Towards Quantum-Resistant Crypto-Agile Authentication, Authorization, and Accountability for Time-Critical Communication in IEC 61850 Digital Substations

Moritz Gstür*
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
moritz.gstuer@kit.edu

Abstract

Time-critical communication in digital substations forms the operational backbone of smart power grids while simultaneously representing an increasingly attractive target for cyberattacks. Existing communication security standards provide only limited support for emerging requirements, including post-quantum resilience, cryptographic agility, fine-grained authorization, and accountability without compromising the latency constraints of protection and control applications. The presented research investigates how these challenges can be addressed through a unified security architecture that enables secure, low-latency communication for both newly deployed and retrofitted legacy substations. The long-term objective of the dissertation is to establish a practical foundation for resilient and future-proof communication security that supports the gradual evolution of critical energy infrastructures toward the post-quantum era. The research follows the authentication, authorization, and accountability paradigm. Our preliminary work introduces a quantum-resistant crypto-agile authentication and encryption framework, and a server-aided attribute-based authorization framework. Experiments indicate that our preliminary work satisfies the transfer time constraints of IEC 61850, and does not disrupt the operation of industrial devices communicating via the protocols GOOSE and SV. Future research investigates the integration of authentication, authorization, and accountability into a unified security architecture for future digital substations.

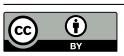
CCS Concepts

• **Security and privacy** → **Authentication**; **Authorization**; **Access control**; **Distributed systems security**; **Security protocols**; **Firewalls**; *Domain-specific security and privacy architectures*; Economics of security and privacy; • **Networks** → *Middle boxes / network appliances*; *Cyber-physical networks.*

Keywords

Authentication, Authorization, Accountability, Access Control, Smart Grid, Digital Substation, Low-Latency Communication, Bump-in-the-Wire, IEC 61850, IEC 62351

*PhD Advisor: Prof. Dr. Veit Hagenmeyer (veit.hagenmeyer@kit.edu), Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany.



This work is licensed under a Creative Commons Attribution 4.0 International License.
CCS '26, The Hague, Netherlands
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3846930

ACM Reference Format:
Moritz Gstür. 2026. Towards Quantum-Resistant Crypto-Agile Authentication, Authorization, and Accountability for Time-Critical Communication in IEC 61850 Digital Substations. In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26), November 15–19, 2026, The Hague, Netherlands.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3830454.3846930

1 Introduction & Research Directions

Modern operational technology (OT) increasingly relies on information and communication technology (ICT) for monitoring and control, blurring the boundary with information technology (IT) while retaining OT's focus on availability and reliability [21]. In the energy sector, this convergence coincides with the transformation towards smart grids with bidirectional energy and data flows [7, 9]. Historical evidence, including incidents such as Stuxnet [8] and Industroyer/CrashOverride [4], demonstrates that energy-related OT and thus the regional and global energy supply are endangered by capable and motivated adversaries [3]. Our project focuses on digital substations, whose communication protocols are standardized by IEC 61850 [14]. The complementary IEC 62351 series [15, 16] offers only limited support for post-quantum resilience, cryptographic agility, fine-grained authorization, and accountability. To bridge this gap, the presented research follows the authentication, authorization, and accountability (AAA) paradigm, unifying quantum-resistant crypto-agile authentication, expressive and fine-grained authorization, and non-repudiable accountability into a secure physical and communication architecture for newly deployed and legacy digital substations. To protect digital substations against today's adversaries as well as future quantum adversaries while taking the strict constraints of IEC 61850 into account, the dissertation is concerned with the following central research directions and questions.

1.1 Quantum-Resistant Crypto-Agile Authentication

OT is vulnerable to the adversarial misuse of a cryptographically relevant quantum computer (CRQC) [22] due to its criticality, increasing connectivity, legacy devices, and limited computational capabilities [5, 18]. In particular, public-key cryptography and thus traditional key agreement protocols relying on the hardness of the integer factorization problem, discrete logarithm problem, and elliptic curve discrete logarithm problem are endangered by CRQCs, as quantum algorithms exist to solve these problems efficiently [1, 2, 5]. Furthermore, this threat is amplified by "harvest now, decrypt later"

attacks, and by substations' exceptionally long operational lifecycles of up to 40 years [17], during which deployed cryptography must remain secure or has to be replaced.

