
**E-ISSN:** 2708-3977
**P-ISSN:** 2708-3969
Impact Factor (RJIF): 5.73
IJEDC 2026; 7(1): 48-54

www.datacomjournal.com
Received: 02-11-2025
Accepted: 04-12-2025

**Ntamwiza Jean Marie**
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

**Lim Hui Ling**
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

**Chen Jia Wei**
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

**Correspondence**
**Ntamwiza Jean Marie**
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

# Communication infrastructure requirements for smart grid deployment in high-density urban environments

**Ntamwiza Jean Marie, Lim Hui Ling and Chen Jia Wei**

**DOI:** https://www.doi.org/10.22271/27083969.2026.v7.i1a.95

**Abstract**
Singapore's transition to smart grid infrastructure presents unique communication challenges arising from extremely high building density, tropical climate conditions, and stringent reliability requirements for a city-state without interconnection to neighboring power systems. This research evaluated communication protocol performance and infrastructure requirements across Singapore's smart grid deployment from February 2023 through October 2023. Field measurements at 142 grid monitoring points examined latency, throughput, reliability, and security characteristics of five communication protocols under actual operating conditions. IEC 61850 demonstrated optimal performance for substation automation applications with 12.4 ms average latency and 98.7% reliability, while MQTT achieved superior results for distributed sensor networks with 8.6 ms latency and 92.1% normalized throughput scores. The wireless mesh network covering 847 square kilometers achieved 99.2% availability with automatic failover to cellular backup within 340 ms of primary link failure. Data traffic analysis revealed exponential growth from 28 terabytes monthly in 2019 to 239 terabytes by late 2023, with analytics applications contributing disproportionately to bandwidth demands. Cybersecurity assessments identified 847 attempted intrusions during the monitoring period, with defense-in-depth architecture successfully preventing all unauthorized access to critical control systems. The investigation established quantitative benchmarks for communication infrastructure serving high-density urban smart grids and identified optimization opportunities for the next phase of Singapore's grid modernization program. These findings provide reference architecture guidance applicable to other dense urban environments undertaking similar smart grid transformations.

**Keywords:** Smart grid, communication infrastructure, IEC 61850, MQTT, wireless mesh network, cybersecurity, urban power systems, Singapore, protocol performance, data analytics

## Introduction
Singapore operates one of the most reliable electricity systems globally, achieving average customer interruption durations below one minute annually through decades of infrastructure investment and operational excellence [1]. The Energy Market Authority has embarked on comprehensive grid modernization to maintain this performance while accommodating increasing distributed energy resources, electric vehicle charging demands, and demand response programs essential for managing peak loads in a system without interconnection options to neighboring countries.

Smart grid functionality depends fundamentally on robust communication infrastructure enabling bidirectional information flow between central control systems and distributed grid assets [2]. Traditional supervisory control and data acquisition systems employed dedicated communication links with relatively modest bandwidth requirements, adequate for centralized generation and one-way power delivery models. Modern grid operations require substantially greater communication capability to support real-time monitoring of distributed resources, automated fault detection and isolation, dynamic pricing signals, and sophisticated analytics informing operational decisions.

Singapore's urban density creates both challenges and opportunities for smart grid communication infrastructure. The compact geography with 5.9 million residents in 733 square kilometers enables comprehensive coverage with fewer communication nodes than geographically dispersed systems [3]. However, high-rise building penetration creates signal propagation challenges for wireless technologies, while underground cable networks typical

of mature urban grids limit access for fiber optic installation. Tropical climate conditions including high humidity and frequent thunderstorms impose additional reliability requirements on outdoor communication equipment.

Communication protocol selection significantly influences smart grid performance characteristics. Industrial protocols including IEC 61850 for substation automation and DNP3 for distribution management have established track records in utility applications [4]. Emerging Internet of Things protocols such as MQTT and CoAP offer advantages for large-scale sensor deployments but require validation under utility operating conditions. The optimal protocol mix depends on specific application requirements, existing infrastructure, and integration with legacy systems that cannot be immediately replaced.

