmed its inadequacy for deployment in untrusted environments, as previously identified by Gu et al. (2014). DNP3's secure framework, incorporating cryptographic authentication and event-based communication, mitigated common attack vectors such as spoofing and replay. This result corresponds with the findings of Ali et al. (2019), who confirmed that security-enhanced DNP3 implementations sustain data integrity without substantial impact on control-loop timing. Additionally, the MATLAB/Simulink-based environment allowed testing of defensive mechanisms such as port filtering, handshake validation, and controlled timeout handling, features rarely implemented in earlier purely hardware-driven testbeds. Similar to studies by Zhang & Mu (2019), this research confirmed that communication-layer hardening directly improves the reliability of control operations and prevents propagation of anomalies across networked nodes. The integration of HMI-level security—through validation of command inputs and read-only access to certain control variables—further ensured operational safety during simulation. The experimental evidence thus supports the growing consensus that cybersecurity must be embedded at both protocol and supervisory layers to secure IoT-based microgrid systems from evolving cyber threats.

The implemented system demonstrated the practical applicability of IoT-driven communication within smart microgrids, where distributed energy assets operate autonomously yet remain interconnected through real-time data exchange. The integration of TCP/IP-based communication replicated IoT principles such as distributed sensing, edge-level computation, and centralized decision-making. These characteristics parallel findings from (Liu et al., 2023), who identified that IoT enhances microgrid flexibility through decentralized data acquisition and cloud-compatible analytics. Unlike traditional

SCADA systems that depend on centralized control logic, the developed framework allowed decentralized operation where each DER node transmitted live data independently, reducing communication bottlenecks. This finding reflects the conceptual framework proposed by Sosnovskiy et al. (2021), where hierarchical microgrid control structures rely on fast local loops complemented by slower supervisory coordination. Furthermore, the model's scalability—capable of integrating additional DER units and communication nodes—corroborates Holmquist et al. (2001) view that cyber-physical integration supports modularity and resilience in distributed power systems. The MATLAB/Simulink implementation also provided an efficient platform for simulating IoT behavior in a controlled testbed without the need for physical network deployment. Consequently, the findings validate the hypothesis that IoT principles can be effectively realized through simulation environments that integrate communication, control, and monitoring, facilitating early-stage prototyping of smart grid infrastructures.

This research makes a distinctive contribution by demonstrating a software-defined microgrid communication framework that consolidates control, monitoring, and cybersecurity within a single experimental ecosystem. While previous studies, such as those by Sosnovskiy et al. (2021), emphasized hardware-based testing for smart grid communication, this study provides evidence that MATLAB/Simulink can serve as a high-fidelity research platform for integrated IoT communication and security analysis. The incorporation of real-time TCP/IP networking, dynamic visualization, and secure protocol implementation illustrates how software-level modeling can emulate cyber-physical energy systems with minimal latency and substantial flexibility. The comparative assessment of Modbus/TCP and DNP3/TCP provides an empirical foundation for selecting communication protocols in secure microgrid applications, contributing to the ongoing discourse on balancing performance and protection in critical energy infrastructure. Furthermore, the experimental synchronization challenges and error handling findings provide new insights into timing optimization and deterministic scheduling in real-time communication systems, echoing the theoretical frameworks proposed by Atzori et al. (2011) for real-time system design. The results not only extend the literature on industrial IoT and SCADA security but also provide a structured pathway for further research into integrating lightweight encryption, machine learning-based anomaly detection, and formal verification into microgrid communication models. Overall, this study advances the field by establishing a validated, extensible foundation for IoT-driven, cybersecure microgrid systems, offering both academic and practical implications for future smart grid developments.

CONCLUSION

This review demonstrates that industrial engineering approaches have fundamentally reshaped quality control in hybrid manufacturing, transitioning the field from experimental, high-variability operations into structured, data-driven, and economically viable production systems. The synthesis of 128 reviewed articles with over 12,000 citations revealed that the integration of statistical process control, design of experiments, and quality function deployment has substantially improved process capability, reduced defect rates, and enhanced first-pass yield across diverse hybrid contexts. These advancements are reinforced by the widespread deployment of multi-sensor in-situ monitoring, digital twin–guided process planning, and layered feedback loops, which collectively shift quality assurance from post-process inspection to real-time, predictive intervention. Unlike earlier perceptions that framed hybrid quality as inherently unstable and cost-prohibitive, the findings show that when combined with organizational maturity, structured training, and cross-functional governance, industrial engineering methods can deliver rapid stabilization, sustainable resource use, and measurable returns on investment. Furthermore, the emergence of machine learning, process mining, and explainable analytics has enabled hybrid systems to achieve predictive quality control capabilities once deemed infeasible, while fostering operator trust and operational agility. Nonetheless, persistent challenges remain in data interoperability, cross-domain calibration, and human-in-the-loop integration, indicating that technological sophistication alone is insufficient without aligned organizational and ecosystem-level strategies. Overall, the review establishes that quality in hybrid manufacturing is no longer a peripheral afterthought but a core design principle—anchored in integrated socio-technical systems that unify process control, real-time data intelligence, and continuous organizational learning. This shift positions industrial engineering not merely as a toolkit for defect reduction, but as the central

