ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Quantum Encryption Techniques for Securing Low-Voltage Communication Systems in Next-Generation Data Transmission Networks

Erwei Tian[1,*], *Jianbin Zhang*[1] *and Tianjian Zhao*[1]

[1] State Grid Zhejiang Electric Power Co., Ltd. Shaoxing Power Supply Company, Shaoxing, Zhejiang, 311800, China

SUMMARY: *Low-voltage communication systems in next-generation data transmission networks connect smart meters, feeder controllers, EV chargers, and distributed energy resources; however, the dense topological structure they have and the limited abilities of their endpoints make the direct deployment on quantum hardware be not practical. In order to solve this restriction, this article puts forward a Hybrid Quantum Encryption Scheme for Low-Voltage Systems (HQES-LV), which keeps quantum key distribution on backbone and gateway layers, uses a post-quantum authenticated control plane, and gives lightweight session protection to edge devices by means of risk-adaptive key renewal. A literature-calibrated digital twin is constructed to simulate mixed control, telemetry, and maintenance traffic, along with replay attacks, man-in-the-middle probing, quantum channel degradation, and gateway outages. Result data indicate that in the pressure condition, the HQES-LV can cut control waiting time down to 6.1 ms, hold the possibility of secret information leakage to 0.4%, and make the time of getting back to normal shorter to 6.7 s. Under a 1.2 p.u. load, it maintains 7.3 ms latency and 98.4% session establishment success. When QBER rises to 5.5%, the proposed scheme still preserves 58.9% effective key availability and 96.7% packet delivery. These findings indicate that practical quantum security for low-voltage systems should be realized through hierarchical orchestration rather than endpoint quantumization, and that the combination of QKD backbone supply, post-quantum fallback, and the adaptive session arrangement can provide a path that is more ready for deployment for future electric power communication networks.*

KEYWORDS: *quantum key distribution; low-voltage communication systems; smart grid cybersecurity; adaptive key scheduling; quantum-classical integrated networks*

1 Introduction

Low-voltage communication systems are the end which is closest to the field in next-generation data transmission networks. Intelligence electric meters, feeder supervision terminals, distributed electric power controllers, energy storage connection ports, and charging establishments continuously carry out the exchange of meter-reading data, condition messages, warning notifications, and control instructions; these communication behaviors directly give support to distribution network state knowing, load adjustment, and edge operation maintenance. The difficult point consists in the great quantity of low-voltage nodes, various connection types, and restricted terminal calculation ability and energy supply budgets. One individual safety mechanism frequently has difficulty in handling together key renewing

*tewhappy@163.com
https://doi.org/10.65102/is20261017
Published: 30 April, 2026

frequency, communication time delay, and long-time arrangement expenses. Power distribution network application items which take smart meter data as the core have expanded from the simple data gathering work to the state estimation, the operation optimization, and the dispatch support, meanwhile the attack surfaces and the entry points of the smart meters themselves have had the corresponding increase [1, 2].

This kind of contradiction circumstance mainly is manifested on the adaptive ability of the traditional public key infrastructure. Low-voltage communication connectionssince long time agohave trusted identity verificationand key exchange methodswhich are based on classical calculation difficult problems; however, under the background that the threat of quantum computing is gradually approaching, only depending on traditional public-key systems can not give a solution that is effective for a long time. With reference to intelligent power grid communication safety, the current studies have already conducted systematic reviews on the adaptive ability, deployment demands, and safety worth of QKD protocols in electric power application situations [3]; Besides this, Alshowkan and other researchers have already proved that using QKD keys can realize the verification of machine-to-machine communications in smart power grids on real public optical fiber networks [4]. In regard to dispersed energy sources, Ahn and other researchers have also put forward a method to combine post-quantum cryptography and QKD together into power edge infrastructure [5]. These endeavors show that power communication security is moving from the problem of "whether quantum security is needed" to "how to realize quantum security."

In the same period, low-voltage communication systems by their own nature are continuously promoting the increase of data density and control sensitivity. Investigation concerning control and optimization on the basis of smart meter data has already proven that communication on the distribution level is no longer only a backend data recording interface, but has entered a closed-loop system that includes state modeling, local optimization, and load prediction [6]. This indicates that security events on low-voltage connections do not only influence privacy any longer, but they also have possibility to affect the control effect and the stability of edge reactions. Comparable viewpoints have appeared in high-level power communication situations, for example studies on QKD safety schemes for key infrastructure including hydropower stations and water barriers [7], as well as analyses of QKD applications for intelligent operation and maintenance of power communication networks [8]. However, the great majority of these research works still get limited to key nodes, special connecting lines, or individual situation types. Regarding access environments which have the features of dense low-voltage terminals, mixed services and long-time online connection work, there still exists the lack of one method that has clear structure, results that can be checked, and deployment constraints which are clearly defined.

Developments in network technology have further heightened the practical urgency of this issue. Recent research no longer views QKD as a point-to-point technology that must rely on isolated dark fiber. Udvary discussed the integration of QKD channels with high-speed classical optical communication networks [9]; Mandil et al. introduced packet switching into QKD networks [10]; Pagano et al. addressed the design of QKD fiber networks from the perspective of the overall quantum layer rather than individual transmission links [11]; Zhang et al. further incorporated routing, channels, key rates, and time slot allocation into a joint optimization framework [12]. At the engineering level, MadQCI has demonstrated the long-term deployability of heterogeneous SDN-QKD networks in production facilities [13]; Dou et al. demonstrated the feasibility of coexistence between QKD and 11 Tbps classical optical transmission over single-mode fiber at distances of hundreds of kilometers [14]; Bae and Koh, on the other hand, have QKD been integrated by them into access network link design problems

[15]. These progressions on the whole show that QKD is getting into a new stage of co-building, fiber sharing, and together arranging with next-generation data transmission networks. When we look deeper, the difficulty in low-voltage communication situations does not only lie in "whether we should bring in quantum security", but it lies in the long-existing mismatch on speed and scale between the supply ability of quantum keys and the session requirements of edge sides. The demands on protection control, state collection, and maintenance communication with respect to time delay, update frequency, and continuation are not uniform. If a uniform key update strategy is adopted, it often amplifies scheduling pressure on the gateway side during high loads or local anomalies.At the same time, low-voltage terminals are numerous, widely dispersed, and have long retrofitting cycles, making it difficult to achieve the conditions for directly supporting quantum capabilities through hardware upgrades in the short term. Therefore, the real question is not whether quantum keys can be generated, but how to stably map limited quantum key resources to high-frequency, dense, and service-diverse edge communication sessions while keeping terminal configurations largely unchanged.

However, three key gaps remain between existing research and low-voltage communication systems. First, most studies deploy quantum capabilities on metropolitan backbones, dedicated experimental links, or high-value nodes, assuming that terminals possess favorable environmental and hardware conditions; in contrast, low-voltage terminals are typically numerous, widely dispersed, and power-constrained, lacking the practical foundation to directly support quantum optical modules.Second, existing smart grid-related work either emphasizes the scenario applicability of QKD or focuses on a specific type of communication authentication or link integration [16, 17], but rarely treats "how to transform quantum backbone keys into keys for dense sessions at the low-voltage end" as a core objective.Third, when quantum links degrade, key pools become depleted, or local gateways fail, existing work typically addresses authentication, routing, or resource allocation separately, lacking a systematic evaluation that integrates post-quantum authentication in the control plane, edge session refresh, adaptive fallback, and service continuity into a single experimental protocol.

