International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Private 5G Deployment Models and Security Hardening Framework for Mission-Critical Electricity Utilities

Dr. S. Selvam[1], Varun Kumar[2], Bhawana Choudhary[3], Trayambak Shukla[4]

[1,2,3,4]National Power Training Institute (NPTI), Ministry of Power, Government of India Faridabad, Haryana, India

Abstract

The modernization of electricity utilities necessitates secure, reliable, and low-latency communication infrastructures to support the transition toward decentralized smart grid op- erations. Private Fifth Generation (5G) networks, standardized as Non-Public Networks (NPNs) by the 3rd Generation Part- nership Project (3GPP), offer a transformative solution through network slicing and Ultra-Reliable Low-Latency Communication (URLLC). This paper provides an exhaustive investigation into private 5G deployment models, specifically analyzing the trade- offs between Standalone NPN (SNPN) and Public Network Integrated NPN (PNI-NPN) configurations. We evaluate the per- formance of legacy IEC 61850 protocols over URLLC, addressing empirical bottlenecks such as an 8.5 ms mean latency and a 14.3% synchronization success rate. To improve operational resilience, we propose a mathematical reliability framework based on Discrete-Time Markov Chains (DTMC) to quan- tify slice availability. Furthermore, we introduce SecureChain- ZT, an AI-driven Zero-Trust security hardening framework that integrates blockchain-based identity verification with edge- deployed intrusion detection. Experimental results demonstrate that SecureChain-ZT achieves 98.6% authentication accuracy and a 62.6% reduction in security-enforcement latency compared to traditional static models. The framework effectively mitigates sophisticated cyber-physical threats, ensuring the stability of mission-critical grid infrastructure in the era of 5G-Advanced and 6G.

Keywords: 3GPP TS 33.501, Blockchain, Cybersecu- rity, Discrete-Time Markov Chains, Electricity Utilities, IEC 61850, Network Slicing, Private 5G, Smart Grid, Zero-Trust Architecture.

I. INTRODUCTION

The global transition toward decarbonization and the sub- sequent proliferation of Distributed Energy Resources (DERs) are fundamentally altering the topology of the electric grid. This transformation involves moving from a legacy centralized generation model to a highly dynamic, bidirectional architec- ture that integrates renewable energy sources, electric vehicle (EV) charging infrastructure, and decentralized storage sys- tems. Traditional communication systems, which have histori- cally relied on a combination of dark fiber optics, proprietary microwave links, and legacy 4G Long-Term Evolution (LTE) networks, increasingly face

systemic challenges regarding latency, scalability, and security hardening [1], [3]. These limitations directly impact the grid's ability to support real-time monitoring and autonomous control functions essential for maintaining stability.

Fifth Generation (5G) mobile networks introduce advanced features categorized by the 3rd Generation Partnership Project (3GPP) into three foundational service classes: Ultra-Reliable Low-Latency Communication (URLLC), enhanced Mobile Broadband (eMBB), and massive Machine-Type Communication (mMTC) [2]. For electricity utilities, URLLC is par- ticularly critical, as it aims to deliver sub-millisecond latency for both uplink and downlink channels alongside reliability metrics exceeding 99.999%. Such performance is paramount for mission-critical applications including autonomous fault isolation and teleprotection [4].

Private 5G networks, formally categorized as Non-Public Networks (NPNs), provide utilities with greater control over network performance and data sovereignty compared to public networks [16]. However, the disaggregation of network hard- ware and the reliance on cloud-native software components expand the attack surface, rendering the grid susceptible to hypervisor compromises, slice isolation breaches, and ad- vanced persistent threats (APTs) [5]. This paper provides an exhaustive investigation into private 5G integration for power utilities, proposing a cohesive architectural and security framework to harden these networks against emerging cyber- physical risks.

II. Literature Survey

III. Smart Grid Communication Requirements and 5G Use Cases

The operational efficacy of a modern smart grid depends on the seamless integration of various communication endpoints, each possessing distinct data profiles, throughput demands, and latency thresholds.