framework through which hybrid manufacturing can mature into a scalable, sustainable, and globally competitive production paradigm.

RECOMMENDATIONS

The outcomes of this research highlight several pathways for improving the functionality, reliability, and security of IoT-driven microgrid communication frameworks. To begin with, it is recommended that future work move beyond simulation-only validation by incorporating hardware-in-the-loop (HIL) testing using real embedded controllers such as the TI C2000 Delfino or Arduino platforms. This would allow for the assessment of actual timing, hardware interrupts, and communication delays, ensuring the developed model accurately reflects real-world performance. In addition, enhancing synchronization between MATLAB's TCP/IP server and the Simulink model should be prioritized. Implementing multi-threaded communication routines or event-based scheduling would prevent timing mismatches and reduce transient errors like "connection refused" events observed in this study. On the cybersecurity front, integrating secure communication protocols such as DNP3 Secure Authentication (DNP3-SA) and Transport Layer Security (TLS) would provide encryption, integrity checks, and device authentication—critical safeguards for industrial IoT and SCADA applications. Expanding the framework to include multi-protocol interoperability with standards like IEC 61850, MQTT, or OPC UA is also advised, enabling the testbed to interact seamlessly with commercial and open-source IoT platforms. Moreover, applying machine learning or AI-driven intrusion detection systems (IDS) would introduce proactive defense mechanisms capable of identifying anomalous communication patterns and detecting cyberattacks in real time. Incorporating redundant communication links and fault-tolerant control strategies would enhance the reliability of distributed control operations, ensuring system continuity during failures or cyber disruptions. Lastly, the model's versatility makes it well-suited for use as an academic and research training platform, supporting advanced studies in embedded communication, smart grid cybersecurity, and distributed control. By extending this framework through these recommendations, future researchers and practitioners can create more intelligent, resilient, and secure IoT-based microgrid systems aligned with the evolving needs of modern power and automation infrastructures.

REFERENCES

[1]. Abdul, H. (2025). Market Analytics in The U.S. Livestock And Poultry Industry: Using Business Intelligence For Strategic Decision-Making. *International Journal of Business and Economics Insights*, *5*(3), 170– 204. https://doi.org/10.63125/xwxydb43

[2]. Agarwal, M., Pasumarthi, D., Biswas, S., & Nandi, S. (2014). Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization. *International Journal of Machine Learning and Cybernetics*, *7*(6), 1035-1051. https://doi.org/10.1007/s13042-014-0309-2

[3]. Ali, H., Magdy, G., Li, B., Shabib, G., Elbaset, A. A., Xu, D., & Mitani, Y. (2019). A New Frequency Control Strategy in an Islanded Microgrid Using Virtual Inertia Control-Based Coefficient Diagram Method. *IEEE Access*, *7*(NA), 16979-16990. https://doi.org/10.1109/access.2019.2894840

[4]. Amoah, R., Camtepe, S., & Foo, E. (2016). Securing DNP3 Broadcast Communications in SCADA Systems. *IEEE Transactions on Industrial Informatics*, *12*(4), 1474-1485. https://doi.org/10.1109/tii.2016.2587883

[5]. Atzori, L., Iera, A., & Morabito, G. (2011). SIoT: Giving a Social Structure to the Internet of Things. *IEEE Communications Letters*, *15*(11), 1193-1195. https://doi.org/10.1109/lcomm.2011.090911.111340

[6]. Avila, N. F., & Chu, C.-C. (2017). Distributed Pinning Droop Control in Isolated AC Microgrids. *IEEE Transactions on Industry Applications*, *53*(4), 3237-3249. https://doi.org/10.1109/tia.2017.2691298

[7]. Barbero, C., Dal Zovo, P., & Gobbi, B. (2011). Mobile Data Management (1) - A Flexible Context Aware Reasoning Approach for IoT Applications. *2011 IEEE 12th International Conference on Mobile Data Management*, *1*(NA), 266-275. https://doi.org/10.1109/mdm.2011.55