In view of these blank spaces, the core problem which this paper deals with is: how to build a layered quantum cipher system-that does not directly arrange quantum hardware on low-voltage terminals-which guarantees the control center and backbone connections can obtain the high-degree key safety that QKD gives, therefore at the same time it keeps allowable time delay, key update speeds, and malfunction restoration abilities on the low-voltage edge. For solving this problem, this article puts forward a mixed quantum encryption plan for low-voltage communication systems, which is named HQES-LV. This project keeps QKD in the backbone and gateway layers, keeps arrangement trust by a post-quantum certificate control plane, and passes quantum safety advantages to low-voltage end devices through a risk-conscious conversation key update method.

This research puts emphasis on three aspects. Firstly, we build a system object arrangement inside the low-voltage communication hierarchical structure, which integrates the control center, regional gateways, feeder coordination nodes and terminal sessions into a unified key arrangement framework. Second, we put forward HQES-LV, which coordinates backbone QKD, the ML-KEM/ML-DSA control level, and light-weight symmetric encrypting at the edge, thus using risk-aware methods to confirm the session key update frequency. In the end, we build a digital twin experimental protocol calibrated with existing literature to make quantitative analysis on the system's transmission performance, security continuity, recovery ability, and deployment influences under the conditions of mixed traffic loads, attack injection, quantum link degradation and gateway failure.

2 Study on Mixing Quantum Cipher for Low Pressure Communication Systems in Next Generation Data Transfer Networks

2.1 System Modeling and Data Calibration for Low-Voltage Communication Hierarchy

The security arrangement of low-voltage communication systems cannot be separated from their actual working circumstance. Different from main station side or special backbone connecting lines, low-voltage situations at the same time bear many kinds of business works, include cycle data upward passing from intelligent electricity meters, feeder condition gathering, scattered power origin controlling, energy storage interface matching, and charging equipment entering. These systems have the characteristic of a great quantity of communication entities, scattered positions, and obvious differences in device abilities, with a large quantity of terminals that work for a long time under low-power, weak-computing conditions with restricted O&M accessibility. Under these circumstances, the direct adoption of a unified key renewal scheme which has been designed for backbone networks, therefore, is easy to bring about key negotiation congestion in regions that have high terminal density, and hence makes it hard to keep the continuity of control services when link performance becomes worse. Hence, this article firstly carries out abstraction of the low-voltage communication system to become a four-layer object hierarchy which contains a control center, regional gateways, feeder coordination nodes, and low-voltage terminals, and thus uses this as a unified framework for follow-up key orchestration and security assessment.

The controlling center takes charge of the global key management work, the issue of risk policies, and the cross-region dispatching work; the area entrance port is in charge of quantum key receiving, key store memory saving, and safe condition gathering together; Feeder coordination nodes are put at the access edge, they take charge of arranging session seeds in accordance with service priority, storing short-term keys, and keeping local key exchange rhythms; low-voltage end points only keep traditional communication interfaces and light encryption abilities, and do not directly carry quantum modules. This kind of layered method is on the basis of two practical considerations. First of all, quantum type devices possess high-level demands for power supply systems, temperature control systems, and link working conditions; the deployment of these devices in control centers and regional gateways is better in accordance with the current engineering constraints. Second, the quantity of low-voltage terminals far surpasses the number that gateways have; Concentrating quantum abilities on sustainable nodes and then spreading them downward through classical security arrangement is more beneficial to controlling the whole deployment expenses and the follow-up operation complexity.

After we confirm the object level arrangement, this paper furthermore divides communication flows into three kinds according to business features. The first kind is protection and control works, named as C1, which mainly contains switch control, alarm connection, and local adjustment orders; these service items are most sensitive to time delay and continuous working condition. The second type is made up of telemetry and meter reading services, which are called C2. These main contents include the uploading of measurement data, state values, and event record documents. Although the average data rate of them is comparatively low, short-term sudden increases of data will take place inside the sampling time windows or on occasions when the working state has alterations. The third kind contains maintenance and firmware services, which are given the name C3. These main works include parameter downloading, configuration synchronizing, and firmware upgrading. This kind needs bigger

data amounts in each transmission, but it has relatively lower demands on millisecond-level real-time property. This categorization not only has the function of dividing services but also can offer a clear priority basis for the following key lifecycle management and resource arrangement: C1 services therefore get priority for stable, short-period session protection with quick recovery; C2 services put their key point on guaranteeing low overhead expenditure and dependability under long-term internet working situations; and C3 services put their focus on lowering the bad influence toward the gateway key pool and control plane when centralized updates are carried out.

For making method assessment more near to the real operation pressures of low-voltage situations, this paper build a testing network that includes 1 control center, 4 region gateways, 16 feeder coordination nodes, and 256 low-voltage terminals. The terminal side consists of 160 smart meters, 48 feeder monitoring/control units, 32 charging facilities, and 16 distributed energy controllers. The control center and regional gateways are connected via quantum backbone links, while regional gateways communicate with feeder coordination nodes, and feeder coordination nodes communicate with terminals via classical links. The security key rate, channel attenuation, and error rate perturbation range of the backbone quantum links were set based on typical parameter ranges from recent research on QKD power communication, access network integration, and fiber-sharing transmission. Edge link latency and service arrival processes were calibrated based on the characteristics of low-voltage meter reading and status data collection services[18-20]. Through this approach of "quantum backbone real-world constraints + low-voltage edge service mapping," the test scenario preserves both the practical limits of quantum key distribution capabilities and the scheduling complexity resulting from the dense access of low-voltage terminals. To characterize the actual key delivery capability of a service path under the combined effects of current channel loss, error rate fluctuations, and scheduling loss, this paper defines path-level effective key availability, as shown in Equation (1).

$$\kappa ppa_p = \min_{e \in p}(R_e^{\sec}(1 - \delta_e)) \tag{1}$$

In the equation, κp represents the effective key availability on path$p$; $R_e^{\sec}$ represents the secure key rate of link$e$; and δ_e represents the key loss ratio caused by increased QBER, link jitter, or scheduling drops. To ensure a consistent basis for subsequent comparisons, this paper uniformly configures the test network's object scale, service categories, link conditions, and event injection parameters, as shown in Table 1.

Table 1: Configuration of the Low-Voltage Communication Testbed

Item	Setting
Control Center	1 unit, QKD main key orchestration node, 40 Gb/s fiber uplink
Regional Gateway	4 units, QKD key pool nodes, each with initial cache of 8 Mbit
Feedline Coordination Node	16 units, local cache of 2 Mbit, responsible for session distribution
Low-Voltage Terminals	256 units, no quantum module, only classic interfaces
C1 Service	Protection/control messages, 256 B, 50 pkt/s, target delay ≤ 10 ms
C2 Service	Telemetry/meter reading messages, 512 B, 0.2 pkt/s, peak burst factor 2.4
C3 Service	Maintenance/firmware messages, 4 KB fragments, event-triggered
Optical Link Conditions	Attenuation 8-16 dB, baseline QBER 1.5%-5.5%
Attack Scenarios	Replay 10%, man-in-the-middle detection 6%, load burst 1.2 p.u., single gateway interruption 300 s
Statistical Protocol	30 repetitions per scenario, 1800 s per repetition

The minimal effective key configuration ability along the path is taken as the upper limit herein because session renewals for low-priority services are finally restricted by the weakest node in the whole key configuration path. If on a determinate path the upstream portion has obvious worsening, the downstream portion cannot gain enough high-level core support, even when the abilities of calculation and storage are sufficient. By introducing the κp, the subsequent scheduling module can consolidate the previously dispersed link states, key rates, and loss factors into a single, actionable metric, providing a unified basis for key exchange frequency control and fallback triggering on the gateway side. To avoid deploying quantum hardware directly to low-pressure endpoints, this paper first organizes system objects into a hierarchical collaborative structure, as shown in Figure 1.

