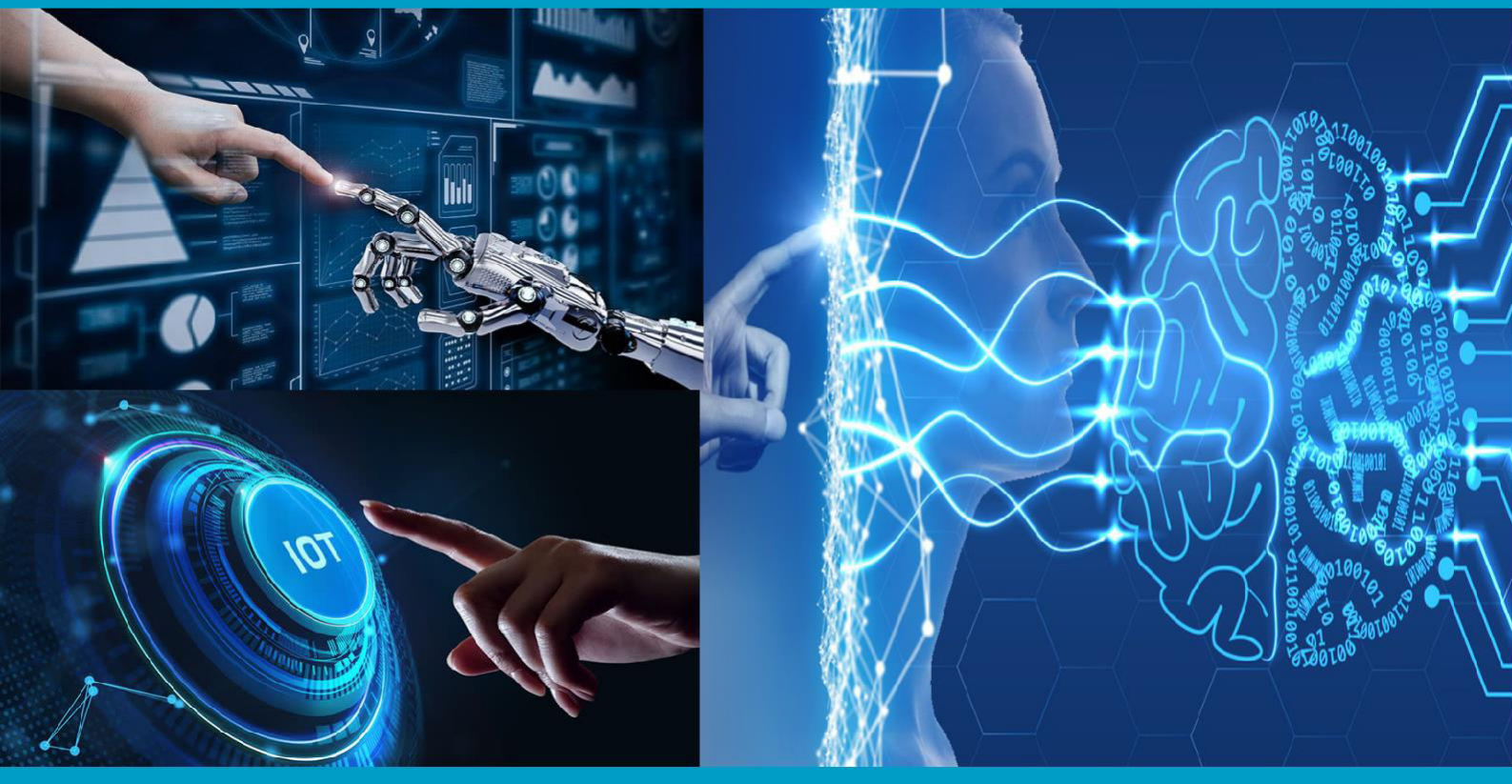
IJMRSETM

e-ISSN: 2395 - 7639




# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

## IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 12, Issue 5, May 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.214

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 5, May 2025 |

# Advancements and Challenges in Digital Substation Systems: A Comprehensive Review of Architectures, Communication, Protection, and Cyber security

