工程与管理科学
Engineering and Management Science
第 8 卷◆第 10 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

量子安全技术在变电站 IEC61850 通信系统中的应用前景分析

任振兴　赵继爽　陆振军　何佳佳
南京国电南自软件工程有限公司　江苏南京　211100

DOI：10.32629/ems.v8i10.22585

［摘　要］伴随电力系统数字化和智能化进程不断推进，变电站 IEC61850 通信模式已成智能变电站信息交互的关键标准，其对报文实时性、可靠性还有安全保密性的要求持续提高。不过传统公钥密码体制正遭遇量子计算发展带来的严峻挑战，IEC61850 通信链路在身份认证、密钥协商、数据加密等环节的量子威胁不容小觑。本文系统梳理 IEC61850 通信架构与安全机制，分析量子计算对现有密码模式的冲击，综述量子密钥分发（QKD）、量子随机数生成（QRNG）、后量子密码（PQC）等量子安全技术的原理与适用性，探讨其在变电站 IEC61850 各层通信中的应用模式、技术可行性与工程限制，并对部署成本、标准适配、运维集成等关键问题展开讨论，最后展望量子安全技术在电力二次系统中的应用前景。

［关键词］量子安全；IEC61850；变电站通信；量子密钥分发；后量子密码

智能变电站属于新型电力系统建设的关键环节，在其二次系统中普遍采用 IEC61850 标准来实现信息交互、功能集成。在“双碳”目标背景下，新能源大量接入、源网荷储协调互动需求增多，致使变电站通信网络规模和复杂程度不断增大，各类测量控制保护信息在站控层、间隔层与过程层之间频繁流转。且电力信息安全形势越来越严峻，网络攻击手法持续升级，IEC61850 所承载的 GOOSE、SV 等实时报文一旦被伪造或篡改，会直接对电网运行安全构成威胁。

1 变电站IEC61850通信系统安全需求分析

1.1 IEC61850 标准体系与通信架构概述

IEC61850 是由国际电工委员会所制定的用于变电站自动化系统的通信标准，它的核心理念是实现变电站内智能电子设备（IED）之间的互操作性、信息共享。此标准运用面向对象的数据建模方式，把变电站里的各类设备抽象成统一的信息模型，并借助抽象通信服务接口（ACSI）来屏蔽底层的通信差异。在物理架构方面，IEC61850 将变电站通信模式划分成站控层、间隔层、过程层这三层：站控层负责监控工作、进行远方通信，一般采用 MMS 报文借助 TCP/IP 以太网进行传输，间隔层负责保护、测控等职能，实现单元级信息处理，过程层通过 GOOSE 与 SV 报文完成开关量、采样值等实时信息的快速交换。其中，GOOSE 报文运用发布/订阅机制，SV 报文承载合并单元采样数据，二者都具备强实时性、周期性发送与广播组播的特点，对传输时延和抖动非常敏感，一般要求在数毫秒之内完成端到端传输。IEC61850 标准模式的建立提高了变电站信息交互的标准化程度和可靠性，为智能变电站的保护、控制、运维提供了统一的信息平台。

1.2 IEC61850 通信系统的安全威胁与脆弱性

IEC61850 标准提高了变电站通信的互操作性与效率，然而其在设计之初没有把信息安全放在核心位置，导致通信系统存在多个脆弱性。GOOSE 与 SV 报文一般采用明文传输且没有身份认证机制，攻击者能通过伪造或注入虚假报文来触发保护误动或拒动，形成严重运行风险。站控层 MMS 通信依靠 TCP/IP 协议栈，虽然能用传统网络安全手段防护，但缺少面向电力业务的轻量级认证与加密机制，容易遭受中间人攻击、重放攻击和拒绝服务攻击。变电站内 IED 设备数量多且型号杂，部分老旧设备不具备升级安全补丁的能力，形成难以统一管控的安全短板。在攻击路径上，既可从外部网络边界渗透，也可借助检修维护等运维环节植入恶意程序，威胁手段越来越多样化、隐蔽化。

2 量子安全关键技术及其原理

2.1 量子密钥分发（QKD）技术

量子密钥分发技术依据量子力学基本原理实现通信双方之间无条件安全的密钥协商，其安全性依靠量子不可克隆定理、测不准原理予以保证，并非建立在计算复杂度假设之上。以典型的 BB84 协议来说明，发送方会随机选取量子态编码密钥比特并通过量子信道进行传输，接收方测量之后双方借助

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

经典信道展开基矢比对与纠错操作，最终实现一致的密钥[1]。QKD 协议的安全性可由信息论意义上的量子密钥率加以度量，即密钥生成率 R 满足如下安全条件：

$$R \geq 1 - H_2(e)$$

其中，$H_2(e)$表示二进制熵函数，e 为量子误码率。在实际应用中，QKD 常常采用基于光纤信道的光子传输方案，这与变电站站内光纤通信网络有着天然的契合之处。