RQ 1.a: How can computationally expensive quantum-resistant authentication and authenticated encryption be deployed to secure low-latency, jitter-sensitive communication of digital substations?

RQ 1.b: Which quantum-resistant cryptographic paradigms, i.e., symmetric, asymmetric, or hybrid, fit the requirements of a digital substation best?

RQ 1.c: How can authentication and authenticated encryption mechanisms allow for agility, interoperability, and retrofitting of heterogeneous substation environments, including heterogeneous protocols, devices, architectures, and stakeholders?

1.2 Expressive & Fine-Grained Authorization & Access Control

The transformation from traditional top-down energy transmission and distribution systems to smart grids increases the number and heterogeneity of devices and stakeholders – including grid operators, energy suppliers, and prosumers alongside utility personnel – involved in a substation's operation [7, 10, 23]. The coarse-grained and static role-based access control (RBAC) mandated by IEC 62351-8 [16] is not expressive enough for this dynamic, heterogeneous, and distributed environment, motivating attribute-based access control (ABAC), which subsumes RBAC and enables more fine-grained access policies [13].

RQ 2.a: How can expressive and flexible yet computationally expensive access control policies be evaluated and enforced in a delay- and jitter-sensitive substation environment, to prevent unauthorized access, enable the separation of duties (SoD), and ensure the principle of least privilege (PoLP)?

RQ 2.b: How can time-dependent system attributes be integrated into the evaluation and enforcement process of access control policies?

RQ 2.c: Does a substation benefit from considering time-dependent system attributes in its authorization and access control processes, and what are the use cases in which the substation benefits the most by considering them?

1.3 Non-Repudiable Accountability

As the third AAA pillar, accountability enables the recording and tracing of security-relevant events [19]. Comprehensive accounting information allows operators to retroactively reconstruct and learn from an attack, and supports proactive intrusion detection and prevention by revealing anomalous behavior before or during an attack. However, existing accountability approaches for smart grids are rarely integrated with authentication and authorization or tailored to substation time constraints [20].

RQ 3.a: How can non-repudiable accountability be retrofitted in a delay- and jitter-sensitive substation environment?

RQ 3.b: Does the aggregation of entries and metrics of sampling-based substation protocols endanger non-repudiation?

RQ 3.c: Does accountability facilitate anomaly detection and substation management?

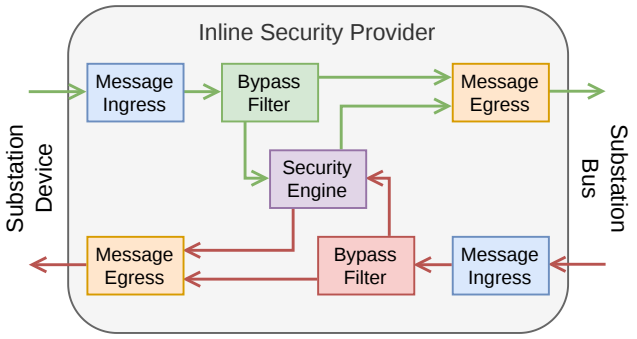


Figure 1: Internal architecture of bump-in-the-wire security provider with bypass filtering.

2 Research Approach & Preliminary Work

The provisioning of AAA in a newly constructed or legacy substation is possible by deploying newly developed substation devices or by updating their implementations. However, neither of these strategies can be realized within weeks, months, or even years, due to necessary research and development, standardization, and deployment. To bridge this gap, our approach provides AAA for any communication between substation devices using a bump-in-the-wire or inline concept. Thus, the security-related services are provided automatically and invisibly to substation devices, enabling short-term deployment via retrofitting. While different parts of AAA may depend upon different infrastructure, including servers for server-aided operations, a central characteristic of our approach is an inline standalone device based on off-the-shelf hardware acting as a core unit providing security to substation devices. For this purpose, an inline security provider intercepts and secures the data link layer communication of a substation device. The internal architecture of an inline security provider is shown in Figure 1. To safeguard the compatibility of our approach with partially incompatible substation environments, e.g., network management protocols or protocols that are susceptible to temporal inconsistencies, the inline security providers allow for selective network traffic bypassing. In summary, contrary to traditional cybersecurity approaches implemented within substation devices, our approach is designed for deployment without time-consuming procurement or firmware changes, is agile with regard to technological and adversarial advancements, and avoids the cost of replacing substation equipment.