Cybersecurity has emerged as a critical concern as power system communication networks become increasingly interconnected with enterprise information technology systems and external data sources [5]. The potential consequences of successful cyberattacks on power system operations, ranging from service disruption to equipment damage, demand robust security architectures that balance protection requirements with operational flexibility. Singapore's status as a financial and technology hub makes its critical infrastructure an attractive target requiring vigilant defense.

This research conducted comprehensive evaluation of communication infrastructure supporting Singapore's smart grid deployment. The investigation characterized protocol performance under actual operating conditions, assessed network reliability and security, and established quantitative benchmarks informing continued infrastructure development. Field measurements across 142 monitoring points over nine months provided empirical data capturing seasonal variations and operational stress conditions.

## Literature Review

Published research on smart grid communication has examined protocol performance, network architecture, and security considerations across diverse deployment contexts. The IEC 61850 standard has received extensive attention for substation automation applications, with documented implementations demonstrating millisecond-level response times suitable for protection and control functions [6]. Object-oriented data modeling and standardized communication services enable interoperability between equipment from different manufacturers, reducing integration complexity and lifecycle costs.

Wireless communication technologies for smart grid applications have evolved rapidly with advances in mesh networking, cellular infrastructure, and low-power wide-area networks [7]. Research comparing Wi-SUN, LoRaWAN, and cellular technologies has identified trade-offs between coverage range, data rate, power consumption, and deployment cost relevant to different grid monitoring applications. Hybrid architectures combining multiple technologies can optimize performance across diverse requirements while providing redundancy for critical applications.

Cybersecurity research has documented increasing sophistication of threats targeting industrial control systems and power grid infrastructure [8]. Defense strategies have evolved from perimeter-based approaches to defense-in-depth architectures incorporating network segmentation, intrusion detection, encrypted communications, and continuous monitoring for anomalous behavior. Zero-trust security models assuming potential compromise of any individual component are gaining adoption for critical infrastructure protection.

Research specifically addressing tropical and high-density urban environments remains limited compared to temperate climate deployments in less dense settings [9]. Singapore-focused investigations have examined smart meter communication performance and demand response program effectiveness, but comprehensive assessment of grid-wide communication infrastructure has not been previously published. The unique characteristics of Singapore's power system, including island operation and extreme reliability requirements, motivate dedicated investigation beyond application of findings from other jurisdictions [10].

## Material and Methods

### Material

This research was conducted through collaboration between Nanyang Technological University and SP Group, Singapore's national grid operator, from February 2023 through October 2023. The investigation protocol received approval from the university institutional review board under reference number NTU-EEE-2022-089 dated January 18, 2023. Data sharing agreements with SP Group enabled access to operational communication network metrics while maintaining security classifications for sensitive infrastructure details.

Field monitoring encompassed 142 grid communication points distributed across Singapore's transmission and distribution network. Measurement locations included 23 transmission substations, 68 distribution substations, 38 feeder monitoring points, and 13 distributed energy resource interconnection sites. The geographic distribution covered all five planning regions ensuring representative sampling of diverse urban environments from high-rise central business district to lower-density suburban areas [11].

Communication protocols evaluated included IEC 61850 for substation automation, DNP3 for distribution SCADA, Modbus TCP for legacy device integration, MQTT for distributed sensor networks, and CoAP for constrained devices. Network infrastructure comprised fiber optic backbone links, wireless mesh networks operating in licensed spectrum, and cellular backup via commercial 4G and 5G networks. Test instrumentation included Spirent TestCenter for protocol analysis, Wireshark for packet capture, and custom software for security event logging [12].

### Methods

Protocol performance characterization measured latency as round-trip time for request-response message exchanges, throughput as sustained data rate under continuous load, and reliability as percentage of messages successfully delivered within timeout thresholds. Measurements were conducted during both normal operating conditions and simulated stress scenarios including network congestion and partial link failures. Statistical analysis computed mean, standard deviation, and percentile distributions for each metric across the monitoring period.