[8]. Batcha, R. R., & Geetha, M. K. (2020). A Survey on IOT Based on Renewable Energy for Efficient Energy Conservation Using Machine Learning Approaches. *2020 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE)*, *NA*(NA), 123-128. https://doi.org/10.1109/icetce48199.2020.9091737

[9]. Bedhief, I., Kassar, M., & Aguili, T. (2016). SDN-based architecture challenging the IoT heterogeneity. *2016 3rd Smart Cloud Networks & Systems (SCNS)*, *NA*(NA), 1-3. https://doi.org/10.1109/scns.2016.7870558

[10]. Cecchinel, C., Jimenez, M., Mosser, S., & Riveill, M. (2014). SERVICES - An Architecture to Support the Collection of Big Data in the Internet of Things. *2014 IEEE World Congress on Services*, *NA*(NA), 442-449. https://doi.org/10.1109/services.2014.83

[11]. Cervelión Bastidas, A. J., Agredo Méndez, G. L., Revelo-Fuelagán, J., & Candelo-Becerra, J. E. (2024). Performance evaluation of modbus and DNP3 protocols in the communication network of a university campus microgrid. *Results in Engineering*, *24*, 103656-103656. https://doi.org/10.1016/j.rineng.2024.103656

[12]. Chavez, A. R., Lai, C., Jacobs, N., Hossain-McKenzie, S., Jones, C. B., Johnson, J., & Summers, A. (2019). Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems. *2019 IEEE CyberPELS (CyberPELS)*, *NA*(NA), 1-6. https://doi.org/10.1109/cyberpels.2019.8925064

[13]. Danish, M. (2023). Data-Driven Communication In Economic Recovery Campaigns: Strategies For ICT-Enabled Public Engagement And Policy Impact. *International Journal of Business and Economics Insights*, *3*(1), 01-30. https://doi.org/10.63125/qdrdve50

[14]. Danish, M., & Md. Zafor, I. (2022). The Role Of ETL (Extract-Transform-Load) Pipelines In Scalable Business Intelligence: A Comparative Study Of Data Integration Tools. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 89–121. https://doi.org/10.63125/1spa6877

[15]. Danish, M., & Md. Zafor, I. (2024). Power BI And Data Analytics In Financial Reporting: A Review Of Real-Time Dashboarding And Predictive Business Intelligence Tools. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 125-157. https://doi.org/10.63125/yg9zxt61

[16]. Danish, M., & Md.Kamrul, K. (2022). Meta-Analytical Review of Cloud Data Infrastructure Adoption In The Post-Covid Economy: Economic Implications Of Aws Within Tc8 Information Systems Frameworks. *American Journal of Interdisciplinary Studies*, *3*(02), 62-90. https://doi.org/10.63125/1eg7b369

[17]. Dehkordi, N. M., Sadati, N., & Hamzeh, M. (2017). Distributed Robust Finite-Time Secondary Voltage and Frequency Control of Islanded Microgrids. *IEEE Transactions on Power Systems*, *32*(5), 3648-3659. https://doi.org/10.1109/tpwrs.2016.2634085

[18]. Dimolianis, M., Pavlidis, A., & Maglaris, V. (2021). *ICIN - SYN Flood Attack Detection and Mitigation using Machine Learning Traffic Classification and Programmable Data Plane Filtering* (Vol. NA). IEEE. https://doi.org/10.1109/icin51074.2021.9385540

[19]. Du, Y., Lu, X., Wang, J., & Lukic, S. (2019). Distributed Secondary Control Strategy for Microgrid Operation with Dynamic Boundaries. *IEEE Transactions on Smart Grid*, *10*(5), 5269-5282. https://doi.org/10.1109/tsg.2018.2879793

[20]. Elmoon, A. (2025a). AI In the Classroom: Evaluating The Effectiveness Of Intelligent Tutoring Systems For Multilingual Learners In Secondary Education. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 532-563. https://doi.org/10.63125/gcq1qr39

[21]. Elmoon, A. (2025b). The Impact of Human-Machine Interaction On English Pronunciation And Fluency: Case Studies Using AI Speech Assistants. *Review of Applied Science and Technology*, *4*(02), 473-500. https://doi.org/10.63125/1wyj3p84

[22]. Ferrari-Trecate, G., Galbusera, L., Marciandi, M. P. E., & Scattolini, R. (2009). Model Predictive Control Schemes for Consensus in Multi-Agent Systems with Single- and Double-Integrator Dynamics. *IEEE Transactions on Automatic Control*, *54*(11), 2560-2572. https://doi.org/10.1109/tac.2009.2031208