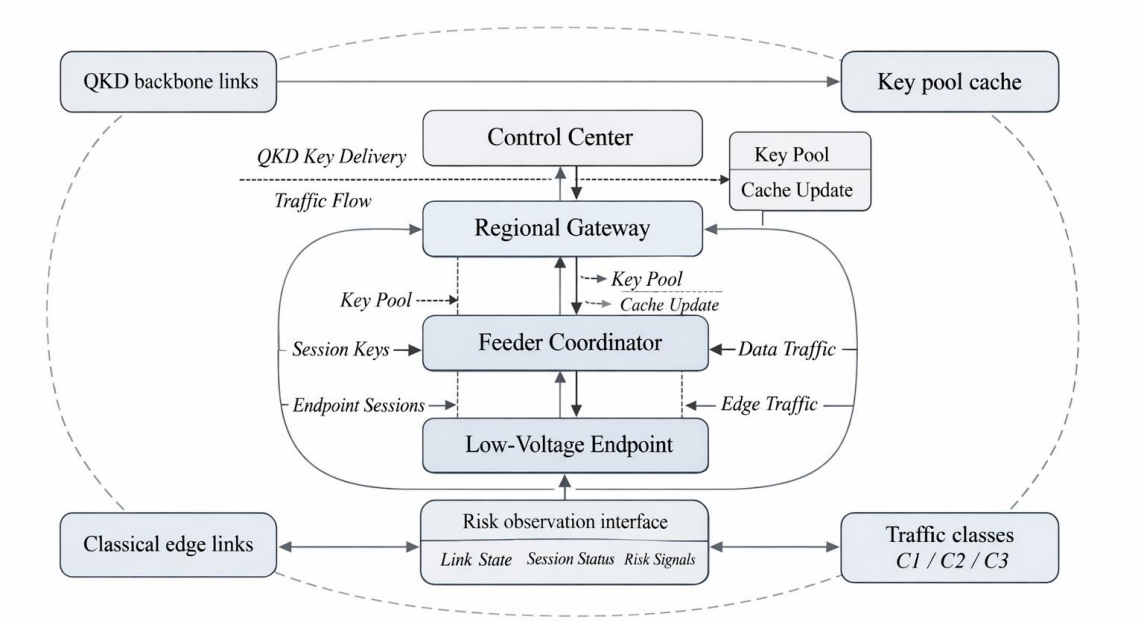

Figure 1: Hierarchical Low-Voltage Communication and Object Organization Mechanism for a.

2.2 Hybrid Quantum Encryption Architecture and Adaptive Key Scheduling

When the object modeling work has been finished, this paper puts forward a mixing type quantum encryption scheme, HQES-LV, which is used in low-voltage communication systems. This scheme has no attempt to give direct distribution of quantum keys to every terminal; On the contrary, it separates quantum key distribution, control plane identity verification, and edge session guard into different layers to carry out cooperative processing. One high-level main secret key is produced through QKD among the control center and the area gateways. Area entrance nodes carry out divided caching and state marking of quantum secret keys, hence they send out session starting seeds to supply cooperation nodes on the basis of supply load, service precedence, and abnormal examination results. The feeder coordination node has no behavior of directly forwarding the original quantum key; on the contrary, it produces short-existence session keys according to the local service framework, which are utilized for AES-256-GCM message protection on the terminal side. This method assists in lowering the direct consumption of quantum keys in high-concurrency edge communication situations, and thus it eliminates the terminal's dependence on special-purpose quantum hardware and complicated authentication stacks.

The control plane of HQES-LV employs post-quantum authentication mechanisms to maintain the reliability of orchestration. Specifically, control messages and key scheduling messages are encapsulated with temporary keys using ML-KEM, and signature verification is performed using ML-DSA.Its purpose is not to replace quantum key distribution, but to ensure that the system can maintain the continuity of key exchange and control messages via verifiable post-quantum classical paths even when backbone quantum links fluctuate, regional gateways experience local failures, or the key pool is temporarily depleted.In other words, QKD is responsible for providing the system with a long-term source of high-grade keys, while the PQC control plane is responsible for maintaining the trusted execution of scheduling commands and fallback procedures; the two undertake security tasks at different levels within HQES-LV. Considering that different service flows exhibit significant differences in criticality, attack exposure levels, and burst characteristics, this paper further defines a comprehensive risk score to quantify the security pressure on terminals or service flows, as shown in Equation (2).

$$\psi_i = \omega_1 c_i + \omega_2 a_i + \omega_3 d_i + \omega_4 b_i \tag{2}$$

In the equation, ψ_i represents the comprehensive risk score of terminal or service flow i; c_i represents service criticality; a_i represents the currently observed attack intensity; d_i represents device exposure; b_i represents the business burst factor; ω_1 through ω_4 are normalized weights, set to 0.35, 0.25, 0.20, and 0.20, respectively. The above weight settings reflect the scheduling preferences outlined in this paper: in low-load scenarios, business criticality remains the primary factor determining the allocation of session update resources, followed by attack intensity, while long-term device exposure and short-term burst behavior jointly influence the specific contraction magnitude [21-24]. The risk score is not used directly to determine whether a packet can be transmitted, but rather to adjust the session key lifetime and refresh priority. This approach prevents the system from performing key exchanges at the same frequency for all terminals during periods of high load, thereby prioritizing the allocation of limited key resources to entities that are genuinely high-risk, highly time-sensitive, or continuously exposed. After obtaining the comprehensive risk score, this paper jointly maps the path key state and business risk to the session key refresh interval to characterize the dynamic key renewal cycles of different services under real-time constraints, as shown in Equation (3).

$$\tau_i = \min\left(\tau_{\max}, \max\left(\tau_{\min}, \frac{\beta \kappa_{p(i)}}{1 + \psi_i}\right)\right) \tag{3}$$

In the equation, τ_i represents the session key refresh interval for business flow i; $\tau_{\min}$ and $\tau_{\max}$ denote the minimum and maximum refresh intervals allowed by the system, set to 30 s and 300 s in this paper, respectively; β is a proportional coefficient, set to 12 in this paper; this function is subject to three constraints. First, when path key provisioning capacity improves, the system can moderately extend the key refresh cycle for low-risk businesses to reduce the control plane load.Second, when the risk score rises, τ_i is reduced, resulting in shorter session lifetimes for control, protection, or high-exposure endpoints. Finally, by clipping $\tau_{\min}$ and $\tau_{\max}$, the system prevents excessively frequent key exchanges or prolonged periods without key updates under extreme conditions.

For the sake of making sure that the scheduling on gateway side does not get restricted within theoretical formulae, this article further carries out the definition of the actual execution flow of HQES-LV. The area entrance first computes the usable degree of the secret store based on the upper quantum connection condition and this machine buffer size, hence keeps a multi-row meeting demand list arranged by supply line and service kind. As for C1 services, when a request comes, session seeds are distributed in accordance with the shortest feasible refresh

cycle, hence priority is given by us to usable key caches which lie on paths with low time delay. Regarding C2 services, the system makes adjustment to the refresh cycle according to historical arrival rules and peak fluctuations, for the purpose of preventing meter reading peaks from overlapping with key exchange peaks. Regarding C3 services, the gateway puts batch windowing in first priority to arrange key exchanges and transmissions, thus it decreases control plane expense when configuration download is conducted. If the κp of a particular link remains persistently below the threshold, the system prioritizes reallocating cached keys from neighboring gateways; if the τ_i requirement cannot be maintained after reallocation, the system enters the PQC fallback path, where ML-KEM encapsulates temporary session seeds and ML-DSA signs scheduling messages. Only when the quantum key supply returns to a stable range will the service flow switch back to the quantum key-dominated refresh mode.

