A Room-Temperature Quantum-Secured ROCOF for Enhancing Grid Reliability

Ruoyan Fan, Zimin Jiang, Yacov A. Shamash and Peng Zhang

***Abstract*—The increasing penetration of inverter-based resources (IBRs) reduces system inertia and makes modern power grids more vulnerable to rapid frequency deviations. Under these conditions, the rate of change of frequency (ROCOF) becomes an important protection indicator. However, current ROCOF protection relies on IEC 61850 GOOSE communication, which contains security vulnerabilities in its communication channel. To address this challenge, we propose a room-temperature, quantum-secured ROCOF framework that combines quantum key distribution (QKD) with hash-based message authentication codes (HMACs), enabling dynamic authentication of ROCOF-based trip signals and ensuring their integrity against adversarial manipulation. The framework is validated on a hardware-in-the-loop platform with an IBR-enriched NPCC system. The experiment results confirm that the GOOSE communication channel remains secure against message manipulation, and that the quantum channel can detect eavesdropping aimed at capturing the quantum key for forging HMAC. The results demonstrate the practical viability of room-temperature QKD for grid protection, strengthening cybersecurity and operational resilience in low-inertia power systems.**

***Index Terms*—Cybersecurity, power system protection, quantum Key distribution, rate of change of frequency**

I. Introduction

The modern power grid is seeing a growing share of inverter-based resources (IBRs), reducing system inertia and increasing vulnerability to rapid frequency deviations. The April 2025 blackout in Spain, Portugal, and France further illustrates how low inertia magnifies frequency disturbances, making fast metrics such as the Rate of Change of Frequency (ROCOF) essential [1], [2].

Modern ROCOF protection must operate within a few milliseconds to support actions such as load shedding or controlled islanding, and in practice relies on IEC 61850 GOOSE messages exchanged within 3–5 ms to achieve this performance [3]. However, the plain-text format of GOOSE leaves the protection channel vulnerable to spoofing or manipulation attacks. Although digital signatures have been proposed to secure these messages, their added processing delay conflicts with the strict latency requirements of ROCOF protection [4]. As a result, today's low-inertia grids face a widening gap between the need for secure ROCOF signaling and the limited time available for conventional encryption.

This work relates to the Department of Navy award N000142512374 issued by the Office of Naval Research. The United States Government has a royalty-free license throughout the world in all copyrightable material contained herein. *Corresponding Author: Peng Zhang.*

The authors are with the Department of Electrical and Computer Engineering, Stony Brook University, NY 11794-2350 USA (e-mails: ruoyan.fan, zimin.jiang, yacov.shamash, p.zhang@stonybrook.edu).

Quantum key distribution (QKD) provides fresh symmetric keys with provable randomness, guaranteed secrecy, and built-in eavesdropping detection—ensuring physically secured keys for protection applications [5]–[13]. In this paper, we design and implement the first room-temperature, quantum-secured ROCOF (QS-ROCOF) scheme, which hardens the vulnerable GOOSE communication channel against both classical and quantum cyberattacks. By using QKD-generated keys for lightweight message authentication, the framework enables sub-millisecond validation of GOOSE messages without noticeable cryptographic delay, resolving the long-standing trade-off between security and real-time performance. The novelties of our work include:

- A lightweight, QKD-secured communication framework that uses physically secured keys and maintains the sub-cycle latency required for ROCOF protection.
- A room-temperature, commercial-off-the-shelf hardware-in-the-loop platform that integrates QKD with utility-grade protection relays.
- A comprehensive validation of resilience against GOOSE manipulation and quantum-channel eavesdropping attacks, demonstrating secure, real-time operation under realistic conditions.

II. Methodology

Our QS-ROCOF framework combines the physical-level security of QKD with lightweight Hash-Based Message Authentication Code (HMAC), as shown in Fig. 1, using quantum-secured keys for real-time verification of ROCOF trip signals.