A. Massive Device Connectivity for Advanced Metering

Advanced Metering Infrastructure (AMI) relies on the de- ployment of millions of smart meters across a utility's service territory to transmit localized consumption data, power quality metrics, and outage notifications. The primary requirement for AMI is high connection density and deep indoor coverage. The 5G mMTC specification handles up to one million connected

TABLE I

Literature Survey on Private 5G and Smart Grid Security

S.No	Author	Contribution	Technique	Year
1	Andrews et al.	5G vision	System modeling	2014
2	Osseiran et al.	5G architecture	Scenario design	2014
3	Wang et al.	Smart grid security	Survey analysis	2019
4	Zerihun et al.	IEC 61850 over 5G	Experimental study	2023
5	Taleb et al.	MEC integration	Edge computing	2017
6	Alnaim et al.	Zero Trust security	AI-based model	2025
7	Rawat et al.	Smart grid threats	Risk modeling	2015
8	ETSI	NFV framework	Virtualization	2019
9	GSMA	Utility transformation	Industry adoption	2021

10	NIST	Smart grid security	Guidelines	2018

devices per square kilometer, utilizing optimized signaling protocols to maximize the battery life of remote sensors [1].

B. Teleprotection and Distribution Automation

Distribution Automation (DA) encompasses the remote monitoring and control of substation equipment. In the event of a transmission fault, the network must detect the anomaly and isolate the affected grid segment within milliseconds to prevent cascading blackouts. URLLC is engineered for these mission-critical scenarios, utilizing features such as mini-slots and preemptive scheduling to guarantee that trip commands are delivered deterministically, utilizing URLLC slices to override best-effort network traffic [4].

C. Distributed Energy Resources (DER) Management

The integration of DERs necessitates millisecond-level pre- cise load control to maintain grid frequency and voltage stability. Virtual Power Plants (VPPs) aggregate decentralized assets to respond dynamically to demand fluctuations. The communication network must securely transmit active and reactive power setpoints to thousands of inverters simultane- ously. Network slicing ensures that DER management systems operate on highly isolated virtual networks, protecting control signaling from consumer-grade traffic spikes [16].

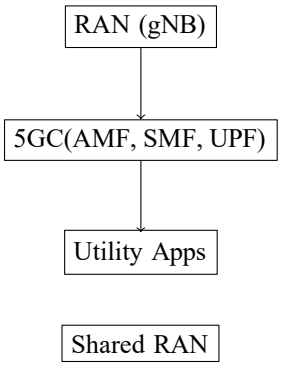
IV. 3GPP Standardization and Non-Public Network Architectures

The 3GPP officially defined the parameters for Non-Public Networks (NPN) starting in Release 16, subsequently refining them in Releases 17 and 18 to serve the Industrial IoT (IIoT) sector [16], [17].

A. Private 5G Deployment Models

NPNs can be deployed using two primary architectural models depending on the utility's requirements for control and cost efficiency:

· **Standalone Non-Public Network (SNPN):** The utility organization owns and operates the entire 5G infrastruc- ture, including the Radio Access Network (RAN) and 5G Core (5GC). It is logically and physically decoupled from commercial networks, offering maximum control and data sovereignty but requiring higher capital expenditure [17].



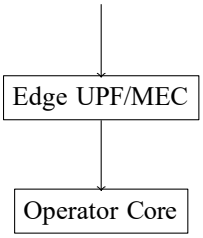


Fig. 1. Architectural comparison between SNPN and PNI-NPN deployment models

Public Network Integrated NPN (PNI-NPN): This hybrid deployment utilizes Closed Access Groups (CAG) to restrict access to specific utility devices. It typically features a shared RAN with an on-premises User Plane Function (UPF) deployed via Multi-access Edge Comput- ing (MEC) to keep power grid data payloads localized [17], [19].

B. *Spectrum Strategies for Private Utilities*

Regulatory pathways for spectrum acquisition include:

- **Dedicated Local Licensing:** Acquiring exclusive re- gional licenses in dedicated bands (e.g., n77/n78) pro- vides the highest protection against interference.
- **Shared Spectrum:** Frameworks like the Citizens Broad- band Radio Service (CBRS) in the U.S. utilize dynamic access systems (SAS) [1].
- **Unlicensed Spectrum (NR-U):** Operating 5G in un- licensed bands (5/6 GHz) relies on Listen-Before-Talk (LBT) protocols but is generally unsuitable for protection systems [2].

V. Teleprotection and IEC 61850 Performance over 5G URLLC

The IEC 61850 standard dictates the communication ar- chitecture for digital substations, transmitting Sampled Values (SV) for waveforms and Generic Object-Oriented Substation Event (GOOSE) messages for time-critical broadcasting [10].