**Prof. Pankaj M Mohan[1], Prof. Sunil R Pawar[2], Prof. Sanjay B Pawar[3]**

Faculty, K K Wagh Polytechnic, Nashik, Maharashtra, India

**ABSTRACT:** The global power grid is currently undergoing a profound transformation, shifting from traditional, hardwired substations to sophisticated Digital Substation Systems (DSS). This evolution is driven by an urgent need for heightened reliability, improved efficiency, and more advanced control capabilities. This comprehensive review draws upon nineteen pivotal research papers, offering an in-depth examination of DSS, encompassing their architectural evolution, communication protocols, protection schemes, and the increasingly critical domain of cyber security. The collective body of work reveals substantial progress in operational speed, cost-effectiveness, and interoperability, largely attributable to the adoption of standards like IEC 61850 and the integration of Internet of Things (IoT) technologies. Yet, this progress is accompanied by persistent challenges, including network latency, maintaining data integrity, ensuring seamless multi-vendor interoperability, and confronting the escalating threat of cyber-attacks, particularly insidious insider threats . The proposed solutions span a wide spectrum, from optimized network topologies and cutting-edge machine learning-based anomaly detection systems to robust cryptographic authentication mechanisms for safeguarding critical data. This analysis aims to provide a holistic perspective on the current state of DSS, emphasizing the intricate interdependencies among technological components and their impact on operational resilience, while also charting essential future research directions to cultivate a more robust, secure, and intelligent energy infrastructure [1].

## I. INTRODUCTION

The shift from conventional, electromechanical substations to Digital Substation Systems (DSS) represents a monumental leap in the modernization of power grids. This transition is not merely an upgrade but a fundamental necessity, driven by the ever-increasing demands for grid reliability, operational efficiency, and sophisticated control in a rapidly evolving energy landscape. DSS harness the power of digital communication, intelligent electronic devices (IEDs), and advanced automation to replace cumbersome hardwired connections, thereby unlocking unprecedented levels of data visibility and control. This report offers a thorough, paper-by-paper examination of the latest breakthroughs and enduring challenges within DSS . Our focus spans their architectural designs, the protocols governing their communications, the intricacies of their protection schemes, and the paramount importance of cyber security. By meticulously dissecting these key research contributions, this review seeks to synthesize core findings, discern emerging trends, illuminate the complex interdependencies among various components, and ultimately, outline the future research pathways vital for forging a resilient and secure digital energy infrastructure [1].

## II. LITERATURE REVIEW

The journey of Digital Substation Systems (DSS) is a complex narrative, marked by significant technological strides and persistent hurdles across multiple domains. This literature review synthesizes insights gleaned from nineteen distinct research papers, organizing their contributions into several thematic pillars: Architectural Evolution and Modularity, Communication Protocols and Network Performance, Advanced Protection Schemes, Cybersecurity Threats and Mitigation, and the Transformative Role of IoT and Simulation in Asset Management [1].

### 2.1. ARCHITECTURAL EVOLUTION AND MODULARITY

The fundamental transformation of substation design, moving away from traditional hardwired systems towards digital architectures, is a recurrent and central theme in the literature [1]. A study in "A Modular, Scalable Automation System for a Distribution Substation" [2] vividly illustrates the limitations of conventional distribution systems, which are often plagued by frequent power interruptions and interoperability issues stemming from proprietary protocols [2]. To counter these shortcomings, the paper introduces a Modular, Scalable Automation System (MSAS), envisioned as a

"future-proof building block" [2]. This system is meticulously structured around three primary cabinets—the Substation Automation Device, Communications Device, and Remote Automation Device Cabinets—and operates across three distinct communication levels: Station, Bay, and Process [2]. This inherent modularity not only promises scalability and cost-effectiveness through design standardization but also significantly enhances interoperability, ultimately leading to swifter service restoration and improved system reliability [2]. Intriguingly, the modular design is also shown to bolster cyber security, facilitating easier isolation of compromised components and streamlining security configurations [2].