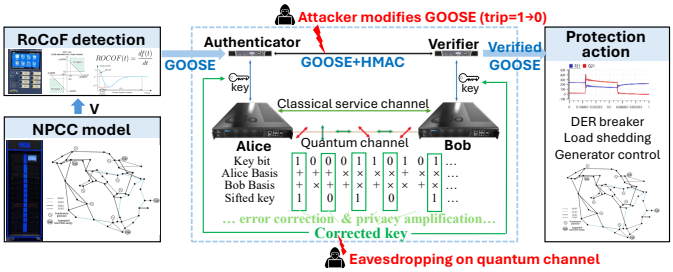

Fig. 1: Quantum-secured ROCOF protection architecture.

A. ROCOF Protection in IBR-Rich Systems

ROCOF is mathematically defined as the time derivative of system frequency as $ROCOF = \frac{df}{dt}$, where f is the system frequency in Hz, estimated from waveforms using digital signal processing techniques, with filtering or sliding windows applied to reduce noise. It is used for islanding

detection and under-frequency load shedding (UFLS), providing predictive, selective load shedding to maintain generation-load balance. Compared to traditional under-frequency relays, ROCOF schemes act faster, enhancing resilience in low-inertia systems [14].

B. QKD for Communication Protection

QKD provides physically secured keys by leveraging the observer effect and the no-cloning theorem in quantum physics, ensuring that any attempt to extract quantum information is inherently detectable and enabling information-theoretic security beyond classical, computation-based key generation.

Building on the two fundamental principles, the standard BB84 protocol distributes keys by encoding information onto single-photon polarization states and detecting any disturbance introduced during transmission [15], [16]. The QKD devices Alice and Bob retain only the outcomes measured in matching bases, and any eavesdropping leads to an increased Quantum Bit Error Rate (QBER). Keys with excessive errors are discarded, while the remaining bits undergo classical post-processing to form a secure symmetric key. This enables QKD to deliver physics-secured keys for critical grid communications, resilient even against quantum-capable adversaries.

The use of room-temperature QKD modules enables practical substation deployment by eliminating cryogenic cooling infrastructure, significantly reducing cost, power consumption, and maintenance complexity, thus making quantum-secured key distribution feasible for real-world protection and control applications—even under advanced cyberattacks.

C. QKD Keys for HMAC Authentication

In the QS-ROCOF architecture, QKD continuously refreshes symmetric keys using entropy from quantum states, ensuring that old keys cannot be reused by adversaries. These quantum-secured keys are applied to a lightweight HMAC scheme that protects ROCOF-related GOOSE messages with fast integrity and authentication guarantees, without the delay associated with asymmetric signatures. With frequently refreshed QKD keys driving a lightweight HMAC process, only authenticated and untampered GOOSE messages can trigger ROCOF protection actions, even under sophisticated cyberattacks.

III. Room-Temperature QS-ROCOF Testbed

We first introduce the IBR-enriched NPCC system built in RTDS to validate the QS-ROCOF scheme, and then present the design of the room-temperature testbed.

A. IBR-Enriched NPCC Power System

To validate the developed QKD-based ROCOF protection method, a modified NPCC system is adopted, which is a reduced model of the power grid in the northeastern United States and Canada. The single-line diagram of the system is shown in Fig. 2. Each synchronous generator is modeled along with its speed governor, exciter and the associated automatic voltage regulator. Note that the ROCOF-based protection

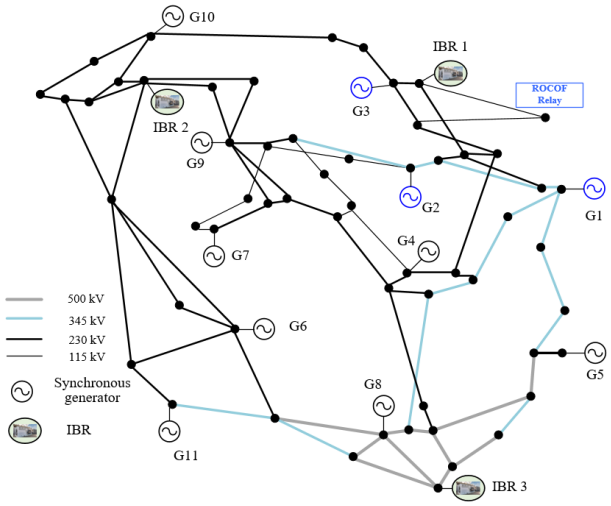

Fig. 2: Single-line diagram of the IBR-enriched NPCC system

in this paper is meant to maintain balance between power generation and loads during severe events, so the secondary frequency regulation to restore the system frequency is not implemented in the model.