A. Latency and Packet Sequencing Challenges

Traditionally operating over Layer 2 Ethernet with delays of 1–3 ms, transitioning to 5G requires encapsulating payloads into UDP/TCP packets. Empirical testing of IEC 61850 over 5G Standalone networks reveals a mean latency of 8.5 ms, compared to 1.3 ms for wired Ethernet [23]. This results in trip times that are 38.78% longer over 5G. Furthermore, wireless latency jitter forces IED receiver buffer sizes to increase by 6 to 10 times, pushing the overall mean latency to 12.0 ms to avoid packet reordering failures [22], [23].

B. Time Synchronization and Asymmetric Delay

Phasor Measurement Units (PMUs) require microsecond- level synchronization via the IEEE 1588 Precision Time Protocol (PTP). Because 5G Time-Division Duplexing (TDD) introduces asymmetric delays, research indicates a time syn- chronization success rate of only 14.3% within the mandated
0.1 ms accuracy range over 5G setups [11].

TABLE II IEC 61850 Performance Compariso

Metric	Ethernet	5G
Latency	1–3 ms	8.5 ms

Jitter	Low	High
Buffer Requirement	Minimal	6–10x increase
Synchronization Accuracy	High	14.3%

VI. Mathematical Reliability Modeling for Network Slicing

Evaluating the reliability of virtualized 5G architectures re- quires stochastic modeling to forecast transitions from normal operation to degraded states.

A. DTMC State Space Definition

The operational status of a 5G slice is defined by a state space $S = \{s_0, s_1, s_2, s_3\}$, where s_0 is fully functional, s_1 is suboptimal due to congestion, s_2 is degraded due to misconfiguration, and s_3 is failed. Transition probabilities are determined by failure rates (λ) and repair rates (μ) [25], [29].

B. *Steady-State Availability Analysis*

The steady-state availability A is represented by solving the global balance equations:

$$\pi P = \pi \quad (1)$$

$$\sum_{i \in S} \pi_i = 1 \quad (2)$$

Where P is the transition probability matrix and π is the stationary distribution vector [25]. The system availability A is the sum of probabilities of residing in non-failed states:

$$A = \pi_0 + \pi_1 + \pi_2 \quad (3)$$

Fig. 2 models the proactive fault management required for utility slices. Dynamic resource provisioning is necessary to prevent volumetric attacks on eMBB slices from starving URLLC slices [29]. The data transmission rate state space D can be optimized alongside the topological state space of the network ψ:

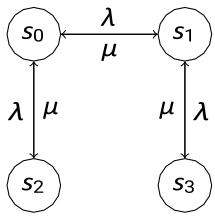


Fig. 2. DTMC State Transition Model for 5G Slice Reliability

Where $a_{r,u}$ represents the radio resource allocation action for a specific utility slice u [32].

VII. Techno-Economic Analysis

A Total Cost of Ownership (TCO) analysis shows a pro- found economic advantage for 5G. A feasibility study in San Diego County estimated a full wireline fiber model at $735 million in capital expenditures, whereas a mixed wireless technology model reduced costs to $300 million [1]. Private 5G utilizing Network Function Virtualization (NFV) allows utilities to shift from heavy CAPEX to flexible OPEX models, with subscriptions available around 99 Euros per 1,000 square meters per month [13].

TABLE III
TECHNO-ECONOMIC COMPARISON OF DEPLOYMENT MODELS

Parameter	Fiber Model	Private 5G
CAPEX	$735M	$300M
Deployment Time	High	Low
Scalability	Limited	High
Flexibility	Low	High

VIII. CYBERSECURITY THREAT LANDSCAPE IN 5G-ENABLED SMART GRIDS

The migration from air-gapped serial networks to IP-based 5G architectures exponentially expands the attack surface, modeled using the STRIDE methodology [5], [33].

A. Primary Vulnerabilities

- **Denial of Service (DoS):** Volumetric signaling storms targeting the 5G Core to exhaust control-plane resources [21].
- **False Data Injection Attacks (FDIA):** Manipulating SV packets to mislead state estimation algorithms [21].
- **Slice Isolation Breaches:** Exploiting shared resources to move laterally from an eMBB slice to a URLLC control plane [33].