The above design endows HQES-LV with three methodological characteristics. First, quantum keys are not directly bound to terminals but are first reorganized via the gateway and feeder coordination nodes, thereby transforming scarce high-level keys into resources that can sustainably support edge session protection. Second, the key exchange cycle is determined jointly by risk scoring and path key provisioning capabilities, avoiding the resource waste and disruption of critical services caused by uniform refresh cycles. Third, the fallback mechanism is not an independent add-on module but is embedded within the entire session scheduling process, maintaining the continuity of the security control plane when quantum key provisioning is insufficient, attacks intensify, or nodes malfunction. For low-voltage communication systems, this hierarchical coordination is better suited to operational conditions characterized by long-term connectivity, dense node deployment, and significant load fluctuations than simply adding a specific type of encryption algorithm. Once the object hierarchy and scheduling logic are defined, the key modules of HQES-LV and their functional relationships can be further summarized as a unified hybrid encryption orchestration mechanism, as shown in Figure 2.

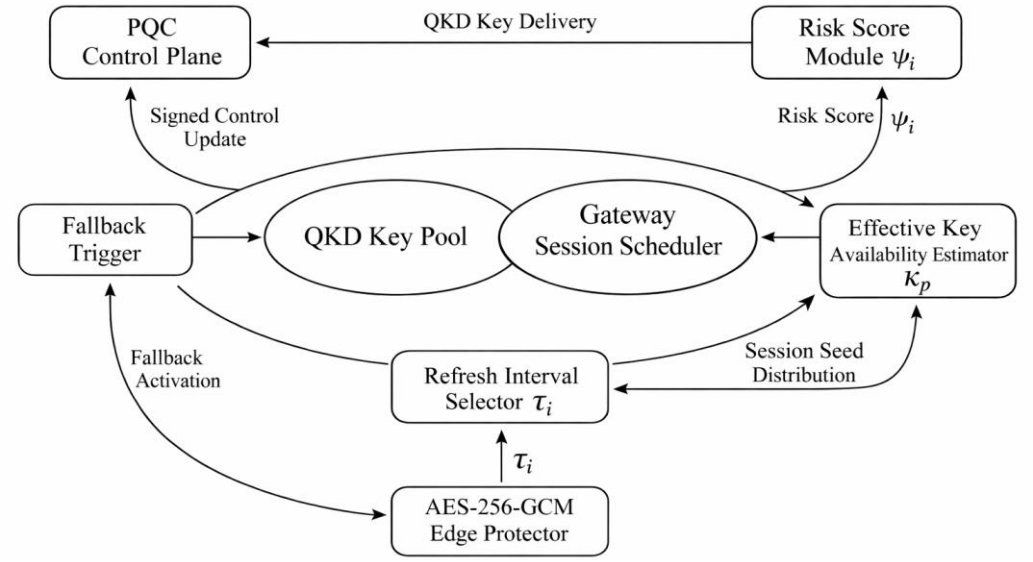

Figure 2: Hybrid Quantum Encryption and Adaptive Key Orchestration Mechanism.

2.3 Comparative Scheme Setup and Protocol Design Evaluation

For the purpose of verifying that HQES-LV has effect in low-voltage situations, this paper puts forward four comparison plans. The Classical plan uses traditional ECC-PKI to be the control plane authentication method, utilizes AES-256-GCM in the data plane, and therefore renews

the session key at a fixed time interval of 300 seconds; The pure PQC scheme utilizes ML-KEM-768 and ML-DSA-65 as control-plane methods, while the data plane still uses AES-256-GCM, with session keys get renewed each 180 seconds; The QKD-static method lets QKD key distribution be conducted between the control center and regional gateways, but it does not employ risk-aware scheduling or PQC backup; keys are undergone a renewal at the edge each one hundred and eighty seconds; HQES-LV is the scheme that this paper puts forward, which on the foundation of quantum backbone key distribution, introduces risk scoring, adaptive refresh and post-quantum fallback. These four schemes have the same network topology structure, service injection scripts, and failure time windows, in order to guarantee a consistent foundation for comparison. For the guarantee of comparability between different schemes, this paper gives unified definitions to control plane mechanisms, key sources, edge protection methods and refresh strategies, which is displayed in Table 2.

Table 2: Baseline Schemes and Cryptographic Settings

Scheme	Control Plane Authentication	Key Source	Edge Protection	Refresh/Fallback Strategy
Classical	ECC-PKI	Classical Negotiation	AES-256-GCM	Fixed 300 s, no fallback
PQC-only	ML-KEM-768 + ML-DSA-65	Post-Quantum Negotiation	AES-256-GCM	Fixed 180 s, no quantum key fallback
QKD-static	Pre-shared Authentication + QKD backbone key	QKD Key Pool	AES-256-GCM	Fixed 180 s, risk-adaptive, no PQC fallback
HQES-LV	ML-KEM-768 + ML-DSA-65	QKD backbone key + temporary PQC fallback	AES-256-GCM	Adaptive 30-300 s, fallback supported

The experiment flow plan is split into three levels. The first layer is made of basic load testing, which is utilized for observing the changes of time delay, key building success rate, and package sending stability of different schemes when the provided load rises under situations where there are no clear attacks. In this article, the provided load is step-by-step increased starting from 0.4 p. u. to 1.2 page. u. to include three representative working situations: low loading, rated loading, and short-time over loading. The second layer is composed of stress situation testing, which overlays 10% playback traffic, 6% man-in-the-middle detection affairs, and as high as 5.5% QBER shake on the basic load. This level puts emphasis on assessing the system's ability of withstanding quantum link worsening and control plane abnormal situations. The third layer is constituted by fault recovery testing, wherein the quantum key distribution link of one regional gateway is deactivated inside a fixed incident window to observe alterations in key pool usage, control service delay, and the time of recovery. Each situation is repeated 30 times, with average values being recorded and fluctuation scopes being retained for following result analysis.

The evaluation metrics in this paper cover security, continuity, and resource cost. Security metrics include the probability of confidentiality breach, session key refresh success rate, and control message authentication pass rate; continuity metrics include end-to-end control service latency, latency jitter, packet delivery rate, and session establishment success rate;resource cost metrics include per-session edge power consumption, per-node control overhead, and recovery time. This set of three metric categories was adopted because the deployment value of a low-voltage communication system does not depend on the extreme values of a single security metric, but rather on the ability to maintain control continuity at an acceptable cost.If a solution

can significantly reduce the probability of a breach but simultaneously leads to a sustained increase in control latency or a significant slowdown in fault recovery, its engineering value remains limited. To provide a unified comparison of the overall performance of different solutions in terms of security, transmission continuity, and resource cost, this paper constructs a comprehensive security utility score, as shown in Equation (4).

$$J = \lambda_1 \hat{S} + \lambda_2 \hat{P} - \lambda_3 \hat{L} - \lambda_4 \hat{E} \tag{4}$$

In the formula, J represents the comprehensive security utility score; $\hat{S}$ represents the normalized confidentiality score; $\hat{P}$ represents the normalized packet delivery rate; $\hat{L}$ represents the normalized latency overhead; $\hat{E}$ represents the normalized energy consumption per session; and λ_1 to λ_4 are set to 0.35, 0.25, 0.20, and 0.20, respectively. Security and continuity are given higher weights here because the core focus of low-power communication is not high-throughput data services, but rather a group of edge devices that require long-term online availability, fault recovery, and controllability [25]. The composite metric J does not replace individual results but serves as a basis for overall assessment in ablation analysis and stress scenario comparisons.