To account for the effects of increasing IBR penetration, three aggregated inverter units with a total rated capacity of 1.5 GW (3 × 500 MW) are connected to the NPCC system, as shown in Fig. 2. Each unit adopts the grid-following control method.

The ROCOF protection is implemented at a feeder with a rated voltage of 115kV, as the blue box shown in Fig. 2. To validate the ROCOF protection, different contingences, i.e., synchronous generators outage, can be simulated with the modified NPCC system.

B. The Room-Temperature QS-ROCOF Testbed

The first-ever room-temperature QS-ROCOF testbed is presented in Fig. 3. It consists of RTDS hardware, a relay with ROCOF function and a QKD system. Specifically, the NPCC system is implemented in the RTDS environment. Voltage/current waveforms simulated in real-time are fed into the relay via the GTAO card of RTDS. The relay calculates the ROCOF of the specified feeder. If the calculated ROCOF value exceeds a certain threshold, a GOOSE trip message will be sent to the corresponding breakers modeled in the NPCC system via a communication channel secured by QKD.

The QKD system consists of two endpoints (Alice and Bob) connected by a quantum channel and a classical service channel. Alice prepares quantum states encoded as single photons and transmits them to Bob through the quantum channel, while the classical service channel is used for basis reconciliation and error estimation. The system operates under the BB84 protocol, where Alice randomly encodes bits in non-orthogonal bases and Bob randomly measures them in compatible or incompatible bases. Then they discard mismatched outcomes, and the remaining results are used to form a shared secret key. Any attempt to eavesdrop will inherently disturb the quantum states, thus increasing the QBER, which Alice and Bob can detect through the classical channel. Once sifted

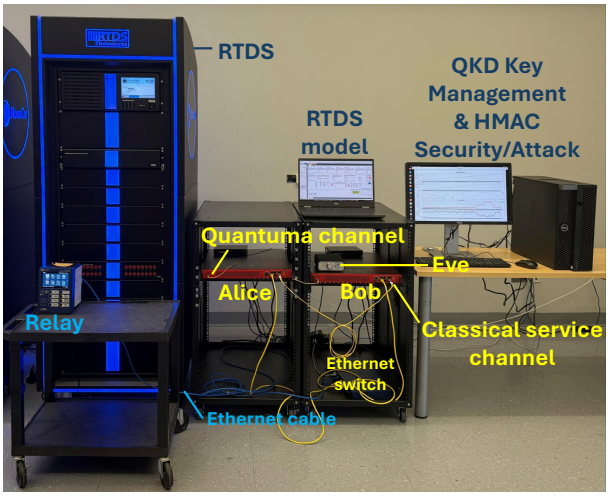

Fig. 3: Room-temperature testbed for QS-ROCOF

bits are reconciled and privacy-amplified, Alice and Bob will share an identical corrected key. Alice provides this key to the Authenticator, while Bob supplies the same key to the Verifier.

When a GOOSE trip message is generated, the Authenticator computes an HMAC using the corrected key from Alice. The authenticated GOOSE packet (message + HMAC) is sent via an Ethernet channel to the corresponding breakers. Upon receipt, the Verifier uses its copy of the corrected key to compute the expected HMAC and verify authenticity and integrity. Only if the HMAC matches is the GOOSE trip forwarded to trigger breakers, and any tampering or mismatch results in immediate rejection.

To evaluate the effectiveness of the QKD-enhanced protection, two representative cyber-attack scenarios are designed, targeting both the quantum channel and the classical communication network.

The first experiment is designed to demonstrate the security of the keys used for HMAC authentication by validating that any attempt to eavesdrop on the quantum channel can be reliably detected. Under normal conditions, the QBER remains within a low range. When an adversarial eavesdropper (Eve) is introduced, disturbances on the photon states lead to an obvious increase in QBER. By setting a safe QBER limit, the eavesdropper can be detected once QBER exceeds this limit. In our experiment, we also demonstrate that even with the presence of Eve, there are still enough quantum keys in the key pool to support safe communication under such attack scenarios.