Delving into the practicalities of this architectural shift, "Bay Control Unit in an IEC 61850 Environment: A Generalized and Systematic Process Flow for Optimized Configuration" [7] addresses a crucial void in previous research [7]. It provides a detailed, systematic process for configuring Bay Control Units (BCUs) within an IEC 61850 environment, a procedure validated by actual commissioning experience [7]. This work underscores the profound transition from hardware-centric to software-centric interlocking, where BCUs incorporate "soft" electrical interlocks that redundantly complement traditional hardwired mechanisms [7]. This approach, while offering increased flexibility and reduced wiring, simultaneously demands rigorous validation to ensure safety [7]. The paper further advocates for the use of UNICAST SNTP mode and optimized data sets, recognizing their importance for maintaining network traffic efficiency in time-critical systems [7].

The economic and operational advantages of digital architectures are further emphasized in "Reverse Blocking Over Current Busbar Protection Scheme Based on IEC 61850 Architecture" [18]. This research details the implementation of a Reverse Blocking Overcurrent Busbar Protection (RBOC-BBP) scheme, which leverages IEC 61850 GOOSE and SV protocols [18]. By replacing complex secondary wiring with a digital local area network (LAN), this digital approach yields substantial engineering benefits, including more flexible diagnostics, reduced labor, and considerable cost savings from less copper wiring and smaller panel footprints [18].

### 2.2. COMMUNICATION PROTOCOLS AND NETWORK PERFORMANCE

The very lifeblood of any DSS is its robust and efficient communication infrastructure. Here, IEC 61850 stands out as the predominant standard, a cornerstone for achieving multi-vendor interoperability and facilitating real-time data exchange [1]. "Comparative Analysis of DNP3 and IEC 61850 from Architectural, Data Mapping, Data Modeling and Data Reporting View" [8] offers a meticulous comparison between DNP3 (prevalent in American utilities) and IEC 61850 (widely adopted in Europe) [8]. The paper highlights IEC 61850's flexible architecture, featuring distinct process and station buses, its publish-subscribe communication model (a stark contrast to DNP3's Master/Slave approach), and its "self-descriptive" data model [8]. These attributes collectively lead to a significant reduction in configuration time and physical reconfiguration efforts, potentially cutting setup time by an impressive 80-85% [8]. This fundamental shift towards a decentralized, event-driven communication model is deemed essential for achieving the ultra-low latency and higher availability demanded by modern Substation Automation Systems (SAS) [8].

The practical implications of IEC 61850's performance are vividly demonstrated in "A Fast and Reliable Blocked Bus Bar Protection Scheme Leveraging on Sampled Value and GOOSE Protection based on IEC 61850 Architecture". This study reveals that digital protection systems can react 10-20 milliseconds faster than their conventional counterparts for busbar faults, with response times as low as 10-13 ms compared to 45-47 ms in traditional systems . This speed is largely attributed to the instantaneous nature of GOOSE messages and the high-bandwidth capabilities of SV packets. Despite these impressive gains, the paper prudently acknowledges the ongoing need for further multi-vendor experimentation to solidify end-user confidence [1].

Optimizing network performance is paramount for ensuring real-time operations [1]. "Analysis for the Improvement of IEC 61850 Based Substation Communications Using OPNET" tackles the challenge of adhering to IEC 61850's stringent 4-millisecond end-to-end (ETE) delay requirement, particularly when transmitting larger data packets. Through OPNET simulations, the research proposes and evaluates a mesh network topology. The findings are compelling: this topology successfully transmits large packets (up to 16,384 bytes) well within the 4-ms limit, consistently outperforming Star, Ring, and Cascaded topologies (e.g., achieving 0.40 ms for mesh versus 0.52 ms for cascaded with 4,096-byte packets). This underscores that effective network design necessitates a holistic consideration of packet size, topology, and traffic patterns [4].

However, the path to seamless digital communication is not without its obstacles [1]. "Comparison between Wired versus Wireless Mode of Digital Protection Scheme Leveraging on PRP Topology" investigates the performance of wired and wireless digital protection schemes, employing Parallel Redundancy Protocol (PRP) topology to mitigate latencies, data losses, and packet clogging in Wide Area Network (WAN) substations. While the study confirms PRP's efficacy in providing redundancies and seamless failover (outperforming RSTP), it also highlights a critical

observation: IEDs struggled to cope with real-world network imperfections, exhibiting an average delay of 18 milliseconds and even instances of malfunction due to these delays and errors . This suggests that while advanced protocols like PRP enhance reliability, the IEDs themselves require more sophisticated internal mechanisms to robustly handle residual network impairments [9].