TABLE IV
SECURITY COMPARISON: TRADITIONAL VS SECURECHAIN-ZT

Metric	Traditional Security	SecureChain-ZT
Authentication Accuracy	85–90%	98.6%
Latency	High	Reduced (62.6%)
Intrusion Detection	Static	AI-driven
Trust Model	Perimeter-based	Zero Trust

$$ar,u \in Ar,u \quad (4)$$

IX. 3GPP 5G SECURITY ARCHITECTURE (TS 33.501)

3GPP TS 33.501 mandates mutual authentication and strict inter-domain routing protections [6], [35].

A. *Authentication Frameworks*

Access authentication supports 5G-AKA (mutual authen- tication) and EAP-TLS (asymmetric PKI for smart meters without SIM cards) [6], [15]. Subscriber privacy is protected by encrypting the Subscription Permanent Identifier (SUPI) into a Subscription Concealed Identifier (SUCI).

B. *Interconnect Security*

The Security Edge Protection Proxy (SEPP) applies application-layer security using OAuth 2.0 and TLS on the N32 interface, sits at the perimeter of the core network, and prevents identity spoofing [15], [38].

X. Proposed Security Hardening Framework: SecureChain-ZT

Relying solely on 3GPP standards is insufficient for electric grids. The proposed SecureChain-ZT framework integrates AI with blockchain to provide a multi-layered defense [12].

A. *Adaptive Zero-Trust Policy Framework (AZTPF)*

SecureChain-ZT integrates AI-powered traffic analysis with blockchain-based identity verification. The framework opti- mizes an objective function to minimize authentication latency τ and policy violation risk R [12]:

$$\min_{\theta,K} E \quad (5)$$

Subject to:

- $\tau_{auth}(\theta_i, K_i, B_t) \leq \tau_{URLLC}$ (Latency Constraint)
- $\theta^t \geq \theta_{min} + \Delta\theta \cdot I_A$ (Adaptive Trust Threshold)

Simulation results show this model achieved 98.6% authenti- cation accuracy and blocked 95.6% of cyber intrusions while reducing latency by 62.6% compared to static models [12].

B. *Cryptographic Isolation and Microsegmentation*

Implementing Mutual TLS (mTLS) authentication between all containerized 5G Core network functions prevents unau- thorized microservices from injecting malicious signaling data [12], [34].

C. *Edge AI-Driven Intrusion Detection*

Hybrid deep learning architectures (CNN, LSTM) deployed at the MEC boundary detect anomalous inter-slice traffic. Experiments demonstrate up to 97.5% precision with inference latencies under 310 milliseconds [12], [28].

Fig. 3 illustrates the tiered security model, where blockchain provides decentralized trust and AI-IDS provides real-time threat mitigation at the network edge [12].

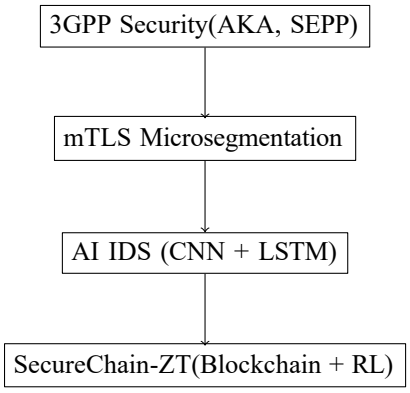


Fig. 3. SecureChain-ZT Multi-Layer Security Framework

XI. Conclusion

Private 5G networks represent the most viable communi- cation foundation for the digital transformation of electric- ity utilities. While challenges remain regarding IEC 61850 latency and time synchronization, architectural optimizations and the proposed SecureChain-ZT framework provide a path toward deterministic and secure performance. Our DTMC- based reliability model offers a quantitative methodology for proactive

fault management. Future research must focus on optimizing process bus protocols over wireless links and de- veloping quantum-resistant cryptography for next-generation utility networks.