In the evaluation work, this paper first operates the four projects on the basis of the identical service script, then records the time delay, link construction, refresh, success breaking probability, and resource use indexes for each situation. After this, group contrast experiments are carried out under the situations of QBER undulations, rising attack strength, and increasing number of influenced gateway links, hence to judge whether the merits of HQES-LV come from the key-sharing mechanism itself or from the synergistic actions of risk-aware scheduling and fallback mechanisms. Through the integration of load testing, stress injection, fault recovery, and metric collection into one unified evaluation framework, this paper additionally delineates the organizational structure of the experimental protocol and evaluation interface, just as Figure 3 shows.

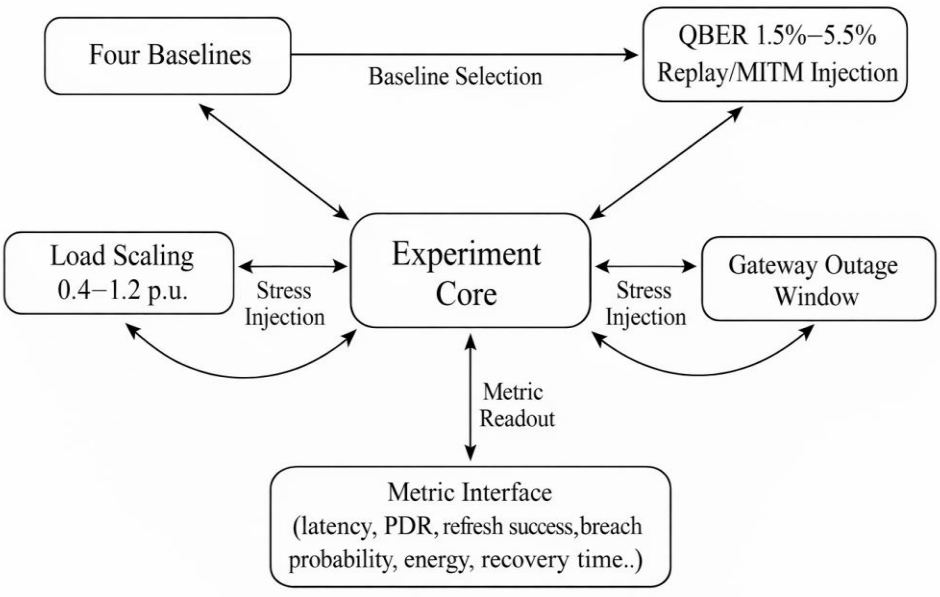

Figure 3: Experimental Protocol, Baseline Grouping, and Evaluation Interface.

3 Performance and Deployment Analysis of HQES-LV in Low-Pressure Communication Scenarios

3.1 Secure Transmission Performance Under Mixed Traffic

After completing the method design, this section first examines the basic transmission performance of HQES-LV under mixed traffic conditions.Low-voltage communication systems simultaneously carry three types of services: control, data acquisition, and maintenance. As the load increases, gateway caching, session updates, and control message processing compete for resources; therefore, relying solely on high-level key sources is insufficient to ensure stable communication at the edge. To compare the transmission latency and session establishment stability of different schemes under continuously increasing mixed-traffic loads, this paper tracks the changes in key metrics as the offered load increases, as shown in Figure 4.

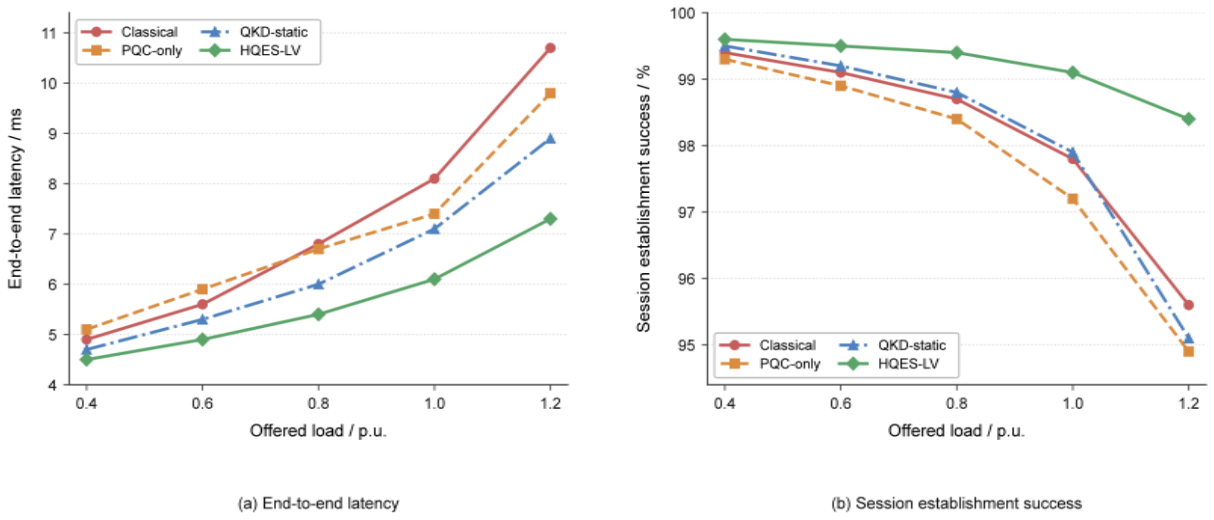

Figure 4: End-to-End Latency and Session Establishment Success versus Offered Load.

In Figure 4, as the offered load increases from 0.4 p.u. to 1.2 p.u., the latency of all four schemes increases, but HQES-LV shows the slowest growth.Under a 1.2 p.u. load, the end-to-end latency of HQES-LV was 7.3 ms, lower than the 8.9 ms of QKD-static, the 9.8 ms of PQC-only, and the 10.7 ms of Classical. This indicates that joint scheduling of key supply status, service risk, and key exchange cycles enables more effective control of session contention on the gateway side.Under low load conditions, the differences among the schemes are minor; however, as the load approaches and exceeds the rated range, the gaps widen significantly. Under a 1.2 p.u. load, HQES-LV still maintains a 98.4% session establishment success rate, while Classical, PQC-only, and QKD-static achieve 95.6%, 94.9%, and 95.1%, respectively.This indicates that the advantage of HQES-LV lies not only in a single transmission process but also in its ability to sustain session availability under high-concurrency conditions. The main results under the stressed scenario are shown in Table 3.

Table 3: Main Quantitative Comparison Under the Stressed Scenario

Metric	Classical	PQC-only	QKD-static	HQES-LV
End-to-End Control Service Delay / ms	8.1	7.4	7.1	6.1
Delay Jitter / ms	1.42	1.33	1.18	0.96
Packet Delivery Ratio (PDR) / %	98.7	98.9	99.1	99.4
Key Refresh Success Rate / %	96.8	97.4	98.2	99.1
Confidentiality Breach Probability / %	3.8	1.9	0.9	0.4
Single Session Edge Energy Consumption / mJ	4.9	7.2	5.6	5.1
Recovery Time / s	18.6	14.8	11.2	6.7

In Table 3, the HQES-LV maintains the control service time delay at 6.1 ms, this is lower than Classical's 8.1 ms, the 7.4 ms of the only use PQC method, and 7.1 ms of the QKD-static; The time delay fluctuation is decreased from 1.42 ms to 0.96 ms, the packet sending success ratio is promoted to 99.4%, and the key renewal success ratio attains 99.1%. On the aspect of safety, HQES-LV has lowered the chance that a secret leakage happens to 0.4%, thus it has a much better performance than the other three projects. These outcomes prove that HQES-LV not only promotes key protection intensity but also promotes the continuation and steadiness of edge-side control services.