Further refining communication efficiency, "Mapping IEC 61850 GOOSE Messages into Time-Sensitive Networking" explores the precise mapping of IEC 61850 GOOSE messages into Time-Sensitive Networking (TSN) while adhering to real-time and fault-tolerance requirements. The paper astutely identifies two distinct GOOSE traffic classes—GOOSE-HP for new events and GOOSE-LP for heartbeat messages—and proposes a more efficient mapping strategy. This involves allocating SV messages to a high-priority Protected Window (priority 7) and assigning GOOSE-HP and GOOSE-LP messages to an Unprotected Window with slightly lower priorities (6 and 5, respectively) [12].

### 2.3. ADVANCED PROTECTION SCHEMES

Digitalization has profoundly enhanced the speed, accuracy, and overall reliability of substation protection systems [1]. "Improvement in Arc Flash Protection Based on IEC 61850 Protocol" illustrates this by focusing on arc flash protection. The research demonstrates that digital SAS, built upon IEC 61850, can instantaneously cut off power supply during an arc flash event, thereby offering improved protection times and optimized maintenance costs compared to conventional methods. Nevertheless, the paper points out those challenges persist, particularly with multi-vendor equipment, which can lead to packet clogging and communication delays [11].

The foundational accuracy of measurements remains paramount in digital systems [1]. "Accuracy and Suitability of the CT Circuit in the REF and Differential Relay Functions in the Digital Substation System" meticulously evaluates the performance of Current Transformer (CT) circuits in Restricted Earth Fault (REF) and differential relay functions within DSS. Following a system perturbation, the repositioning of a neutral LV CT was rigorously validated through comprehensive stability tests, confirming the circuit's integrity and stability. This work underscores a crucial point: even as communication becomes digital, the reliability of protection systems ultimately hinges on the precision of the initial analog-to-digital conversion, emphasizing the enduring need for highly accurate analog front-ends. Moreover, digitalization facilitates a more precise definition of fault zones, which is vital for achieving system selectivity [3].

As previously noted, "Reverse Blocking over Current Busbar Protection Scheme Based on IEC 61850 Architecture" further reinforces the reliability and effectiveness of digital RBOC-BBP. This scheme achieves tripping times that are 10 ms faster for busbar faults compared to conventional relays. Its advantages include instantaneous GOOSE/SV flow, an expandable LAN, inherent connection supervision, and the ability to maintain continuous operation until human intervention can be arranged [18].

### 2.4. CYBERSECURITY THREATS AND MITIGATION

The convergence of Information Technology (IT) and Operational Technology (OT) systems within DSS introduces a new frontier of significant cyber security vulnerabilities [1]. "Cyber-Physical Testbed Frameworks for Digital Infrastructure" directly addresses the escalating susceptibility of digital substations to unauthorized breaches . The paper critically observes that cybersecurity was not an initial design priority in the IEC 61850 standard, leading to inherent weaknesses. It highlights the particular vulnerability of Sampled Value (SV) messages—being non-routable, non-blocking, plaintext (unencrypted), and multicast—to various attacks, including replay, spoofing, and Denial-of-Service (DoS) . To counter these threats, the paper proposes integrating Message Authentication Code (MAC) technology, specifically Hash-based Message Authentication Code (HMAC) and Galois Message Authentication Code (GMAC), into SV communications to ensure data integrity and authenticity. A stringent requirement for these MAC operations is their completion within 3 milliseconds to meet real-time operational demands. However, a notable limitation is the potential for skilled adversaries to compromise symmetric keys, necessitating future research into more robust key distribution methods [10].