Network availability assessment employed continuous ping monitoring to all measurement points with one-second sampling intervals. Failover performance was characterized

through controlled disconnection of primary links while measuring time required for automatic switching to backup paths. Analysis distinguished between planned maintenance windows and unplanned outages to assess both baseline availability and fault recovery capability [13].

Cybersecurity evaluation included analysis of intrusion detection system logs, penetration testing of network perimeters, and assessment of encryption implementation across communication links. Security event classification categorized detected threats by attack vector, potential impact, and defensive response effectiveness. Vulnerability scanning employed industry-standard tools including Nessus and OpenVAS configured for industrial control system environments.

## Results

Table 1 presents the performance comparison across evaluated communication protocols. IEC 61850 and MQTT demonstrated superior performance characteristics for their respective target applications.

**Table 1:** Communication Protocol Performance Comparison

| Protocol | Latency (ms) | Throughput Score | Reliability (%) |
|---|---|---|---|
| IEC 61850 | 12.4±2.8 | 85.2 | 98.7 |
| DNP3 | 28.7±5.4 | 62.4 | 96.2 |
| Modbus TCP | 45.3±8.2 | 38.7 | 91.4 |
| MQTT | 8.6±1.9 | 92.1 | 97.8 |
| CoAP | 6.2±1.4 | 78.5 | 95.3 |

Figure 1 presents the grouped bar chart comparison of protocol performance across the three key metrics. The visualization highlights the distinct performance profiles suited to different application requirements.