Three primary reasons exist which can explain this difference. First, the existence of effective keys on the path level is directly brought into key exchange cycle computation, thus eliminating the dependence on fixed time windows for key management when the load situation is high. Second, through risk scoring, we give priority to those services which have high criticality and high exposure, therefore let them get shorter session cycles. Third, the key pool redistribution which is done at the gateway can mitigate that local peak load loads propagate to become the global link-establishment failures. Hence, the main value of HQES-LV exists in effectively changing the backbone quantum security abilities into session continuousness on the low-pressure edge.

3.2 Robustness Analysis Under Quantum Link Degradation and Module Failure Conditions

The good performance that is got under normal load alone is not enough to prove the deployment value of this scheme. As for low-voltage communication systems, it is more important to make certain whether the system is able to keep a recoverable working condition when quantum link degeneration happens, local hotspots come into being, or gateway abnormalities appear. For the purpose of observing the distribution features of risk space in low-voltage communication topologies under different security configurations, this paper furthermore gives confidentiality risk heatmaps on the zone-to-feeder dimension, which is displayed in Figure 5.

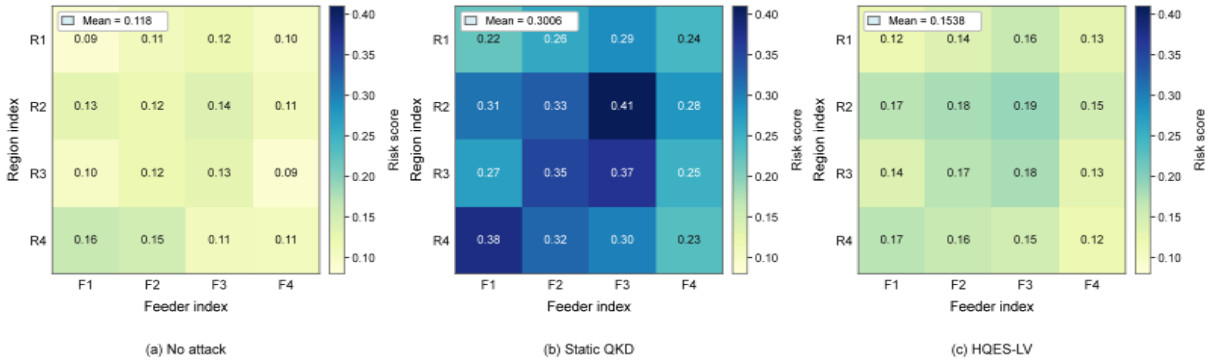

Figure 5: Topology-Wide Confidentiality Risk Heatmaps Under Three Network States.

In Figure 5, when the scenario that no attack happens is considered, the average risk value inside the zone-feeder grid is 0.118; under static QKD situations, the average value increases to 0.3006, and the local hot spots are clearly gathered in the high-concurrency and high-exposure areas; After we use the HQES-LV method, the average risk value falls to 0.1538, and the peak values in hotspot regions also have obvious reduction. This shows that HQES-LV not only just promotes safety intensity on average, but it restrains the ceaseless buildup of danger in partial regions through shortening the conversation life period of high-risk bodies and reallocating the usable key buffer storage. For the analysis of the influence that quantum link degeneration exerts on the system's key delivery ability and the continuity of packet transmission, this paper makes a comparison on the changes of effective key usability and packet delivery ratio under different QBER situations, which is displayed in Figure 6.

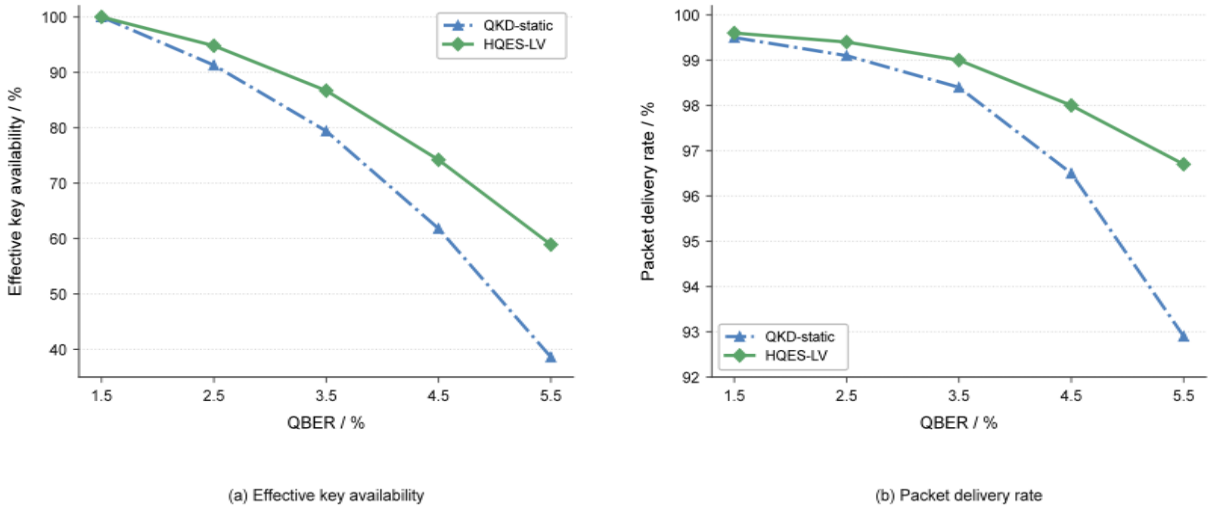

Figure 6: Effective Key Availability and Packet Delivery versus QBER.

As QBER increases from 1.5% to 5.5%, the effective key availability of QKD-static drops from 100.0% to 38.6%, while HQES-LV remains at 58.9%; the corresponding packet delivery rates are 92.9% and 96.7%, respectively.This indicates that once the quantum link enters an unstable range, the static scheme is more quickly affected by insufficient key supply, whereas HQES-LV maintains higher availability through risk compression and post-quantum fallback. To identify the specific contributions of each core module of HQES-LV to overall performance, this paper further conducts an ablation analysis of adaptive refresh, PQC fallback, and gateway key pooling, as shown in Figure 7.

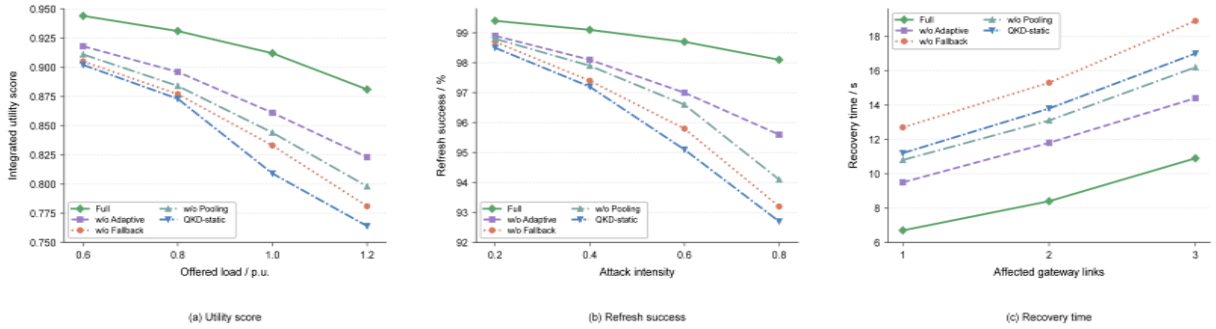

Figure 7: Ablation of Adaptive Refresh, PQC Fallback, and Gateway Key Pooling.