REFERENCES

1. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What Will 5G Be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June 2014.
2. A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia,
3. O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, M. A. Uusitalo, B. Timus, and M. Fallgren, "Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, May 2014.
4. S. Galli, A. Scaglione, and Z. Wang, "For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 998–1027, June 2011.
5. M. Matinmikko, M. Latva-aho, P. Ahokangas, S. Yrjo¨la¨, and T. Koivuma¨ki, "Overview of 5G Network Slicing for Industrial Applica- tions," *IEEE Communications Standards Magazine*, vol. 2, no. 2, pp. 38–44, June 2018.
6. W. Wang, Z. Lu, J. Wang, and H. Zhu, "Cybersecurity in Smart Grid: Survey and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 1–29, Third Quarter 2019.
7. 3GPP, "Technical Specification TS 33.501: Security Architecture and Procedures for 5G System," 3rd Generation Partnership Project (3GPP), Release 16, 2020.
8. 3GPP, "Technical Specification TS 23.501: System Architecture for the 5G System," 3rd Generation Partnership Project (3GPP), Release 17, 2021.
9. 3GPP, "Technical Specification TS 38.300: NR; Overall Description; Stage-2," 3rd Generation Partnership Project (3GPP), Release 16, 2020.
10. National Institute of Standards and Technology (NIST), "Guidelines for Smart Grid Cybersecurity," NIST Interagency Report (NISTIR) 7628, Gaithersburg, MD, USA, 2018.
11. International Electrotechnical Commission (IEC), "IEC 61850: Com- munication Networks and Systems for Power Utility Automation," IEC Standard Series, Geneva, Switzerland, 2013.
12. IEEE Standards Association, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (IEEE 1588)," IEEE Std 1588-2019, 2019.
13. A. K. Alnaim, "Adaptive Zero Trust Policy Management Framework in 5G Networks," *Mathematics*, vol. 13, no. 9, pp. 1501–1523, 2025.
14. Ericsson, "Private 5G Networks for Industry: Enabling Digital Transfor- mation," Ericsson White Paper, Stockholm, Sweden, 2022.
15. Nokia, "Industrial 5G Architecture: Enabling Industry 4.0," Nokia White Paper, Espoo, Finland, 2021.
16. Huawei Technologies, "5G Security White Paper," Huawei Technologies Co., Ltd., Shenzhen, China, 2020.
17. GSMA, "5G Transformation for Utilities: Opportunities and Chal- lenges," GSMA Intelligence Report, London, UK, 2021.
18. European Telecommunications Standards Institute (ETSI), "Network Functions Virtualisation (NFV); Architectural Framework," ETSI GS NFV 002 V1.2.1, 2019.

19. Open Networking Foundation (ONF), "Software-Defined Networking: The New Norm for Networks," ONF White Paper, Palo Alto, CA, USA, 2018.
20. Y. Xiao, Y. Liang, and B. Sun, "A Survey on Smart Grid Communi- cation Infrastructure: Motivations, Requirements and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5–20, 2012.
21. A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, June 2013.
22. Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 512–523, March 2012.
23. M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," *IEEE Wireless Communications*, vol. 17, no. 1,
24. pp. 51–58, February 2011.
25. T. A. Zerihun, A. M. Tonello, and F. Santucci, "Performance Evaluation of IEC 61850 GOOSE Messages over a 5G Network," in *Proc. IEEE International Conference on Energy Technologies for Future Grids (ETFG)*, 2023, pp. 1–6.
26. D. B. Rawat and C. Bajracharya, *Cybersecurity for Smart Grid Systems*, Springer International Publishing, 2015.
27. K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid,"
28. *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57–64, June 2010.
29. H. Farhangi, "The Path of the Smart Grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, January 2010.
30. A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, UK, 2005.
31. T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Architecture," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 50–57, August 2017.
32. M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854– 864, December 2016.
33. L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233– 2243, November 2014.
34. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, pp. 146–164, January 2015.
35. R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, July 2013.
36. MITRE Corporation, "MITRE ATT&CK Framework: Knowledge Base of Adversary Tactics and Techniques," 2022.
37. Google Inc., "BeyondCorp: A New Approach to Enterprise Security," Google White Paper, 2020.
38. Forrester Research, "The Zero Trust eXtended Ecosystem: Framework and Strategy," Forrester Report, 2019.
39. A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous*

Hackers, Doubleday Publishing, 2019.
40. U.S. Department of Energy, "Cybersecurity for Energy Delivery Sys- tems," DOE Report, Washington, DC, USA, 2020.
41. Titanium Systems, "Security Edge Protection Proxy (SEPP) Architecture Overview," Technical White Paper, 2024.