Our preliminary work comprises two independent but architecturally compatible security mechanisms thus far. Firstly, our quantum-resistant crypto-agile inline authentication and encryption approach called QIRA provides a lightweight communication protocol based on a hybrid cryptosystem to enable in-flight authentication and encryption of network data frames [12]. Secondly, our real-time server-aided attribute-based authorization and access control approach called RTS-ABAC provides an attribute-based authorization protocol as well as a protocol for access control decision enforcement [11]. Both approaches utilize an inline security provider, are crypto-agile by being scheme-agnostic, and allow for selective network traffic bypassing.

3 Planned Evaluation & Preliminary Results

We plan to provide formal security proofs using state-of-the-art verification tools as well as informal security analyses including the mitigation of adversarial attacks in laboratory-based experiments. Furthermore, we aim to provide reproducible benchmarks that statistically confirm the performance claims of our research. To demonstrate the compatibility with industrial digital substation hardware, we plan to conduct an experimental demonstration of applicability using intelligent electronic devices, merging units, and I/O-boxes by General Electric, Siemens, SEL, and Hitachi ABB in our laboratory, the KASTEL Security Lab Energy [6].

Our preliminary evaluations using inexpensive off-the-shelf hardware for the inline security providers show that the quantum-resistant authentication and authenticated encryption of QIRA lead to a unidirectional transfer time increase of 0.83 ms on average, using ML-KEM for key encapsulation and HMAC-SHA256, AES-256-GMAC/GCM/CCM, and ChaCha20-Poly1305 for data encapsulation [12]. The utilization of access control provided by RTS-ABAC leads to a transfer time increase of 0.78 ms on average [11]. Thus, the data indicate that an integrated authentication, authorization, and access control approach is able to satisfy the 3 ms transfer time constraint of the IEC 61850-5 [14] protocols GOOSE and SV. Furthermore, during laboratory-based experiments, neither QIRA nor RTS-ABAC disrupts the operation of industrial substation devices communicating via GOOSE and SV [11, 12].

4 Conclusions & Outlook

The presented research aims to enable the evolution of IEC 61850 digital substations toward the post-quantum era by providing future-proof quantum-resistant crypto-agile authentication, fine-grained attribute-based authorization, and accountability. Due to its retrofitting-capable bump-in-the-wire architecture, the presented approach enables the deployment of authentication, authorization, and accountability in both newly constructed and legacy digital substations. Preliminary analyses using industrial substation devices indicate the compatibility of the presented approach with the time-critical IEC 61850 protocols GOOSE and SV. Further research is required to design an accountability mechanism capable of meeting the requirements and constraints of substation communication, as well as integrating authentication, authorization, and accountability into a unified security solution. Moreover, further research has to formally prove the security characteristics, harden the presented approach against different cyberattacks, and evaluate its applicability for other time-critical systems with similar requirements.

Acknowledgments

This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).

References

[1] Abdullah Aydeger, Engin Zeydan, Awaneesh Kumar Yadav, Kasun T. Hemachandra, and Madhusanka Liyanage. 2024. Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. In *2024 15th International Conference on Network of the Future (NoF)*. IEEE, 195–203. doi:10.1109/nof62948.2024.10741441

[2] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. 2016. *Report on Post-Quantum Cryptography.* Technical Report. National Institute of Standards and Technology. doi:10.6028/NIST.IR.8105

[3] Communications Security Establishment Canada. 2021. *Cyber threat bulletin: Cyber threat to operational technology.* Retrieved March 15, 2026 from https://open.canada.ca/data/dataset/98bad300-28f1-49b9-9b34-2d46de4c9a58

[4] Cybersecurity and Infrastructure Security Agency (CISA). 2021. *CrashOverride Malware.* Retrieved March 15, 2026 from https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware

[5] Cybersecurity and Infrastructure Security Agency (CISA). 2024. *Post-Quantum Considerations for Operational Technology.* Technical Report. https://www.cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology

[6] Ghada Elbez, Gustavo Sánchez, Sine Canbolat, Sophie Corallo, Clemens Fruböse, Florian Lanzinger, Nicolai Kellerer, Gustav Keppler, Felix Neumeister, Bernhard Beckert, Anne Koziolek, Martina Zitterbart, and Veit Hagenmeyer. 2025. Insights and Lessons Learned from a Realistic Smart Grid Testbed for Cybersecurity Research. In *Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems (E-Energy '25)*. ACM, 805–812. doi:10.1145/3679240.3734649

[7] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. 2012. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials* 14, 4 (2012), 944–980. doi:10.1109/surv.2011.101911.00087

[8] Jonathan Fildes. 2010. *Stuxnet worm targeted high-value Iranian assets.* Retrieved March 15, 2026 from https://www.bbc.com/news/technology-11388018

[9] C.W. Gellings, M. Samotyj, and B. Howe. 2004. The future's smart delivery system. *IEEE Power and Energy Magazine* 2, 5 (Sept. 2004), 40–48. doi:10.1109/mpae.2004.1338121

[10] Avi Gopstein, Cuong Nguyen, Cheyney O'Fallon, Nelson Hastings, and David A. Wollman. 2021. *NIST Framework and Roadmap for Smart Grid Interoperability Standards.* Technical Report NIST Special Publication 1108r4. National Institute of Standards and Technology. doi:10.6028/NIST.SP.1108r4

[11] Moritz Gstür, Gustav Keppler, Mohammed Ramadan, Ghada Elbez, and Veit Hagenmeyer. 2026. RTS-ABAC: Real-Time Server-Aided Attribute-Based Authorization & Access Control for Substation Automation Systems. arXiv:2603.23012 [cs.CR] doi:10.48550/arXiv.2603.23012

[12] Moritz Gstür, Mohammed Ramadan, and Veit Hagenmeyer. 2026. Quantum-Resistant Crypto-Agile Inline Authentication and Encryption Framework for IEC 61850 Digital Substations. In *Proceedings of the 2026 ACM Sustainability Week (ACM Sustainability Week '26)*. ACM, 1–8. doi:10.1145/3765611.3815134

[13] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. 2014. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* Technical Report NIST Special Publication 800-162. National Institute of Standards and Technology. doi:10.6028/nist.sp.800-162

[14] International Electrotechnical Commission. 2014. Part 5: Communication requirements for functions and device models. *Communication networks and systems for power utility automation (IEC 61850)* (2014).

[15] International Electrotechnical Commission. 2020. Part 6: Security for IEC 61850. *Power systems management and associated information exchange - Data and communications security (IEC 62351)* (2020).

[16] International Electrotechnical Commission. 2020. Part 8: Role-based access control for power system management. *Power systems management and associated information exchange - Data and communications security (IEC 62351)* (2020).

[17] Mick Mackey. 2018. Asset Management of Secondary Systems of Substations. In *Substations.* Springer, Cham, 845–897. doi:10.1007/978-3-319-49574-3_38

[18] Javier Oliva del Moral, Antonio deMarti iOlius, Gerard Vidal, Pedro M. Crespo, and Josu Etxezarreta Martinez. 2024. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. *IEEE Internet of Things Journal* 11, 18 (Sept. 2024), 30217–30244. doi:10.1109/jiot.2024.3410702

[19] Robert W. Shirey. 2007. Internet Security Glossary, Version 2. RFC 4949. doi:10.17487/RFC4949

[20] Arthur A. Z. Soares, Yona Lopes, Diego Passos, Natalia C. Fernandes, and Debora C. Muchaluat-Saade. 2021. 3AS: Authentication, Authorization, and Accountability for SDN-Based Smart Grids. *IEEE Access* 9 (2021), 88621–88640. doi:10.1109/access.2021.3090346

[21] Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. 2023. *Guide to Operational Technology (OT) Security.* Technical Report NIST Special Publication 800-82, Rev.3. National Institute of Standards and Technology. doi:10.6028/nist.sp.800-82r3

[22] Frank K. Wilhelm, Rainer Steinwandt, Paul Lageyre, and Susanna Kirchhoff. 2025. *Status of quantum computer development V2.2.* Technical Report. Federal Office for Information Security (BSI). https://www.bsi.bund.de/dok/study_status_quantum_computer

[23] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. 2012. A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials* 14, 4 (2012), 998–1010. doi:10.1109/surv.2012.010912.00035