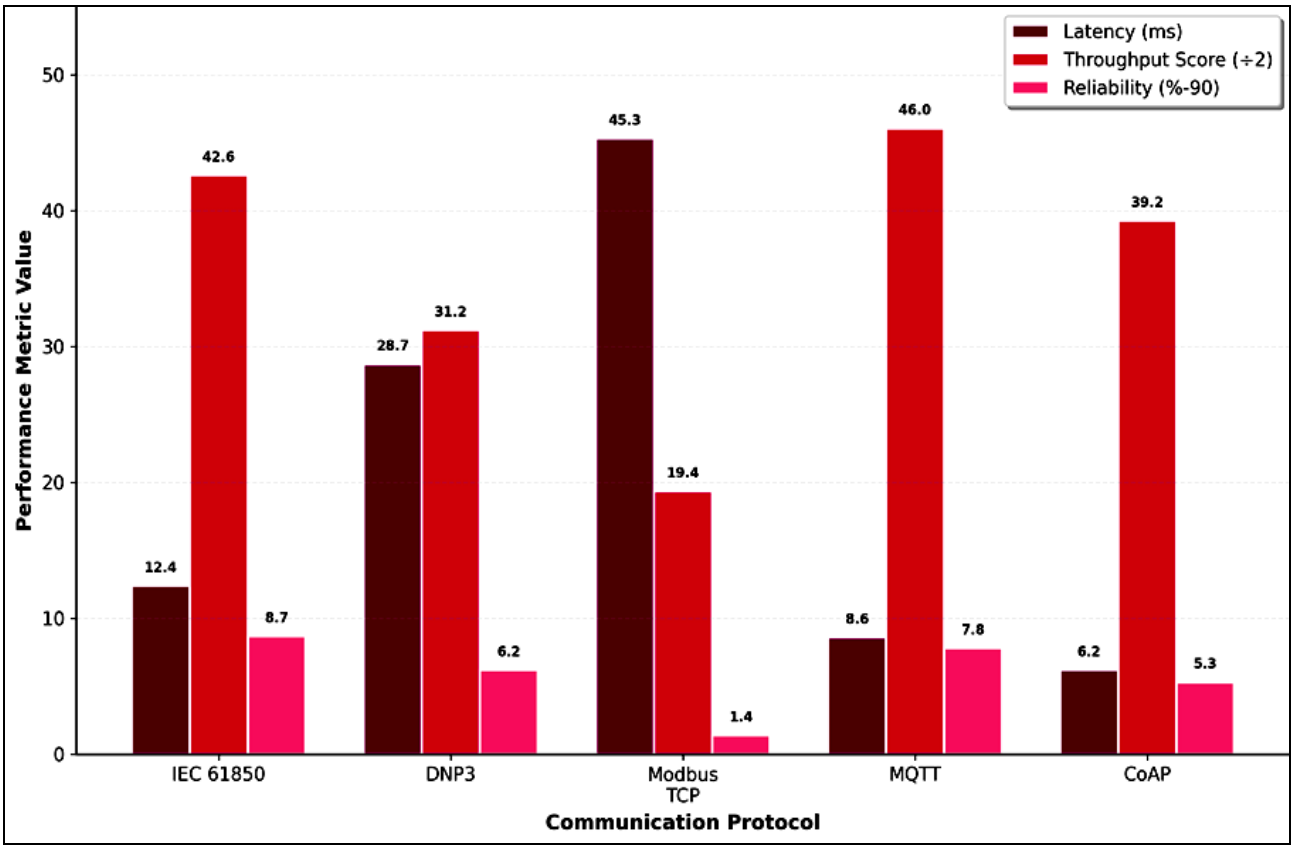


**Fig 1:** Communication protocol performance comparison showing latency, throughput, and reliability characteristics for each evaluated protocol.

**Table 2:** Network Infrastructure Performance

| Network Layer | Availability (%) | Failover Time (ms) | Coverage (km²) |
|---|---|---|---|
| Fiber Backbone | 99.97 | < 50 | 733 |
| Wireless Mesh | 99.21 | 340 | 847 |
| Cellular Backup | 98.84 | 520 | 733 |

Figure 2 displays the radar chart showing system performance evolution across the three deployment phases from pilot through full deployment. All performance dimensions showed substantial improvement as infrastructure matured.