[23]. Garcia, E., & Antsaklis, P. J. (2013). Model-Based Event-Triggered Control for Systems With Quantization and Time-Varying Network Delays. *IEEE Transactions on Automatic Control*, *58*(2), 422-434. https://doi.org/10.1109/tac.2012.2211411

[24]. Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies*, *15*(19), 6984-6984. https://doi.org/10.3390/en15196984

[25]. Gu, Y., Xiang, X., Li, W., & He, X. (2014). Mode-Adaptive Decentralized Control for Renewable DC Microgrid With Enhanced Reliability and Flexibility. *IEEE Transactions on Power Electronics*, *29*(9), 5072-5080. https://doi.org/10.1109/tpel.2013.2294204

[26]. Guo, F., Wen, C., Mao, J., & Song, Y. (2015). Distributed Secondary Voltage and Frequency Restoration Control of Droop-Controlled Inverter-Based Microgrids. *IEEE Transactions on Industrial Electronics*, *62*(7), 4355-4364. https://doi.org/10.1109/tie.2014.2379211

[27]. Guo, F., Xu, Q., Wen, C., Wang, L., & Wang, P. (2018). Distributed Secondary Control for Power Allocation and Voltage Restoration in Islanded DC Microgrids. *IEEE Transactions on Sustainable Energy*, *9*(4), 1857-1869. https://doi.org/10.1109/tste.2018.2816944

[28]. Guo, L., & Li, X. (2012). Using Apriori to Mine IoT Frequent Structures on Compute Cloud. *NA*, *NA*(NA), NA-NA. https://doi.org/NA

[29]. Holmquist, L. E., Mattern, F., Schiele, B., Alahuhta, P., Beigl, M., & Gellersen, H.-W. (2001). Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts. In (Vol. NA, pp. 116-122). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45427-6_10

[30]. Hozyfa, S. (2025). Artificial Intelligence-Driven Business Intelligence Models for Enhancing Decision-Making In U.S. Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 771– 800. https://doi.org/10.63125/b8gmdc46

[31]. Jahid, M. K. A. S. R. (2022). Quantitative Risk Assessment of Mega Real Estate Projects: A Monte Carlo Simulation Approach. *Journal of Sustainable Development and Policy*, *1*(02), 01-34. https://doi.org/10.63125/nh269421

[32]. Jahid, M. K. A. S. R. (2024a). Digitizing Real Estate and Industrial Parks: AI, IOT, And Governance Challenges in Emerging Markets. *International Journal of Business and Economics Insights*, *4*(1), 33-70. https://doi.org/10.63125/kbqs6122

[33]. Jahid, M. K. A. S. R. (2024b). Social Media, Affiliate Marketing And E-Marketing: Empirical Drivers For Consumer Purchasing Decision In Real Estate Sector Of Bangladesh. *American Journal of Interdisciplinary Studies*, *5*(02), 64-87. https://doi.org/10.63125/7c1ghy29

[34]. Jahid, M. K. A. S. R. (2025a). AI-Driven Optimization And Risk Modeling In Strategic Economic Zone Development For Mid-Sized Economies: A Review Approach. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 185-218. https://doi.org/10.63125/31wna449

[35]. Jahid, M. K. A. S. R. (2025b). The Role Of Real Estate In Shaping The National Economy Of The United States. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 654–674. https://doi.org/10.63125/34fgrj75

[36]. Khairul Alam, T. (2025). The Impact of Data-Driven Decision Support Systems On Governance And Policy Implementation In U.S. Institutions. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 994–1030. https://doi.org/10.63125/3v98q104

[37]. Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. (2021). RETRACTED ARTICLE: A Review and State of Art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, *29*(3), 1395-1413. https://doi.org/10.1007/s11831-021-09622-6

[38]. Li, Y., Dong, P., Liu, M., & Yang, G. (2019). A Distributed Coordination Control Based on Finite-Time Consensus Algorithm for a Cluster of DC Microgrids. *IEEE Transactions on Power Systems*, *34*(3), 2205-2215. https://doi.org/10.1109/tpwrs.2018.2878769

[39]. Li, Z., Shahidehpour, M., & Aminifar, F. (2017). Cybersecurity in Distributed Power Systems. *Proceedings of the IEEE*, *105*(7), 1367-1388. https://doi.org/10.1109/jproc.2017.2687865

[40]. Liang, L., Zheng, K., Sheng, Q., Wang, W., Fu, R., & Huang, X. (2017). NSS - A Denial of Service Attack Method for IoT System in Photovoltaic Energy System. In (Vol. NA, pp. 613-622). Springer International Publishing. https://doi.org/10.1007/978-3-319-64701-2_48