The second experiment is a man-in-the-middle (MITM) attack on the IEC 61850 GOOSE communication channel, which transfers ROCOF-triggered trip signals between the protection relay and the breakers simulated in the RTDS environment. In this scenario, the attacker intercepts the GOOSE traffic and modifies the trip signal from "1" to "0", thereby suppressing legitimate tripping actions such as load shedding. If successful, this attack would delay or prevent protective responses during a disturbance, potentially leading to cascading failures and, ultimately, large-scale system collapse. To mitigate this threat, corrected quantum keys generated by the QKD system are used to compute HMACs for each GOOSE message. At the receiving end, the integrity of every message is verified prior to execution. Any tampered message fails the HMAC verification and is discarded, ensuring that only authentic trip commands issued by the relay are executed.

The MITM adversary was physically implemented using a Linux machine configured with dual Ethernet interfaces in bridge mode, enabling interception, modification, and retransmission of GOOSE messages without altering the network topology, which emulates realistic substation attack, and thereby providing a credible validation environment for QKD-protected authentication [14]–[17].

IV. Results and Discussion

This section provides the experimental results and discussion. We first demonstrate the QKD system performance for providing keys for HMAC process and detecting eavesdropping attacks on the quantum channel. Then, we present the performance of QKD-HMAC for identifying MITM attacks. Finally, we validate the QS-ROCOF method with the NPCC test system.

A. QKD Performance and Eavesdropper Detection

Fig.4 illustrates the key generation process of the QKD channel and the impact of an eavesdropper on the quantum channel, corresponding to the first attack experiment.

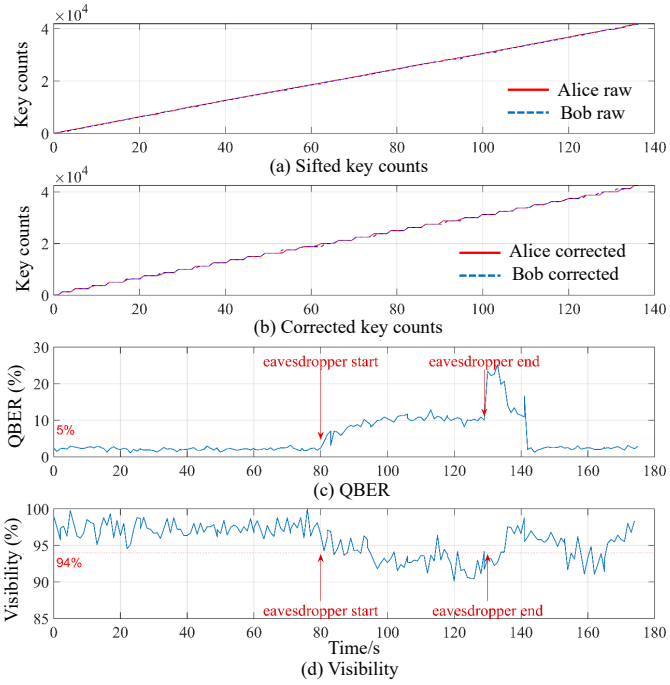

Fig. 4: QKD performance under normal and eavesdropping conditions

As shown in Fig.4 (a) and (b), both sifted and corrected key counts increase linearly throughout the experiment, confirming a stable and continuous key generation process. When an eavesdropper is introduced at 80s, the QBER rises sharply above the 5% threshold, while the visibility simultaneously drops below the 94% threshold, indicating a degradation of quantum coherence caused by the intrusion, as shown in

Fig. 4 (c) and (d). After the eavesdropper is removed at 130s, the QBER exhibits a short transient increase before decreasing back to its nominal value. This overshoot is due to the sliding error-estimation window, which still includes some of the attacked bits immediately after the intrusion ends. These results demonstrate that attacks on the quantum channel can be clearly detected through the QBER and visibility metrics.

B. HMAC Validation

Fig. 5 presents the validation of message integrity on a classical communication channel using HMAC values generated from QKD-derived keys. On the sender side, Alice transmits a sinusoidal signal, while on the receiver side, Bob verifies the signal with an HMAC computed using the shared quantum key. The $AttackFlag = 1$ in Fig. 5 (b) denotes intervals where a man-in-the-middle adversary is emulated to deliberately alter the transmitted data.