2.2 量子随机数生成（QRNG）技术

量子随机数生成技术借助量子物理过程固有的随机性来产生真随机序列，为密码系统提供高质量的随机源。与基于算法生成的伪随机数不同，QRNG 从单光子探测、真空涨落或者相位噪声等量子现象当中提取熵，其随机性来源于量子测量结果的本质不确定性，所以无法被任何经典算法预测或者重现。在变电站 IEC61850 通信系统里，QRNG 可以服务于多个关键环节：一方面用于生成密码算法所需要的种子密钥、一次性会话密钥，能够提高密钥熵质量，另一方面用于 QKD 协议的随机基矢选择、状态制备，保障量子密钥协商过程的安全性，再者用于身份认证中的随机挑战值生成，增强抗重放攻击的能力。

2.3 后量子密码（PQC）技术

后量子密码技术是一种能够抵御量子计算攻击，并且能够在经典硬件上运行的密码算法模式，它所追求的目标是在不借助量子信道的情况下给予长期的安全保障。现阶段主流的研究方向有好几大类，分别是基于格、基于哈希、基于编码、基于多变量等，其中基于格的密码体制由于拥有安全性与计算效率这两个优点而受到众多关注，它的安全性是建立在格上困难问题的基础上。与 QKD 相比，PQC 具备部署灵活、不需要专用量子信道和现有通信协议兼容性良好等优势，适合当作电力通信系统的渐进式升级途径[2]。不过 PQC 算法大多存在密钥尺寸大、签名体积大的情况，可能会给 IEC61850 里带宽与实时性受限的 GOOSE/SV 报文带来额外的开销，需要在安全强度和通信效率之间做出权衡。

3 量子安全技术在IEC61850通信中的应用模式分析

3.1 面向 GOOSE/SV 实时报文的轻量化安全设计

GOOSE 与 SV 报文肩负着变电站里最关键的保护和控制信息传输任务，具备强实时性、周期性发送、广播组播、小报文体积等特点。对安全机制的实时性要求非常严格，一般要求认证和完整性校验的额外处理时延控制在微秒至毫秒量级。这一特征决定了面向 GOOSE/SV 的安全设计要遵循轻量化原则，很难直接套用开销较大的公钥密码方案（见表 1）。在此背景下，可以优先考虑基于对称密钥的消息认证码（MAC）机制来实现报文完整性与来源认证，用极小的计算和带宽开销满足实时性要求，其认证密钥可以由 QKD 或者 PQC 协商的会话密钥提供[3]。针对 PQC 签名体积大的问题，应探索轻量级哈希签名或者短签名方案在 GOOSE/SV 场景中的适配性，并且结合报文分片、批量认证等手段降低传输开销。

表 1　GOOSE/SV 报文轻量化安全设计关键要求

安全需求维度	具体要求	设计约束
认证与完整性	报文来源可信、内容不被篡改	处理时延控制在微秒级
计算开销	附加处理量尽量小	适配 IED 算力有限现状
传输开销	签名/认证附加字节最小化	报文体积小、带宽受限
方案可扩展	支持报文批量与分片认证	兼顾周期性与突发性发送

3.2 面向 MMS 等管理报文的密钥管理体系

站控层 MMS 通信负责承载监控、调度、远程维护等管理信息，其传输时延要求不是特别严格，然而对于数据机密性、完整性还有身份认证方面有着较高要求，非常适合部署相对完备的密钥管理体系。能够借助 QKD 技术在站控层和远方调度端之间建立量子密钥信道，达成会话密钥的安全分发、定期更新，并且在此基础上融合传统 PKI 证书模式，建立“量子密钥+经典证书”的混合信任机制[4]。密钥管理要包括密钥生成、分发、存储、更新、撤销、审计等整个生命周期的各个环节，针对量子密钥的“用后即焚”特性来设计合理的密钥缓冲和预分配策略，以此来应对密钥消耗速率和网络波动的情况。

3.3 混合量子安全架构设计

QKD 和 PQC 在安全特性、工程适用性方面存在互补优势，因此适宜建立“QKD+PQC+QRNG”协同的混合量子安全架构，以此达成安全强度与部署可行性的统一。此架构采用分层分域的设计思路，在站控层与过程层等对安全等级和带宽约束要求不同的区域，分别实施差异化的防护策略，对于高安全