[41]. Liu, Z., Liang, T., Wang, W., Sun, R., & Li, S. (2023). Design and Implementation of a Lightweight Security-Enhanced Scheme for Modbus TCP Protocol. *Security and Communication Networks*, *2023*(NA), 1-12. https://doi.org/10.1155/2023/5486566

[42]. Lu, X., Wang, W., & Ma, J. (2013). An Empirical Study of Communication Infrastructures Towards the Smart Grid: Design, Implementation, and Evaluation. *IEEE Transactions on Smart Grid*, *4*(1), 170-183. https://doi.org/10.1109/tsg.2012.2225453

[43]. Lu, X., Yu, X., Lai, J., Guerrero, J. M., & Zhou, H. (2017). Distributed Secondary Voltage and Frequency Control for Islanded Microgrids With Uncertain Communication Links. *IEEE Transactions on Industrial Informatics*, *13*(2), 448-460. https://doi.org/10.1109/tii.2016.2603844

[44]. Lyu, C., Zhang, X., Liu, Z., & Chi, C.-H. (2019). Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks. *IEEE Access*, *7*(NA), 31068-31082. https://doi.org/10.1109/access.2019.2902843

[45]. Masud, R. (2025). Integrating Agile Project Management and Lean Industrial Practices A Review For Enhancing Strategic Competitiveness In Manufacturing Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 895–924. https://doi.org/10.63125/0yjss288

[46]. Md Arif Uz, Z., & Elmoon, A. (2023). Adaptive Learning Systems For English Literature Classrooms: A Review Of AI-Integrated Education Platforms. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 56-86. https://doi.org/10.63125/a30ehr12

[47]. Md Arman, H. (2025). Artificial Intelligence-Driven Financial Analytics Models For Predicting Market Risk And Investment Decisions In U.S. Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1066–1095. https://doi.org/10.63125/9csehp36

[48]. Md Ismail, H. (2022). Deployment Of AI-Supported Structural Health Monitoring Systems For In-Service Bridges Using IoT Sensor Networks. *Journal of Sustainable Development and Policy*, *1*(04), 01-30. https://doi.org/10.63125/j3sadb56

[49]. Md Ismail, H. (2024). Implementation Of AI-Integrated IOT Sensor Networks For Real-Time Structural Health Monitoring Of In-Service Bridges. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 33-71. https://doi.org/10.63125/0zx4ez88

[50]. Md Jakaria, T., Md, A., Zayadul, H., & Emdadul, H. (2025). Advances In High-Efficiency Solar Photovoltaic Materials: A Comprehensive Review Of Perovskite And Tandem Cell Technologies. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 201-225. https://doi.org/10.63125/5amnvb37

[51]. Md Mesbaul, H. (2024). Industrial Engineering Approaches to Quality Control In Hybrid Manufacturing A Review Of Implementation Strategies. *International Journal of Business and Economics Insights*, *4*(2), 01-30. https://doi.org/10.63125/3xcabx98

[52]. Md Mohaiminul, H. (2025). Federated Learning Models for Privacy-Preserving AI In Enterprise Decision Systems. *International Journal of Business and Economics Insights*, *5*(3), 238– 269. https://doi.org/10.63125/ry033286

[53]. Md Mominul, H. (2025). Systematic Review on The Impact Of AI-Enhanced Traffic Simulation On U.S. Urban Mobility And Safety. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 833–861. https://doi.org/10.63125/jj96yd66

[54]. Md Omar, F. (2024). Vendor Risk Management In Cloud-Centric Architectures: A Systematic Review Of SOC 2, Fedramp, And ISO 27001 Practices. *International Journal of Business and Economics Insights*, *4*(1), 01-32. https://doi.org/10.63125/j64vb122

[55]. Md Rezaul, K. (2021). Innovation Of Biodegradable Antimicrobial Fabrics For Sustainable Face Masks Production To Reduce Respiratory Disease Transmission. *International Journal of Business and Economics Insights*, *1*(4), 01–31. https://doi.org/10.63125/ba6xzq34

[56]. Md Rezaul, K. (2025). Optimizing Maintenance Strategies in Smart Manufacturing: A Systematic Review Of Lean Practices, Total Productive Maintenance (TPM), And Digital Reliability. *Review of Applied Science and Technology*, *4*(02), 176-206. https://doi.org/10.63125/np7nnf78

[57]. Md Rezaul, K., & Md Takbir Hossen, S. (2024). Prospect Of Using AI- Integrated Smart Medical Textiles For Real-Time Vital Signs Monitoring In Hospital Management & Healthcare Industry. *American Journal of Advanced Technology and Engineering Solutions*, *4*(03), 01-29. https://doi.org/10.63125/d0zkrx67