The challenge of detecting subtle, "stealthy" insider attacks, which often modify legitimate messages slightly while mimicking benign patterns, is central to "Anomaly Detection for Insider Attacks from Untrusted Intelligent Electronic Devices in Substation Automation Systems". Traditional detection methods, which typically examine individual packets in isolation, prove inadequate against such sophisticated threats. This paper introduces an innovative detection method that combines feature selection and extraction with a sliding window-based sequential classification mechanism, powered by Bidirectional Long Short-Term Memory (BiLSTM) networks. This approach achieved a remarkably low false-negative rate (FNR) of 0.372% (with a window size of 22 packets and a step size of 1 packet) for previously unseen devices, representing a substantial improvement over traditional models (which showed FNRs as high as 51.921%). The research underscores the critical role of sliding windows, particularly for handling the unbalanced datasets typical in SASs (where benign traffic vastly outnumbers malicious events), and highlights the

impracticality of collecting comprehensive attack datasets for every single IED, thus emphasizing the need for generalizable detection models [5].

Further reinforcing the utility of machine learning in cybersecurity, "ML-based Anomaly Detection System for IEC 61850 Communication in Substations" proposes a supervised ML-based anomaly detection system (ADS) for IEC 61850-based SAS networks. This system employs traffic augmentation and data balancing techniques. Experimental evaluations demonstrate impressive performance, achieving high accuracy and true-positive rates (exceeding 99%) and low false-negative rates (less than 1%). K-Nearest Neighbors (KNN) emerged as the most accurate algorithm, achieving 99.80% detection accuracy for one dataset and 99.84% for another. This work serves as a foundational step towards the real-time implementation of ML-ADS in substation environments [14].

Beyond the core substation, securing the broader smart grid ecosystem is also vital [1]. "SecLoRa: A Secure LoRa Based Communication System for Residential Smart-grids" explores the applicability of LoRa technology for building secure, low-power, and robust communication systems for residential smart-grids, particularly for smart metering. It proposes SecLoRa, a peer-to-peer LoRa-based system with end-to-end AES-256 encryption. The study found the computational cost of encryption/decryption to be negligible compared to packet airtime, though it noted a trade-off between Packet Delivery Ratio (PDR) and airtime, where higher airtime improved PDR and extended maximum distance [19].

### 2.5. ROLE OF IOT AND SIMULATION IN ASSET MANAGEMENT

The integration of Internet of Things (IoT) and advanced simulation tools is proving indispensable for proactive asset management and rigorous system validation within DSS [1]. "Application of Industry 4.0 Technology and Internet of Things in Power Transmission Protection Monitoring and Asset Management" delves into the transformative potential of Industry 4.0 and IoT in enhancing power transmission protection, monitoring, and asset management. The paper advocates for IoT as a cyber-physical system, structured with a three-layered architecture (Device, Data Service, and Application), designed to enable predictive maintenance. This shift from reactive to proactive strategies promises significant benefits, including reduced maintenance and operational costs, fewer outages, and real-time monitoring. The research outlines a stepwise approach for implementing IoT-based asset management, encompassing sensor integration, data collection and validation, quantification of equipment health (leveraging machine learning, fuzzy logic, and natural language processing), and the finalization of asset management strategies . The extensive data collection facilitated by IoT is seen as laying the groundwork for creating comprehensive digital representations, or "digital twins," of physical assets [6].

For rigorous system validation, simulation tools play a crucial role [1]. "Power Systems Simulation and Analysis: A Review on Current Applications and Future Trends in DRTS of Grid-Connected Technologies" reviews Digital Real-Time Simulation (DRTS) and Hardware-In-the-Loop (HIL) simulation in grid-connected technologies. The review highlights HIL's significant advantages in mitigating the risk of damage to real equipment and reducing testing costs, emphasizing its utility in analyzing complex power system behavior without direct real-world experimentation [15].
Practical applications of digital systems for compliance and remote monitoring are exemplified in "Remote Protection Reading System Implementation Experiences in Cruz Solar Substation". This article details the successful implementation of a Remote Protection Reading System (SLRP) in a Chilean solar substation. The system effectively acquires oscillographic records, stores protection settings, and registers events in a Linux repository, making them accessible via remote SSH within 60 seconds. This demonstrates the tangible benefits of digital systems in meeting stringent operational and regulatory requirements [16].