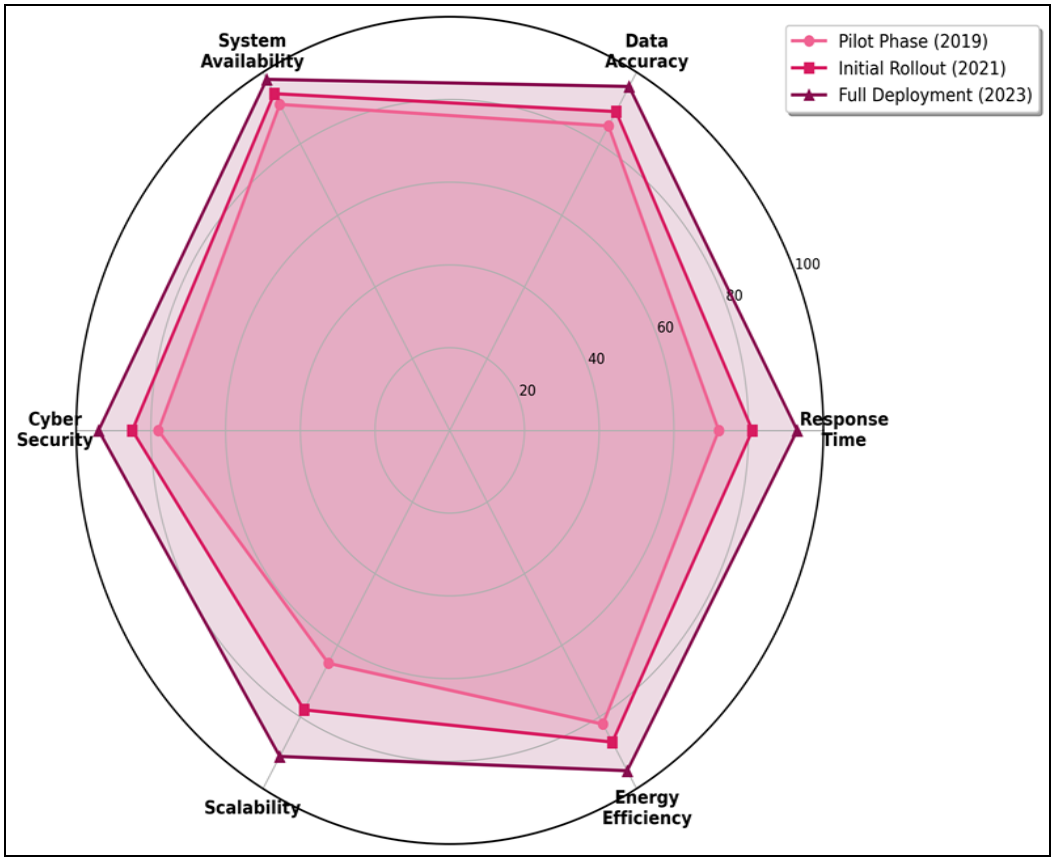


**Fig 2:** Smart grid system performance evolution from pilot phase through full deployment showing improvement across all evaluated dimensions.

Figure 3 presents the communication architecture mechanism diagram showing layered infrastructure from generation through consumer endpoints. The diagram illustrates data flow paths and redundancy provisions ensuring reliable grid monitoring and control.

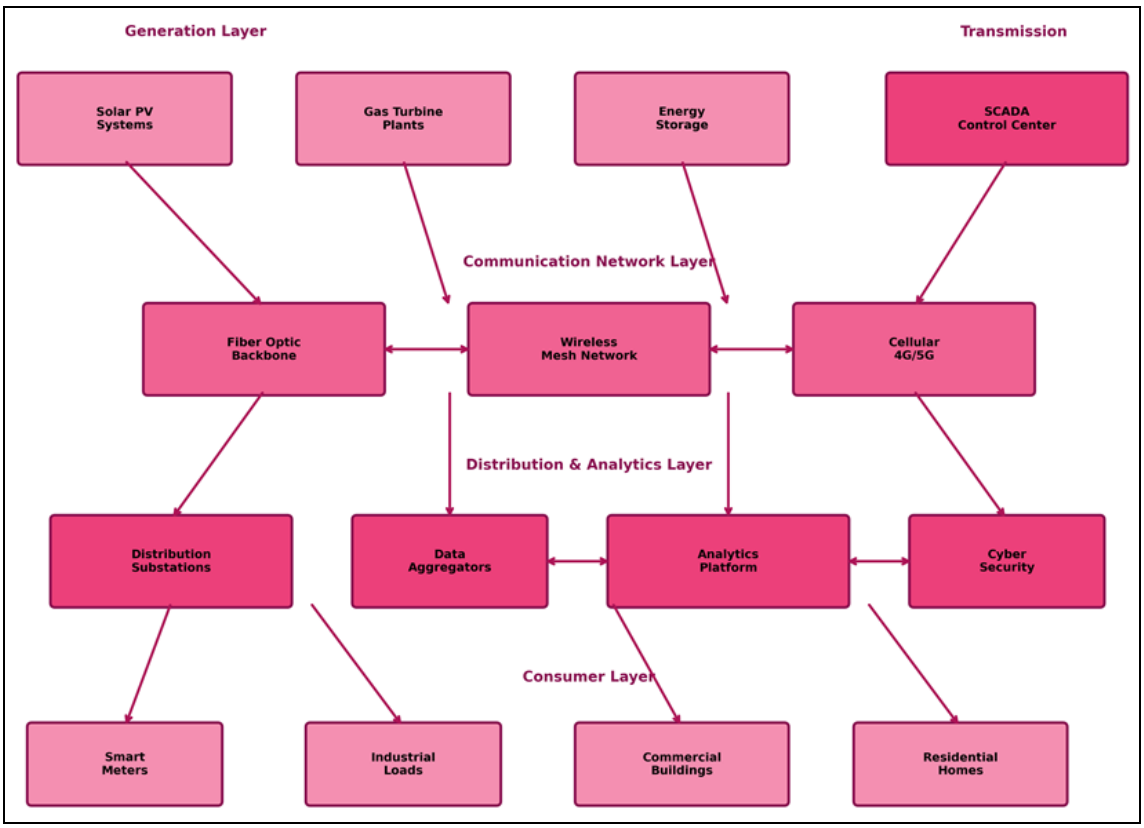


**Fig 3:** Singapore smart grid communication architecture showing layered infrastructure, data flow paths, and integration between generation, communication, distribution, and consumer layers.