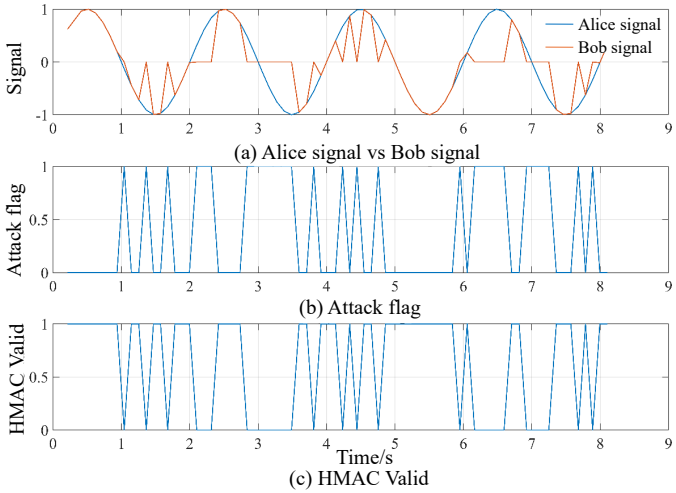

Fig. 5: Signal integrity verification results using HMAC

During these attack periods, Bob's received waveform deviates from Alice's original signal, as shown in Fig. 5 (a). The integrity of each message is validated through the HMAC. As illustrated in Fig. 5 (c), the HMACValid indicator drops from 1 to 0 exactly when the AttackFlag is active, demonstrating that the tampered messages fail authentication.

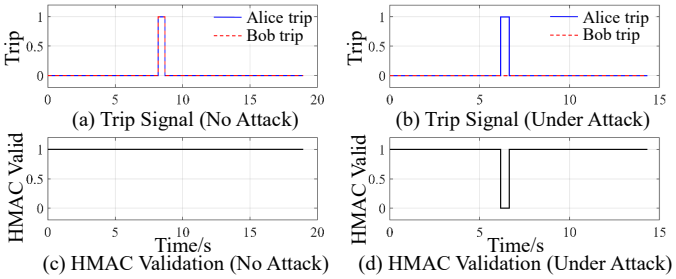

Fig. 6: ROCOF-based trip signal transmission and HMAC validation results

Fig. 6 demonstrates the protection of GOOSE-based trip commands under both normal and MITM conditions. Under normal conditions, the trip signals observed at the sender and receiver sides are identical, and the HMAC validation remains at 1 throughout the event, as shown in Fig. 6 (a) and (c), confirming that all messages are authenticated. In contrast, when an MITM adversary modifies Alice's transmitted trip signal by forcing its value from "1" to "0", as shown in Fig. 6 (b), Bob no longer receives the tripping command, and the HMACValid indicator in Fig. 6 (d) drops to 0 during the attack, showing that the tampered GOOSE message fails authentication and is immediately discarded.

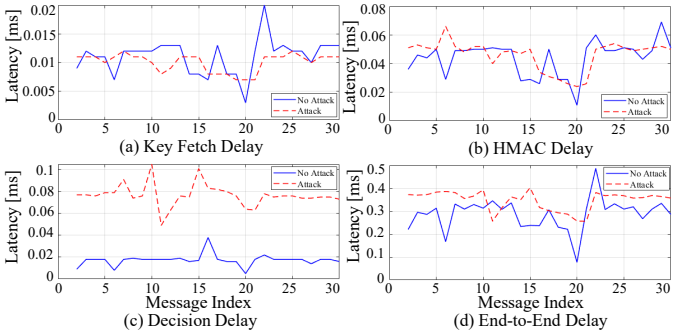

Fig. 7: Latency analysis of QKD-HMAC protected GOOSE communication

Fig. 7 presents the latency characteristics of the QKD-HMAC protected GOOSE communication channel. The results show that all component delays remain at the sub-millisecond level, and the end-to-end (E2E) latency consistently stays below 0.5 ms. This demonstrates that our protection structure does not introduce noticeable overhead to the ROCOF communication channel.