Finally, assessing the resilience of these complex cyber-physical systems is vital [1]. "Resilience Assessment and Improvement for Cyber-Physical Power Systems under Typhoon Disasters" proposes a framework for evaluating CPPS resilience, particularly under extreme weather events like typhoons, by considering the deep coupling between cyber and physical layers. The framework analyses the interaction of information flow and energy flow during failure periods from both geographical and control coupling perspectives. This method is shown to improve quantization accuracy compared to conventional power system assessment methods, offering a more precise evaluation of enhancement measures at different stages [17].

## III. CONCLUSION

The movement to Digital Substation Systems (DSS) indicates a real shift in the power grid infrastructure and the potential for considerable operational speed, efficiency, and cost savings achievable through IEC 61850 standards, modular architectures, and improved communication protocols. The digital protection schemes provide remarkably faster fault isolation; the introduction of IoT will enable proactive asset management and "digital twins". This digital

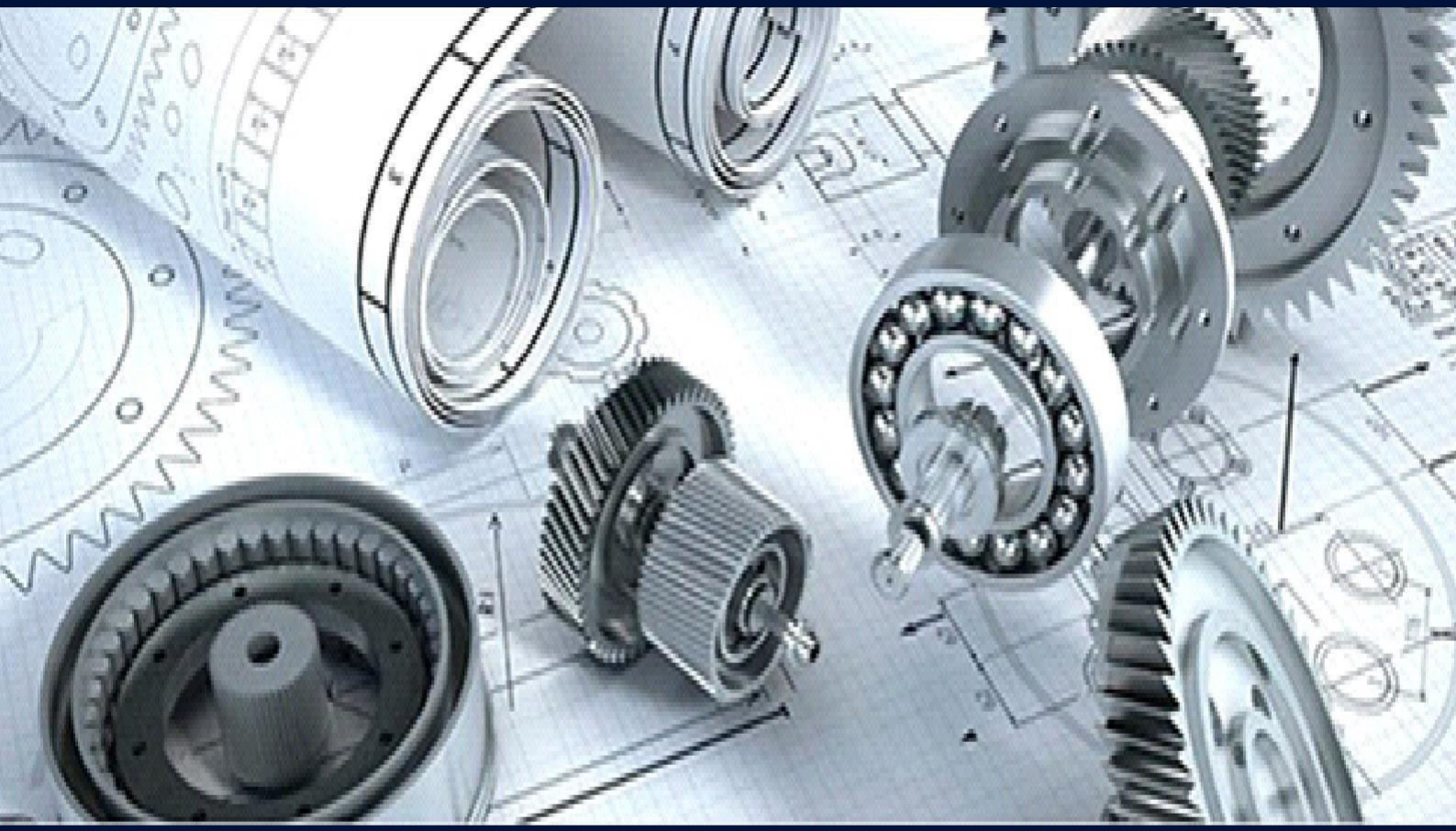
solves countless operational efficiency, but digitalization brings complexity, with cyber security as the critical issue of the digitalization movement as IEC 61850 has known shortcomings and the plaintext protocol has inherent weaknesses, making it vulnerable to "stealthy" insider attacks. Many of the system designs incorporate machine learning-type anomaly detection but there is still work to be done to develop flawless real-time detection systems and network performance with disparate IEDs. Consider also that performance in a Network may be even worse in a growing WAN because of latency and packet loss. Ultimately, the successful outcome of DSS comes down to finding a business case to ensure the maximum economic value is balanced against fiscal prudence to relationships in operational robustness, reliability, and ongoing cyber security needs [1].