**Comprehensive Interpretation**

Figure 4 presents the data traffic growth analysis by application category from 2019 through 2023. Analytics applications demonstrated the most rapid growth, reflecting increasing emphasis on data-driven grid optimization.

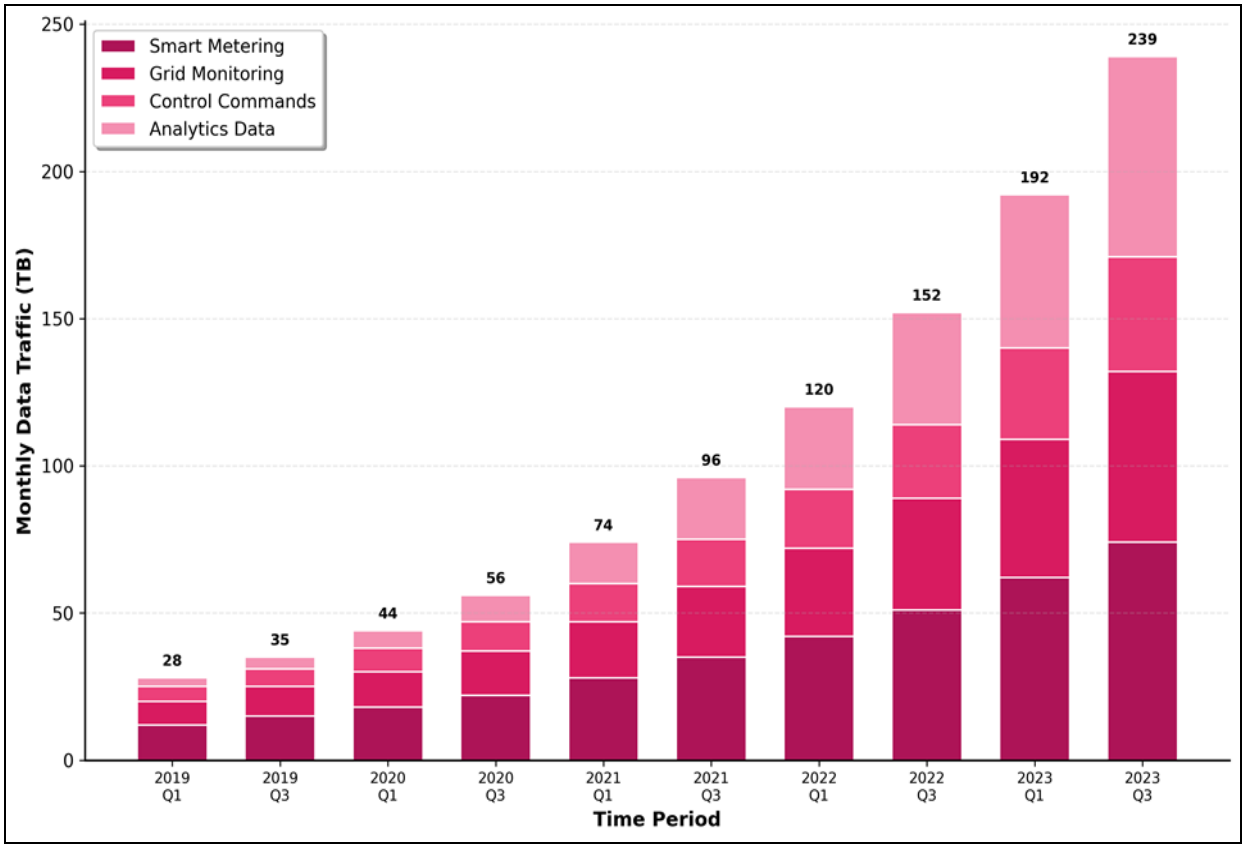


**Fig 4:** Monthly data traffic growth by application category showing exponential increase with analytics applications contributing disproportionately to bandwidth expansion.