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

等级的调度关键链路引入 QKD 来提供信息安全保证，对于站内实时通信链路则运用经优化的 PQC、轻量级对称机制予以实用化防护[5]。混合架构非常重视与现有 IEC61850 安全规范的兼容、平滑演进，通过安全功能模块化封装、标准接口适配，实现量子安全组件的可插拔部署，减少对现有设备与协议模式的冲击。混合量子安全架构的建立，在量子计算威胁持续演进的状况下,能够为变电站 IEC61850 通信系统提供具备纵深防御能力的长期安全底座。

4 应用前景与关键问题分析

4.1 技术可行性分析

从技术方面来考量，量子安全技术在变电站 IEC 61850 通信系统里的部署有着一定的可行性。QKD 依靠光纤传输这一特性，和变电站站内光纤通信网络很契合，其密钥生成速率、误码率指标能够满足中低速率密钥需求的场景，PQC 算法在算力充足的站控层设备上运行不存在实质性能障碍，并且标准化进程持续进行，成熟算法具备工程落地条件，轻量级对称认证机制与 GOOSE/SV 的实时性要求基本相符。不过，QKD 在长距离光纤传输时受信道衰减影响较大，密钥成码率随距离增长迅速下降，限制了其在广域调度链路中的应用，PQC 的大密钥与大签名体积也需要在报文开销受限的场景中进一步优化[6]。

4.2 工程与成本约束

量子密钥分发设备有光源、探测与后处理模块，其单站成本相对较高，还要铺设专用量子信道，这给变电站空间和供电条件提出额外要求。变电站现场电磁干扰强、温度波动、振动等环境因素可能对量子设备稳定运行和单光子探测精度产生不利影响，需通过防护设计、环境适应测试来保障[7]。另外,量子安全系统运维需要专业密钥管理与设备维护能力，这对运维人员技能水平有更高要求，相关培训与人才储备成本不可忽视。在成本效益权衡时，应优先在枢纽变电站、重要调度节点等高安全需求场景试点，通过规模化应用逐渐摊薄成本，并结合国产化设备替代降低采购门槛，从而为量子安全技术推广创造经济可行性。

4.3 标准与产业化挑战

标准与产业化对量子安全技术的落地起着关键支撑作用，也是当前面临的一项主要挑战。一方面，现有的 IEC61850、IEC62351 安全标准还没有针对量子安全机制给出清晰的适配指引，QKD 接口、PQC 算法套件和现有安全协议的融合规则需要进一步明确，标准的滞后会限制设备互操作、规模化部署。另一方面，量子安全技术涉及的设备形态、密钥管理流程、安全评估方法等缺少统一的行业规范，相关的检测认证模式也在建设初期。在产业化方面，量子安全产业链处于成长阶段，QKD 设备成本、PQC 算法实现效率、国产化芯片适配等问题需要产业协同解决[8]。推动量子安全技术在电力行业的落地，标准组织、科研机构、设备厂商与电网企业要协同推进，加快标准制定和试点示范，形成从技术研发到工程应用的安全良性生态。

结论

IEC61850 通信系统在身份认证、密钥管理、数据保护等环节存在量子计算带来的长期安全威胁，而量子密钥分发、量子随机数生成、后量子密码等技术为应对这一挑战给出了可行路径。通过针对 GOOSE/SV 实时报文进行轻量化安全设计、建立面向 MMS 管理报文的密钥管理体系、搭建“QKD+PQC+QRNG”协同的混合量子安全架构，能够在保证实时性的前提下提高通信系统的抗量子攻击能力。

[参考文献]

[1]尹沛捷,胡晓娇,王羽飞,等. 通信技术与信息安全：挑战与应对策略[J].火控雷达技术,2026,55(3):23-28+43.

[2]安雪碧,马杉,郑玥,等. 量子安全 OTN 技术在大型体育赛事中的应用[J].通信与信息技术,2026,(5):138-142+152.

[3]滕晓辉. 基于量子点荧光编码的安全识别及验证技术[J].上海轻工业,2026,(5):190-192.

[4]李昕洪,盆海波,易杰宁,等. 抗量子安全在新型电力系统中的应用思考[J/OL].电力系统自动化,1-14[2026-10-13].

[5]张义,沈运,杨春旭. 量子通信技术在网络安全防御中的前瞻性应用研究[J].信息与电脑,2026,38(12):177-179.

[6]焦艳玲,刘学兵. 基于量子计算的新型加密技术在数据安全中的应用[J].中国新技术新产品,2026,(9):146-148.

[7]刘煜橦,陈琦,丁颜,等. 抗量子计算密码迁移的密码敏捷技术研究综述[J].网络空间安全科学学报,2026,4(2):100-114.

[8]郭朋朋. 计算机网络信息安全中数据加密技术的应用探析[J].软件,2026,47(3):171-173.

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.