## IV. FUTURE WORK

Building upon current research, future work in Digital Substation Systems (DSS) is paramount to ensure robust and secure energy infrastructure. Key areas include advancing interoperability through extensive multi-vendor validation for IEC 61850 technology [1], and fortifying cybersecurity defenses by developing secure key distribution methods and expanding machine learning-based anomaly detection for critical messages [5, 10, 14]. Optimizing network performance with robust redundancy protocols like IEC 62439-3 PRP/HSR is essential to handle latencies and packet loss [9]. Further efforts are needed in enhancing IoT integration for centralized asset management and automated decision-making, requiring comprehensive data analytics platforms and improved sensor deployment [6, 19]. Additionally, refining protection schemes through more practical experiments and detailed testing methodologies for Bay Control Units (BCUs) is crucial [1, 3, 7]. Finally, fostering knowledge sharing among operators and end-users will facilitate the widespread adoption of IEC 61850 [1].

## REFERENCES

[1] A Fast and Reliable Blocked Bus Bar Protection Scheme Leveraging on Sampled Value and GOOSE Protection based on IEC 61850 Architecture.
[2] A Modular, Scalable Automation System for a Distribution Substation.
[3] Accuracy and Suitability of the CT Circuit in the REF and Differential Relay Functions in the Digital Substation System.
[4] Analysis for the Improvement of IEC 61850 Based Substation Communications Using OPNET.
[5] Anomaly Detection for Insider Attacks From Untrusted Intelligent Electronic Devices in Substation Automation Systems.
[6] Application of Industry 4.0 Technology and Internet of Things in Power Transmission Protection Monitoring and Asset Management.
[7] Bay Control Unit in an IEC 61850 Environment: A Generalized and Systematic Process Flow for Optimized Configuration.
[8] Comparative Analysis of DNP3 and IEC 61850 from Architectural, Data Mapping, Data Modeling and Data Reporting View.
[9] Comparison between Wired versus Wireless Mode of Digital Protection Scheme Leveraging on PRP Topology.
[10] Cyber-Physical Testbed Frameworks for Digital Infrastructure.
[11] Improvement in Arc Flash Protection Based on IEC 61850 Protocol.
[12] Mapping IEC 61850 GOOSE Messages into Time-Sensitive Networking.
[13] Method to Quantifying the Logical Node Importance for IEC 61850 Based Substation Automation Systems.
[14] ML-based Anomaly Detection System for IEC 61850 Communication in Substations.
[15] Power Systems Simulation and Analysis: A Review on Current Applications and Future Trends in DRTS of Grid-Connected Technologies.
[16] Remote Protection Reading System Implementation Experiences in Cruz Solar Substation.
[17] Resilience Assessment and Improvement for Cyber-Physical Power Systems Under Typhoon Disasters.
[18] Reverse Blocking Over Current Busbar Protection Scheme Based on IEC 61850 Architecture.
[19] SecLoRa: A Secure LoRa Based Communication System for Residential Smart-grids




# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT



+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com