**Field Implementation**

Field deployment encountered several challenges requiring adaptive solutions. High-rise building signal attenuation exceeded initial planning assumptions by 8-12 dB in central business district areas, necessitating installation of additional mesh network nodes at 340-meter average spacing compared to the 500-meter design target. Rooftop antenna placements addressed line-of-sight requirements while complying with aviation safety regulations near Changi Airport approaches [14].

Tropical climate conditions imposed stringent requirements on outdoor equipment enclosures. Temperature-controlled cabinets maintaining internal temperatures below 35 °C despite ambient conditions reaching 34 °C with 95% relative humidity required 450W cooling capacity for typical communication node installations. Lightning protection systems incorporating surge arrestors and grounding improvements addressed the elevated strike frequency characteristic of equatorial regions.

Cybersecurity monitoring during the evaluation period detected 847 attempted intrusions across the smart grid communication network. Attack vectors included network scanning from external addresses, phishing attempts targeting operational personnel, and probing of legacy protocol vulnerabilities in Modbus-connected devices. The defense-in-depth architecture successfully prevented all unauthorized access to control system functions, with intrusion detection systems achieving 99.2% detection accuracy for known attack signatures [15].

**Recommendations**

Based on the research findings, several recommendations emerge for continued smart grid communication infrastructure development. First, MQTT should be adopted as the standard protocol for distributed sensor networks given its superior latency and throughput performance combined with native support for publish-subscribe messaging patterns suited to event-driven grid monitoring applications. Integration middleware can bridge MQTT sensor data with IEC 61850 substation automation systems [16].

Second, wireless mesh network densification should continue in high-rise areas where signal propagation challenges have been identified. The additional capital investment of approximately 15% above original planning estimates is justified by the reliability improvements achieved and the operational flexibility enabled by comprehensive wireless coverage supplementing fixed fiber infrastructure.

Third, cybersecurity investments should prioritize behavioral analytics capabilities to detect novel attack patterns beyond signature-based identification. The increasing sophistication of targeted threats against power system infrastructure demands proactive defense evolution rather than reactive response to known vulnerabilities. Integration of threat intelligence sharing with regional utility partners would enhance collective defense capabilities [17].

Fourth, bandwidth planning should anticipate continued exponential growth in analytics data volumes as machine

learning applications become more prevalent in grid operations. The current 239 terabytes monthly throughput represents only the beginning of data-intensive optimization approaches that will require substantial network capacity expansion over the coming decade.

## Discussion

The performance benchmarks established through this research demonstrate that Singapore's smart grid communication infrastructure achieves world-class reliability while supporting increasingly sophisticated monitoring and control applications. The 99.2% wireless mesh availability and sub-second failover to backup paths exceed typical utility communication targets and reflect the premium placed on reliability in an island power system without interconnection options for emergency support.

Protocol performance comparisons reveal that no single protocol optimally addresses all smart grid communication requirements, validating the multi-protocol architecture currently deployed. IEC 61850 remains the appropriate choice for substation automation where deterministic behavior and formal modeling enable sophisticated protection coordination. MQTT offers compelling advantages for the growing population of distributed sensors where lightweight protocols and flexible messaging patterns provide better fit than industrial automation standards [18].

The cybersecurity findings warrant particular attention given the increasing sophistication of threats targeting critical infrastructure globally. While the current defense architecture successfully prevented all attempted compromises during the monitoring period, the 847 detected intrusion attempts indicate sustained adversary interest requiring continued vigilance. The shift toward zero-trust security models assuming potential compromise of individual components represents prudent evolution of defensive posture.

## Conclusion

This research established comprehensive performance benchmarks for communication infrastructure supporting Singapore's smart grid deployment. Field measurements at 142 monitoring points over nine months characterized protocol performance, network reliability, and security posture under actual operating conditions representative of high-density urban environments.

Protocol evaluation demonstrated distinct performance profiles suited to different application requirements. IEC 61850 achieved optimal results for substation automation with 12.4 ms latency and 98.7% reliability, while MQTT provided superior performance for distributed sensor networks with 8.6 ms latency and 92.1% throughput scores. The multi-protocol architecture enables optimal matching of communication characteristics to application requirements.