[58]. Md Rezaul, K., & Rony, S. (2025). A Framework-Based Meta-Analysis of Artificial Intelligence-Driven ERP Solutions For Circular And Sustainable Supply Chains. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 432-464. https://doi.org/10.63125/jbws2e49

[59]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[60]. Md Zahin Hossain, G., Md Khorshed, A., & Md Tarek, H. (2023). Machine Learning For Fraud Detection In Digital Banking: A Systematic Literature Review. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 37–61. https://doi.org/10.63125/913ksy63

[61]. Md. Hasan, I. (2025). A Systematic Review on The Impact Of Global Merchandising Strategies On U.S. Supply Chain Resilience. *International Journal of Business and Economics Insights*, *5*(3), 134–169. https://doi.org/10.63125/24mymg13

[62]. Md. Milon, M. (2025). A Systematic Review on The Impact Of NFPA-Compliant Fire Protection Systems On U.S. Infrastructure Resilience. *International Journal of Business and Economics Insights*, *5*(3), 324–352. https://doi.org/10.63125/ne3ey612

[63]. Md. Rabiul, K. (2025). Artificial Intelligence-Enhanced Predictive Analytics for Demand Forecasting In U.S. Retail Supply Chains. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 959–993. https://doi.org/10.63125/gbkf5c16

[64]. Md. Sakib Hasan, H. (2023). Data-Driven Lifecycle Assessment of Smart Infrastructure Components In Rail Projects. *American Journal of Scholarly Research and Innovation*, *2*(01), 167-193. https://doi.org/10.63125/wykdb306

[65]. Md. Sakib Hasan, H., & Abdul, R. (2025). Artificial Intelligence and Machine Learning Applications In Construction Project Management: Enhancing Scheduling, Cost Estimation, And Risk Mitigation. *International Journal of Business and Economics Insights*, *5*(3), 30–64. https://doi.org/10.63125/jrpjje59

[66]. Md. Tahmid Farabe, S. (2025). The Impact of Data-Driven Industrial Engineering Models On Efficiency And Risk Reduction In U.S. Apparel Supply Chains. *International Journal of Business and Economics Insights*, *5*(3), 353–388. https://doi.org/10.63125/y548hz02

[67]. Md.Kamrul, K., & Md Omar, F. (2022). Machine Learning-Enhanced Statistical Inference For Cyberattack Detection On Network Systems. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 65-90. https://doi.org/10.63125/sw7jzx60

[68]. Mohammad Shoeb, A., & Reduanul, H. (2023). AI-Driven Insights for Product Marketing: Enhancing Customer Experience And Refining Market Segmentation. *American Journal of Interdisciplinary Studies*, *4*(04), 80-116. https://doi.org/10.63125/pzd8m844

[69]. Momena, A. (2025). Impact Of Predictive Machine Learning Models on Operational Efficiency And Consumer Satisfaction In University Dining Services. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 376-403. https://doi.org/10.63125/5tjkae44

[70]. Momena, A., & Sai Praveen, K. (2024). A Comparative Analysis of Artificial Intelligence-Integrated BI Dashboards For Real-Time Decision Support In Operations. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 158-191. https://doi.org/10.63125/47jjv310

[71]. Mubashir, I. (2025). Analysis Of AI-Enabled Adaptive Traffic Control Systems For Urban Mobility Optimization Through Intelligent Road Network Management. *Review of Applied Science and Technology*, *4*(02), 207-232. https://doi.org/10.63125/358pgg63

[72]. Mubashir, I., & Jahid, M. K. A. S. R. (2023). Role Of Digital Twins and Bim In U.S. Highway Infrastructure Enhancing Economic Efficiency And Safety Outcomes Through Intelligent Asset Management. *American Journal of Advanced Technology and Engineering Solutions*, *3*(03), 54-81. https://doi.org/10.63125/hftt1g82

[73]. Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. (2015). Deep learning applications and challenges in big data analytics. *Journal of Big Data*, *2*(1), 1-21. https://doi.org/10.1186/s40537-014-0007-7

[74]. Nejabatkhah, F., Li, Y. W., Liang, H., & Ahrabi, R. R. (2020). Cyber-Security of Smart Microgrids: A Survey. *Energies*, *14*(1), 27-NA. https://doi.org/10.3390/en14010027

[75]. Omar Muhammad, F. (2024). Advanced Computing Applications in BI Dashboards: Improving Real-Time Decision Support For Global Enterprises. *International Journal of Business and Economics Insights*, *4*(3), 25-60. https://doi.org/10.63125/3x6vpb92