The above results confirm that QKD-derived keys used for HMAC enable reliable real-time detection of falsified trip signals on the GOOSE channel, thereby ensuring that only authentic protection commands are executed.

C. Validation of QS-ROCOF based Protection

The performance of the developed QS-ROCOF protection is validated with the modified NPCC system. A severe load imbalance case, i.e., synchronous generators G1, G2 and G3 outage, 1.8 GW tripped power, is performed so that the system would collapse without load shedding. Therefore, the trip signal should be secured to make sure the loads can be shed timely. Two scenarios, i.e., without and with the developed QKD-based ROCOF protection, are provided. The testing results without the QKD-based protection are shown in Fig. 8.

As shown in Fig. 8(a), when generators G1, G2, and G3 are tripped, the ROCOF drops below the 0.7 Hz/s threshold for load shedding. Consequently, the load-shedding command (Alice trip), shown in Fig. 8(b), is issued and sent to the load. Without the proposed HMAC-based authentication, the received command (Bob trip) is altered by an MITM attack and is therefore invalid. As a result, load shed could not be performed in time, leading to a severe generation–load imbalance. As illustrated in Fig. 8(c), this imbalance ultimately leads to system collapse.

The testing results with QKD-based ROCOF protection are shown in Fig. 9. It can be seen that once a severe event occurs, the ROCOF is below the threshold, and a trip signal is sent to

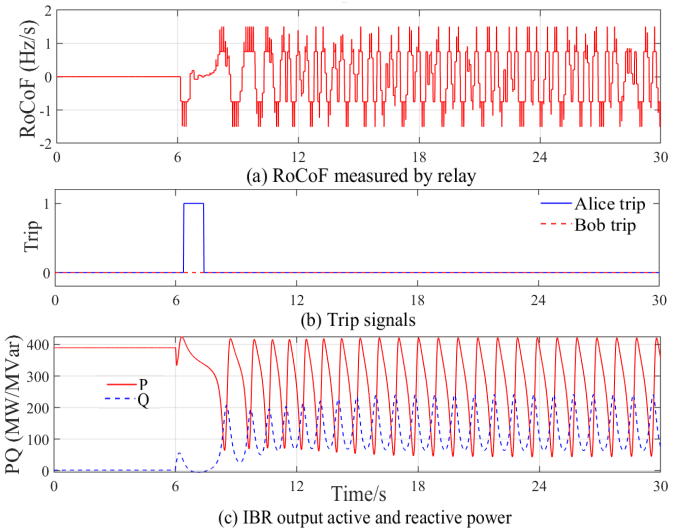

Fig. 8: Testing results without QKD-based ROCOF protection

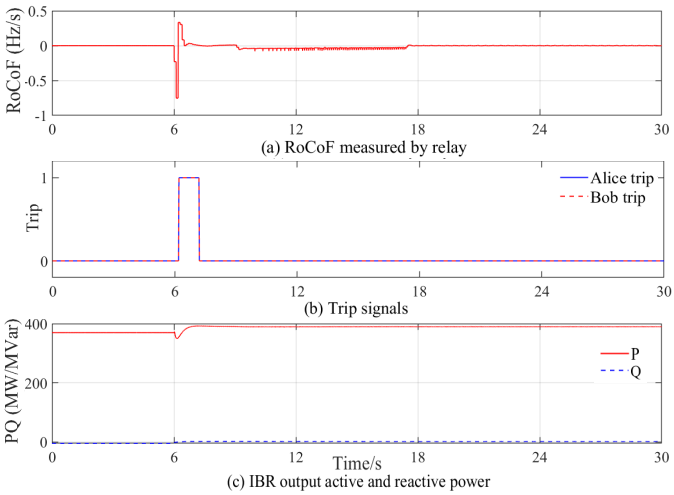

Fig. 9: Testing results with QKD-based ROCOF protection

the loads to be shed. With the HMAC-based method, the trip signal can be corrected even if the MITM attack manipulates the original trip signal, as shown in Fig. 9(b). Therefore, the system remains stable since the balance between power generation and load is well maintained.

In summary, the testing results in Figs. 8 and 9 demonstrate that the proposed QS-ROCOF protection method ensures secure trip delivery and preserves grid stability. Even under cyberattacks or quantum-channel intrusion, the system can immediately detect and reject compromised signals, thereby maintaining both communication integrity and overall system-level stability.

