Karlsruhe Institute of Technology

Institute for Automation and Applied Informatics (IAI)
Secure Energy Systems Group (SES)

Towards Quantum-Resistant Crypto-Agile AAA for Time-Critical Communication in Digital Substations

ACM CCS '26 Doctoral Symposium, The Hague, Netherlands

Moritz Gstür

Motivation

Smart Grids in the Quantum Era

Constrained
3 ms
IEC 61850-5 transfer-time limit

Long-Lived
40 yrs
Substation lifecycle

Proven Target
HNDL
Harvest now, decrypt later

Converging
IT & OT
New devices & stakeholders

Consequence: Quantum-resistant crypto-agile cybersecurity for IEC 61850 digital substations is needed today

Research Gap

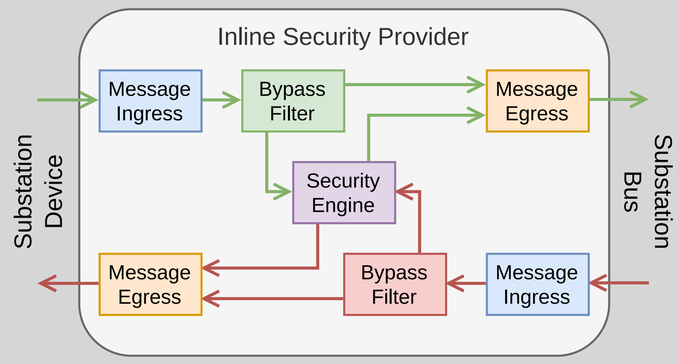
IEC 62351 Falls Short

Requirement	IEC 62351	This Work
Integrity & Authenticity	✓	✓
Quantum Resistance	✗	✓
Crypto-Agility	✗	✓
Fine-Grained Authorization	✗	✓
Accountability	✗	✓
Retrofittable to Legacy	✗	✓

Security Inheritance: AAA is only as secure as its weakest part
⇒ Solve all three pillars together

Approach

Retrofittable Endpoint-Agnostic Bump-in-the-Wire Security Provider



Research Directions – Authentication · Authorization · Accountability

RQ1 Authentication

QIRA
Quantum-Resistant Inline Retrofittable Authentication & Authenticated Encryption

Published · ACM Sustainability Week '26 [1]

1.a Architecture: How can costly quantum-resistant authentication and encryption secure low-latency, jitter-sensitive communication?

1.b Paradigms: Which quantum-resistant paradigm (symmetric, asymmetric, or hybrid) fits substations best?

1.c Compliance: How can these mechanisms enable agility, interoperability, and retrofitting in heterogeneous substations?

+ 0.83 ms Avg. transfer-time increase

RQ2 Authorization

RTS-ABAC
Real-Time Server-Aided Attribute-Based Authorization & Access Control

Preprint · arXiv:2603.23012 [2]

2.a Architecture: How can expressive yet costly access control policies be evaluated and enforced under delay and jitter constraints?

2.b Strategies: How can time-dependent system attributes be integrated into policy evaluation and enforcement?

2.c Benefit: Does a substation benefit from time-dependent attributes, and in which use cases the most?

+ 0.78 ms Avg. transfer-time increase

RQ3 Accountability

RIPA (Concept)
Retrofittable Inline Pattern-Based Accounting

Planned · Next Research Phase

3.a Architecture: How can non-repudiable accountability be retrofitted under delay and jitter constraints?

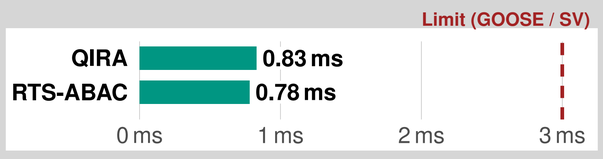
3.b Threat to Validity: Does aggregating entries and metrics of sampling-based protocols endanger non-repudiation?

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

TBD Avg. transfer-time increase

Evaluation

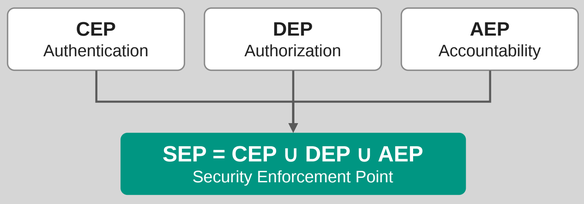
Well Inside the 3 ms Budget



- **Hypothesis:** Integrated AAA can meet the 3 ms limit
- **Applicability:** Lab experiments with industrial substation devices (GE, Siemens, SEL, Hitachi ABB)
  ⇒ No disruption of GOOSE & SV communication!

Towards Unified AAA

One Security Enforcement Point



- **Idea:** Merge bump-in-the-wire enforcement points
- **Goal:** min(components) + min(messages)
- **Pitfall:** Tight coupling endangers system evolution

Outlook

From Prototype to AAA Product

- Unified AAA security solution
- Formal security proofs
- Attack mitigation in lab experiments
- Transfer to other time-critical systems

Status

RQ1	RQ2	RQ3
Almost Fully Answered	Almost Fully Answered	Next Phase

Moritz Gstür – moritz.gstuer@kit.edu
PhD Advisor: Prof. Dr. Veit Hagenmeyer
https://www.iai.kit.edu/english/groups_4106.php
Paper: doi.org/10.1145/3830454.3846930

References
[1] M. Gstür, M. Ramadan, V. Hagenmeyer. Quantum-Resistant Crypto-Agile Inline Authentication and Encryption Framework for IEC 61850 Digital Substations. In: *ACM Sustainability Week '26*, 2026. doi:10.1145/3765611.3815134
[2] M. Gstür, G. Keppler, M. Ramadan, G. Elbez, V. Hagenmeyer. RTS-ABAC: Real-Time Server-Aided Attribute-Based Authorization & Access Control for Substation Automation Systems. arXiv:2603.23012, 2026.

Acknowledgments
Supported by the Helmholtz Association (HGF), topic Engineering Secure Systems, and by KASTEL Security Research Labs (structure 46.23.02).