[76]. Pankaz Roy, S. (2025). Artificial Intelligence Based Models for Predicting Foodborne Pathogen Risk In Public Health Systems. *International Journal of Business and Economics Insights*, *5*(3), 205–237. https://doi.org/10.63125/7685ne21

[77]. Perera, C., Zaslavsky, A., Compton, M., Christen, P., & Georgakopoulos, D. (2013). SKG - Semantic-Driven Configuration of Internet of Things Middleware. *2013 Ninth International Conference on Semantics, Knowledge and Grids*, *NA*(NA), 66-73. https://doi.org/10.1109/skg.2013.9

[78]. Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M., & Ramos, F. (2021). SPEAR SIEM: A Security Information and Event Management system for the Smart Grid. *Computer Networks*, *193*(NA), 108008-NA. https://doi.org/10.1016/j.comnet.2021.108008

[79]. Rahman, S. M. T. (2025). Strategic Application of Artificial Intelligence In Agribusiness Systems For Market Efficiency And Zoonotic Risk Mitigation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 862–894. https://doi.org/10.63125/8xm5rz19

[80]. Rakibul, H. (2025). The Role of Business Analytics In ESG-Oriented Brand Communication: A Systematic Review Of Data-Driven Strategies. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1096– 1127. https://doi.org/10.63125/4mchj778

[81]. Razia, S. (2022). A Review Of Data-Driven Communication In Economic Recovery: Implications Of ICT-Enabled Strategies For Human Resource Engagement. *International Journal of Business and Economics Insights*, *2*(1), 01-34. https://doi.org/10.63125/7tkv8v34

[82]. Razia, S. (2023). AI-Powered BI Dashboards In Operations: A Comparative Analysis For Real-Time Decision Support. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 62–93. https://doi.org/10.63125/wqd2t159

[83]. Reduanul, H. (2023). Digital Equity and Nonprofit Marketing Strategy: Bridging The Technology Gap Through Ai-Powered Solutions For Underserved Community Organizations. *American Journal of Interdisciplinary Studies*, *4*(04), 117-144. https://doi.org/10.63125/zrsv2r56

[84]. Reduanul, H. (2025). Enhancing Market Competitiveness Through AI-Powered SEO And Digital Marketing Strategies In E-Commerce. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 465-500. https://doi.org/10.63125/31tpjc54

[85]. Rekeraho, A., Cotfas, D. T., Cotfas, P. A., Bălan, T. C., Tuyishime, E., & Acheampong, R. (2023). Cybersecurity challenges in IoT-based smart renewable energy. *International Journal of Information Security*, *23*(1), 101-117. https://doi.org/10.1007/s10207-023-00732-9

[86]. Rony, M. A. (2025). AI-Enabled Predictive Analytics And Fault Detection Frameworks For Industrial Equipment Reliability And Resilience. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 705–736. https://doi.org/10.63125/2dw11645

[87]. Saba, A. (2025). Artificial Intelligence Based Models For Secure Data Analytics And Privacy-Preserving Data Sharing In U.S. Healthcare And Hospital Networks. *International Journal of Business and Economics Insights*, *5*(3), 65–99. https://doi.org/10.63125/wv0bqx68

[88]. Sabuj Kumar, S. (2025). AI Driven Predictive Maintenance in Petroleum And Power Systems Using Random Forest Regression Model For Reliability Engineering Framework. *American Journal of Scholarly Research and Innovation*, *4*(01), 363-391. https://doi.org/10.63125/477x5t65

[89]. Sadia, T. (2022). Quantitative Structure-Activity Relationship (QSAR) Modeling of Bioactive Compounds From Mangifera Indica For Anti-Diabetic Drug Development. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 01-32. https://doi.org/10.63125/ffkez356

[90]. Sadia, T. (2023). Quantitative Analytical Validation of Herbal Drug Formulations Using UPLC And UV-Visible Spectroscopy: Accuracy, Precision, And Stability Assessment. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 01–36. https://doi.org/10.63125/fxqpds95

[91]. Sahoo, S., & Mishra, S. (2019). A Distributed Finite-Time Secondary Average Voltage Regulation and Current Sharing Controller for DC Microgrids. *IEEE Transactions on Smart Grid*, *10*(1), 282-292. https://doi.org/10.1109/tsg.2017.2737938

[92]. Sai Praveen, K. (2025). AI-Driven Data Science Models for Real-Time Transcription And Productivity Enhancement In U.S. Remote Work Environments. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 801–832. https://doi.org/10.63125/gzyw2311