In Figure 7, the comprehensive utility score of the full scheme under a 1.2 p.u. load is 0.881; this drops to 0.823 after removing adaptive refreshing, to 0.798 after removing gateway key pool orchestration, and further to 0.781 after removing PQC fallback, approaching the 0.764 score of QKD-static.Refresh success rates and recovery times follow the same trend: under high attack intensity conditions, the complete scheme maintains a refresh success rate of 98.1%, while the scheme without PQC fallback achieves only 93.2%; when the number of affected gateway links increases to 3, the recovery time for the complete scheme is 10.9 s, whereas it reaches 18.9 s for the scheme without PQC fallback.The results indicate that the robustness of HQES-LV does not stem from any single module, but rather from the synergy of quantum key distribution, adaptive refreshing, key pool orchestration, and fallback mechanisms. HQES-LV maintains a more gradual performance degradation curve under link degradation and local anomalies, capable of limiting the impact of anomalies to a recoverable range.

3.3 Analysis of Resource Overhead, Recovery Process, and Engineering Deployment Suitability

After we have made confirmation that this plan can provide better performance and ability to recover, therefore it is necessary for us to make judgment on whether its resource costs are able to be accepted. Low-voltage communication systems include very many nodes and long work cycles; if the acquisition of security benefits is done at the cost of too much energy use and control extra expenditure, thus the system will have difficulty in providing actual deployment value. For the evaluation of how resource costs change when different session refresh intervals are used, this paper makes a comparison on the relationship between every-session energy consumption and every-node control overhead, which is displayed in Figure 8.

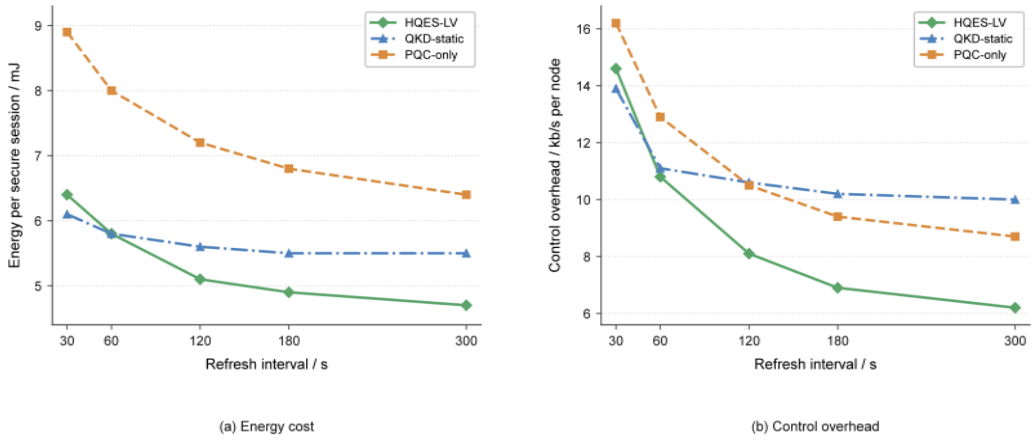

Figure 8: Energy Cost and Control Overhead versus Key Refresh Interval.

In Figure 8, too frequent refreshes significantly increase the burden on the edge execution and control planes. Taking 30 s as an example, HQES-LV's per-session energy consumption is 6.4 mJ, and the control overhead is 14.6 kb/s; when the refresh interval is increased to 300 s, although the control overhead decreases to 6.2 kb/s, the exposure time for high-risk services increases accordingly.A comprehensive comparison shows that approximately 120 s is a more reasonable compromise. At this point, HQES-LV's per-session energy consumption is 5.1 mJ and the control overhead is 8.1 kb/s, both of which are better than QKD-static's 5.6 mJ and 10.6 kb/s, and lower than PQC-only's 7.2 mJ and 10.5 kb/s.This indicates that the benefits of HQES-LV are not achieved by blindly increasing the key exchange frequency, but rather through the targeted use of session update resources. The fault recovery process is shown in Figure 9.

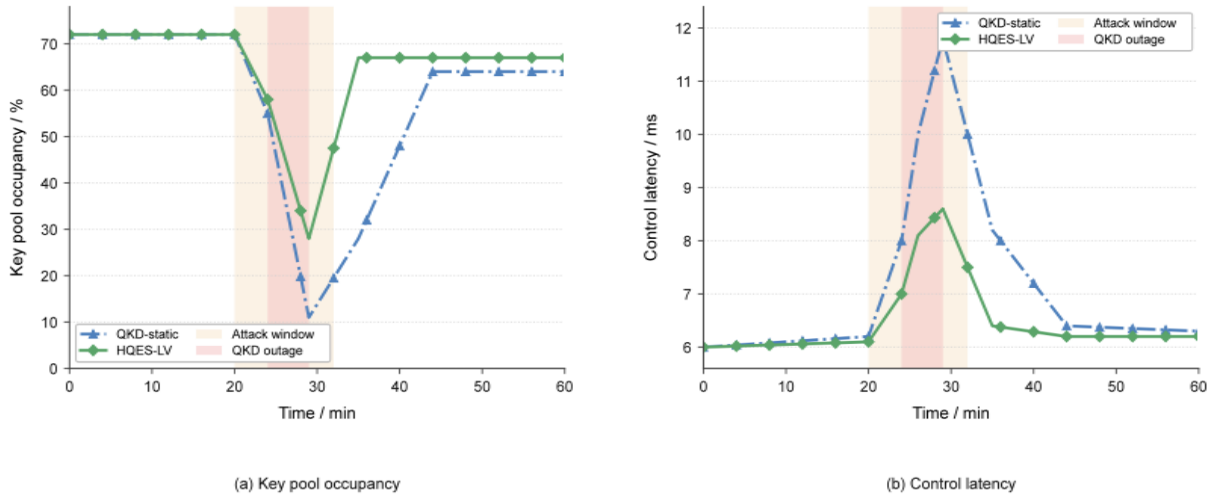

Figure 9: Case Study of Gateway Outage and Attack Recovery.

In Figure 9, within the key supply cut-off period from minute 24 to minute 29, the key pool usage rate of QKD-static quickly decreased from 72% to 11%, while HQES-LV has only dropped to 28%; after the link is recovered, HQES-LV also got back to the stable scope more quickly. The restoring process for control service time delay is likewise shorter: QKD-static got a peak of 11.8 ms, it takes 14.1 s to restore to below 6.5 ms; The peak value of HQES-LV is attained at 8.6 ms, therefore its recovery time is merely 6.7 s. To the control objects on the low voltage side, this indicates that local abnormal situations have a smaller probability to develop into continuous desynchronization of scheduling or concentrated repeated attempts. From the angle of error origins, the outcomes are mainly affected by three elements: changes in the quantum link condition decide the maximum boundary of key provision; the non-uniform coming of edge services enlarges the shortcomings of static key exchange; and the verifying and backup procedures of the control plane hence decide the recovering expense in the abnormal period. By means of risk-perceiving mechanisms and cache redistribution, HQES-LV alleviates the enlarged effects that are produced by the concurrent overlapping of these three kinds of factors. Therefore, HQES-LV is more appropriate for putting into use in low-voltage communication scenes which have the features of numerous terminals, complicated service structures, and area gateways that are provided with enough caching and safe execution abilities.