V. Conclusion

This work presents the first room-temperature QS-ROCOF framework for power grids. By integrating QKD with lightweight HMAC authentication in a GOOSE-based ROCOF scheme, the proposed architecture enables real-time validation of trip commands—combining the speed of lightweight hashing with the physics-level security of quantum keys.

Hardware-in-the-loop experiments show that both cyber manipulation of GOOSE messages and intrusion on the quantum channel are immediately detected and rejected, ensuring the integrity of protection signals and preserving system stability. These results demonstrate that quantum-secure protection can enhance both the cyber and operational reliability of future inverter-dominated, cyber-physical grids.

Looking ahead, this framework can be extended to multi-node, wide-area protection and applied to different types of relays, with future work exploring performance limits under extreme operating conditions, offering a pathway toward quantum-enhanced security in large-scale utility networks.

References

[1] T. Bašakarad, N. Holjevac, I. Kuzle, I. ivanković and N. Zovko, "Rocof importance in electric power systems with high renewables share: a simulation case for croatia," The 12th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MEDPOWER 2020), Online Conference, 2020.

[2] ICS Investigation Expert Panel, "Grid incident in Spain and Portugal on 28 April 2025," ENTSO-E Factual Report, Oct. 2025.

[3] A. d. Santos, B. Soares, C. Fan, M. Kuipers, S. Sabino, A. M. R. C. Grilo, P. R. B. A. Pereira, M. S. Nunes, and A. Casaca, "Characterization of substation process bus network delays," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2085-2094, May 2018.

[4] S. Hussain, A. Iqbal, S.S. Hussain, S. Zanero, A. Shikfa, E. Ragaini, I. Khan and R. Alammari, "A novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids," *Scientific reports*, 2023.

[5] Y. Zhou, Z. Tang, N. Nikmehr, P. Babahajiani, F. Feng, T.-C. Wei, H. Zheng, and P. Zhang, "Quantum computing in power systems," *iEnergy*, vol. 1, no. 2, pp. 170-187, June 2022.

[6] L. Wang, P. Zhang, Z. Tang, and Y. Qin, "Programmable crypto-control for IoT networks: an application in networked microgrids," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7601-7612, May 2023.

[7] Z. Tang, P. Zhang, W. O. Krawec and L. Wang, "Quantum networks for resilient power grids: theory and simulated evaluation," *IEEE Transactions on Power Systems*, vol. 38, no. 2, pp. 1189-1204, March 2023

[8] Z. Tang, P. Zhang, W. O. Krawec and L. Wang, "Enabling resilient quantum-secured microgrids through software-defined networking," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1-11, 2022.

[9] Z. Tang, P. Zhang, W. O. Krawec and Z. Jiang, "Programmable quantum networked microgrids," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1-13, 2020.

[10] Z. Tang, P. Zhang and W. O. Krawec, "A quantum leap in microgrids security: the prospects of quantum-secure microgrids," *IEEE Electrification Magazine*, vol. 9, no. 1, pp. 66-73, March 2021.

[11] P. Zhang, *Microgrids: Theory and Practice*. John Wiley & Sons, 2024.

[12] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan,"Secure quantum key distribution with realistic devices,"*Reviews of Modern Physics*, vol. 92, no. 2, pp. 025002, 2020.

[13] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec and P. Zhang, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1250-1263, March 2021.

[14] Q. Hong, M. Karimi, M. Sun, S. Norris, O. Bagleybter, D. Wilson, I. F. Abdulhadi, V. Terzija, B. Marshall, and C. D. Booth, "Design and validation of a wide area monitoring and control system for fast frequency response," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3394-3404, July 2020.

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.

[16] R. Wolf, *Quantum Key Distribution*, Springer, 2021.

[17] Z. Gao, J. Wang and M. Illindala, "Intrusion detection system with updated structure and feature selection algorithm for Man-in-the-Middle attacks in the smart grid," *IEEE Transactions on Industry Applications*, vol. 61, no. 5, pp. 8150-8157, Sept.-Oct. 2025.