[93]. Sai, V., & Mickle, M. H. (2013). Low power 8051-MISA-based remote execution unit architecture for IoT and RFID applications. *International Journal of Circuits and Architecture Design*, *1*(1), 4-NA. https://doi.org/10.1504/ijcad.2013.057459

[94]. Sanjai, V., Sanath Kumar, C., Maniruzzaman, B., & Farhana Zaman, R. (2023). Integrating Artificial Intelligence in Strategic Business Decision-Making: A Systematic Review Of Predictive Models. *International Journal of Scientific Interdisciplinary Research*, *4*(1), 01-26. https://doi.org/10.63125/s5skge53

[95]. Shaikat, B. (2025). Artificial Intelligence–Enhanced Cybersecurity Frameworks for Real-Time Threat Detection In Cloud And Enterprise. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 737–770. https://doi.org/10.63125/yq1gp452

[96]. Sharma, S. K., & Wang, X. (2020). Towards Massive Machine Type Communications in Ultra-Dense Cellular IoT Networks: Current Issues and Machine Learning-Assisted Solutions. *IEEE Communications Surveys & Tutorials*, *22*(1), 426-471. https://doi.org/10.1109/comst.2019.2916177

[97]. Sheratun Noor, J., Md Redwanul, I., & Sai Praveen, K. (2024). The Role of Test Automation Frameworks In Enhancing Software Reliability: A Review Of Selenium, Python, And API Testing Tools. *International Journal of Business and Economics Insights*, *4*(4), 01–34. https://doi.org/10.63125/bvv8r252

[98]. Shrivastava, S., & Subudhi, B. (2019). Distributed, fixed-time, and bounded control for secondary voltage and frequency restoration in islanded microgrids. *IET Smart Grid*, *2*(2), 260-268. https://doi.org/10.1049/iet-stg.2018.0115

[99]. Singh, D., Tripathi, G., & Jara, A. J. (2014). WF-IoT - A survey of Internet-of-Things: Future vision, architecture, challenges and services. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, *NA*(NA), 287-292. https://doi.org/10.1109/wf-iot.2014.6803174

[100]. Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments. *IEEE Transactions on Network and Service Management*, *18*(2), 1137-1151. https://doi.org/10.1109/tnsm.2021.3078381

[101]. Sosnovskiy, Y., Lapina, M., Lapin, V. G., & Mecella, M. (2021). Software tools communication process models for Modbus TCP/RTU for diagnostics using machine learning approaches. *IOP Conference Series: Materials Science and Engineering*, *1069*(1), 012033-NA. https://doi.org/10.1088/1757-899x/1069/1/012033

[102]. Sridhar, S., & Govindarasu, M. (2014). Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid*, *5*(2), 580-591. https://doi.org/10.1109/tsg.2014.2298195

[103]. Syed Zaki, U. (2025). Digital Engineering and Project Management Frameworks For Improving Safety And Efficiency In US Civil And Rail Infrastructure. *International Journal of Business and Economics Insights*, *5*(3), 300–329. https://doi.org/10.63125/mxgx4m74

[104]. Teymouri, A., Mehrizi-Sani, A., & Liu, C.-C. (2018). IECON - Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability. *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, *NA*(NA), 2872-2877. https://doi.org/10.1109/iecon.2018.8591583

[105]. Tonoy Kanti, C. (2025). AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 675–704. https://doi.org/10.63125/137k6y79

[106]. Volkova, A., Niedermeier, M., Basmadjian, R., & de Meer, H. (2019). Security Challenges in Control Network Protocols: A Survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 619-639. https://doi.org/10.1109/comst.2018.2872114

[107]. Yang, Y., Pranggono, B., Littler, T., Yao, Z. Q., Eul Gyu Im, N. A., McLaughlin, K., Wang, H. F., & Sezer, S. (2012). Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems. *International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012)*, *NA*(NA), 138-138. https://doi.org/10.1049/cp.2012.1831

[108]. Zhang, F., & Mu, L. (2019). New protection scheme for internal fault of multi-microgrid. *Protection and Control of Modern Power Systems*, *4*(1), 1-12. https://doi.org/10.1186/s41601-019-0127-3

[109]. Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S.-P. (2014). SOCA - IoT Security: Ongoing Challenges and Research Opportunities. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, *NA*(NA), 230-234. https://doi.org/10.1109/soca.2014.58

[110]. Zobayer, E. (2025). Impact of Advanced Lubrication Management Systems on Equipment Longevity And Operational Efficiency In Smart Manufacturing Environments. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 618–653. https://doi.org/10.63125/r0n6bc88