4 Conclusion

This article discusses the putting into practice of quantum safety protection in low-voltage communication systems that are inside next-generation data transmitting networks. It has built

a layered cooperative framework that includes control centers, regional gateways, feeder coordination nodes and low-voltage terminals, and therefore puts forward HQES-LV. This plan keeps QKD on backbone and gateway layers, keeps the trust of arrangement through a post-quantum verification control plane, hence spreads quantum security benefits to the low-voltage edge by a risk-conscious conversation renew mechanism, hence realizing security promotion without directly placing quantum hardware on the terminal side.

(1) This present paper accomplishes a systematic arrangement and experimental expression of low-voltage communication entities. Regarding the hybrid control, remote measurement, and upkeep services, this paper has built a digital twin test network to carry out comparison analysis. Through bringing key pool condition, service precedence, link worsening, and partial attacks into a combined assessment frame, it gives an analysis platform for quantum safety investigation in low-voltage situations that more nearly matches arrangement restrictions.

(2) The method proposed in this paper achieves a stable balance among transmission performance, security continuity, and resilience. Results show that under stress scenarios, HQES-LV controls the end-to-end delay of control services to 6.1 ms, reduces the probability of confidentiality breach to 0.4%, and shortens the recovery time to 6.7 s; it maintains a 98.4% session establishment success rate under a 1.2 p.u. load, and retains 58.9% valid key availability and a 96.7% packet delivery rate even when the QBER rises to 5.5%. These results demonstrate that quantum security in low-voltage communication systems is better achieved through layered orchestration rather than pursuing end-to-end quantumization.

(3) The present research still possesses certain limitations. The present verification is founded on a literature-calibrated digital twin environment and has not yet handled problems like long-term temperature drift, equipment aging, cross-domain management, and heterogeneous link coordination in actual utility networks; In addition, the edge part still uses a mechanism of quantum secure transmission on the session level. In the future, research work can further combine real feeder operation data from actual scenes, long-time online experiments, and cross-location optical network platforms to carry out more strict verification on the long-term stability, resource cost and engineering maintainability of HQES-LV.

Funding

Technology project funding from State Grid Zhejiang Electric Power Co., Ltd (5211SX230003)

References

Tian Erwei was born in Fuping, Shaanxi Province, China, in 1990. He holds a master's degree and is currently an engineer at State Grid Zhejiang Electric Power Co., Ltd. Shaoxing Power Supply Company, Shaoxing, Zhejiang, China. His main research focus is power system automation.

Zhang Jianbin who is the author entered this world in Zhuji, which belongs to Zhejiang Province, China, in the year 1992. He possesses a bachelor's degree and at present he is an engineer in State Grid Zhejiang Electric Power Co., Company Limited The Power Supply Corporation of Shaoxing, Shaoxing, Zhejiang, in the country of China. The main direction of his research work is the automation of power systems.

Zhao Tianjian took birth in Zhuji, which belongs to Zhejiang Province, China, in the year 1993. He has obtained a master's degree and at present he is an engineering worker at State Grid Zhejiang Electric Power Co., Co. Zhejiang Province, China, Shaoxing City, Shaoxing Electric Power Supply Company. The main direction of his research work is the automation of power

systems.

References

[1] Athanasiadis, C. L., Papadopoulos, T. A., Kryonidis, G. C., et al. (2024). A review of distribution network applications based on smart meter data analytics. Renewable and Sustainable Energy Reviews, 191, 114151.

[2] Nambundo, J. M., de Souza Martins Gomes, O., de Souza, A. D., et al. (2025). Cybersecurity and major cyber threats of smart meters: A systematic mapping review. Energies, 18(6), 1445.

[3] Kong, P.-Y. (2022). A review of quantum key distribution protocols in the perspective of smart grid communication security. IEEE Systems Journal, 16(1), 41-54.

[4] Alshowkan, M., Evans, P. G., Starke, M., et al. (2022). Authentication of smart grid communications using quantum key distribution. Scientific Reports, 12(1), 12731.

[5] Ahn, J., Kwon, H.-Y., Ahn, B., et al. (2022). Toward quantum-secured distributed energy resources: Adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD). Energies, 15(3), 714.

[6] Chen, Z., Amani, A. M., Yu, X., et al. (2023). Control and optimization of power grids using smart meter data: A review. Sensors, 23(4), 2118.

[7] Green, A., Lawrence, J., Siopsis, G., et al. (2023). Quantum key distribution for critical infrastructures: Towards cyber-physical security for hydropower and dams. Sensors, 23(24), 9818.

[8] Wen, H., Xu, A., & Qi, H. (2023). Application of quantum key distribution in intelligent security operation and maintenance of power communication networks. Results in Physics, 54, 107041.

[9] Udvary, E. (2023). Integration of QKD channels into classical high-speed optical communication networks. Infocommunications Journal, 15(4), 2-9.

[10] Mandil, R., DiAdamo, S., Qi, B., et al. (2023). Quantum key distribution in a packet-switched network. npj Quantum Information, 9(1), 85.

[11] Pagano, A., Mercinelli, R., Valvo, M., et al. (2024). Quantum key distribution in optical fibers: A comprehensive design view of the overall quantum layer beyond transmission. Journal of Optical Communications and Networking, 16(8), D111-D118.

[12] Zhang, Q., Ayoub, O., Gatto, A., et al. (2024). Routing, channel, key-rate, and time-slot assignment for QKD in optical networks. IEEE Transactions on Network and Service Management, 21(1), 148-160.

[13] Martin, V., Brito, J. P., Ortíz, L., et al. (2024). MadQCI: A heterogeneous and scalable SDN-QKD network deployed in production facilities. npj Quantum Information, 10(1), 80.

[14] Dou, T., Liu, R., Liao, S., et al. (2024). Coexistence of 11 Tbps (110×100 Gbps) classical optical communication and quantum key distribution based on single-mode fiber. Optics Express, 32(16), 28356-28369.

[15] Bae, S., & Koh, S.-T. (2025). Optical link design for quantum key distribution-integrated optical access networks. Photonics, 12(5), 418.

[16] Grice, W., Olama, M., Lee, A., et al. (2025). Quantum key distribution applicability to smart grid cybersecurity systems. IEEE Access, 13, 17398-17413.

[17] Lin, I.-C., Lin, K.-Y., Wu, N.-I., et al. (2025). A quantum key distribution scheme for securing smart grids. Cryptography, 9(2), 28.

[18] Hernandez-Hernandez, J. C., Larrabeiti, D., Calderon, M., et al. (2025). Designing optimal quantum key distribution networks based on time-division multiplexing of QKD transceivers: qTDM-QKDN. Future Generation Computer Systems, 164, 107557.

[19] Yan, W., Zheng, X., Wen, W., et al. (2025). A measurement-device-independent quantum key distribution network using optical frequency comb. npj Quantum Information, 11(1), 97.

[20] Wu, Q., Ribezzo, D., Di Sciullo, G., et al. (2025). Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers. Light: Science & Applications, 14, 274.

[21] Xie, Y., Hao, Y., Lin, Y., et al. (2025). Efficient routing algorithm for trusted relay quantum key distribution networks via quantum reinforcement learning. Optics Express, 33(22), 46545-46563.

[22] Bhatia, V., Kasegenya, A., & Chen, B. (2025). Dynamic security-aware resource allocation in quantum key distribution-enabled optical networks. Photonics, 12(7), 645.

[23] Sax, R., Boaron, A., Boso, G., et al. (2023). High-speed integrated QKD system. Photonics Research, 11(6), 1007-1014.

[24] National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203).

[25] National Institute of Standards and Technology. (2024). Module-Lattice-Based Digital Signature Standard (FIPS 204).