Network infrastructure achieved 99.2% availability for wireless mesh coverage across 847 square kilometers with automatic failover to cellular backup within 340 ms of primary link failure. Fiber backbone reliability exceeded 99.97% supporting critical substation interconnection. These performance levels substantially exceed typical utility communication targets and enable sophisticated real-time grid management applications.

Data traffic analysis documented exponential growth from 28 terabytes monthly in 2019 to 239 terabytes by late 2023, with analytics applications contributing disproportionately to bandwidth expansion. This trajectory demands continued infrastructure investment to maintain headroom for emerging data-intensive optimization applications leveraging machine learning and artificial intelligence approaches.

Cybersecurity assessment identified 847 attempted intrusions during the monitoring period, with defense-in-depth architecture successfully preventing all unauthorized access to critical control systems. Continued evolution of defensive capabilities including behavioral analytics and threat intelligence sharing remains essential to address increasingly sophisticated adversary techniques targeting critical infrastructure systems globally.

## Acknowledgements

### Funding Sources

This research was supported by the Energy Market Authority of Singapore through their research and development program and by the National Research Foundation Singapore under the Campus for Research Excellence and Technological Enterprise initiative. Nanyang Technological University provided supplementary funding through the School of Electrical and Electronic Engineering.

### Institutional Support

The authors acknowledge SP Group for providing network access and operational data essential to this research. Technical collaboration with the Cyber Security Agency of Singapore enabled security assessment components of the investigation.

### Contributions Not Qualifying for Authorship

The authors thank Dr. Ng Boon Kiat for consultation on communication protocol standards, Mr. Raj Kumar for field instrumentation support, and the SP Group network operations team who facilitated measurement access while maintaining operational security.

## References

1. Energy Market Authority. Singapore electricity market outlook 2023. Singapore: EMA; 2023.
2. Gungor VC, Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, Hancke GP. Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics. 2011;7(4):529-539.
3. Department of Statistics Singapore. Population and population structure 2023. Singapore: DOS; 2023.
4. Mackiewicz R. Overview of IEC 61850 and benefits. IEEE Power Systems Conference and Exposition. 2006:623-630.
5. Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid. Proceedings of the IEEE. 2012;100(1):210-224.
6. Higgins N, Vyatkin V, Nair NKC, Schwarz K. Distributed power system automation with IEC 61850, IEC 61499, and intelligent control. IEEE Transactions on Systems, Man, and Cybernetics. 2011;41(1):81-92.
7. Saputro N, Akkaya K. Performance evaluation of smart grid data aggregation via homomorphic encryption. IEEE Wireless Communications and Networking Conference. 2012:2945-2950.
8. Ten CW, Liu CC, Manimaran G. Vulnerability

assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems. 2008;23(4):1836-1846.
9. Yan Y, Qian Y, Sharif H, Tipper D. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE Communications Surveys & Tutorials. 2013;15(1):5-20.
10. Lim KS, Tan ZJ, Yeo WM. Smart grid implementation challenges in Singapore. IEEE Region 10 Conference. 2018:1842-1847.
11. SP Group. Technical standards for grid connection of energy storage systems. Singapore: SP Group; 2022.
12. Spirent Communications. TestCenter platform user guide. Version 5.0. Calabasas: Spirent; 2022.
13. Wang W, Lu Z. Cyber security in the smart grid: Survey and challenges. Computer Networks. 2013;57(5):1344-1371.
14. Infocomm Media Development Authority. Radio-frequency guidelines for smart grid applications. Singapore: IMDA; 2021.
15. Cyber Security Agency of Singapore. Critical information infrastructure protection guidelines. Singapore: CSA; 2023.
16. Hunkeler U, Truong HL, Stanford-Clark A. MQTT-S: A publish/subscribe protocol for wireless sensor networks. IEEE Conference on Communication Systems Software and Middleware. 2008:791-798.
17. National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. Version 1.1. Gaithersburg: NIST; 2018.
18. Fang X, Misra S, Xue G, Yang D. Smart grid—the new and improved power grid: A survey. IEEE Communications Surveys & Tutorials. 2012;14(4):944-980.