PS-CAMM: A Crypto-Agility Maturity Model for Real-Time Substation Automation

Sunwoo Lee, Woo-Hyun Choi, Hyuk Lim, and Seunghyun Yoon
Korea Institute of Energy Technology (KENTECH)
Naju, Republic of Korea
Email: {sunwoolee, woohyunchoi, hlim, syoon}@kentech.ac.kr

***Abstract*—Quantum computing challenges the long-term viability of widely deployed public-key cryptography and motivates crypto-agility, the ability to migrate cryptographic algorithms in a timely and controlled manner. However, existing crypto-agility maturity models such as CAMM and FS-ISAC are largely shaped by IT assumptions and do not directly capture the operational constraints of substation automation, where protection messaging must meet hard real-time bounds, many devices are firmware-locked, and redundancy protocols require coordinated dual-network operation. This paper presents PS-CAMM (Power Systems Crypto-Agility Maturity Model), an OT-oriented extension of CAMM that (i) gates maturity advancement on quantitative real-time KPIs, (ii) requires hardware-in-the-loop (HIL) evidence to validate safety during migration, and (iii) specifies PRP/HSR-aware operational procedures for cutover and rollback. We also outline an optional AI-assisted assessment component that supports evidence collection and consistency checking from documents and test logs, while keeping final maturity determination criteria-based and auditable.**

***Index Terms*—Crypto-agility, IEC 61850, Post-quantum cryptography, PRP/HSR, Substation automation**

I. Introduction

The advent of quantum computing challenges the security assumptions of widely deployed public-key cryptography and motivates crypto-agility: timely, controlled migration of cryptographic algorithms. While NIST's Post-Quantum Cryptography (PQC) standardization provides candidate algorithms, practical migration in operational-technology (OT) environments remains constrained by timing-critical operation and limited device flexibility.

Substation automation systems illustrate these constraints clearly. Protection messaging such as IEC 61850 GOOSE is subject to strict end-to-end latency requirements (e.g., 3 ms for Type-1A), and many Intelligent Electronic Devices (IEDs) are firmware-locked with restricted update paths. In addition, redundancy protocols such as PRP/HSR require coordinated operation across dual networks during cutover and rollback. Existing crypto-agility maturity models (e.g., CAMM [1] and FS-ISAC [2]) provide useful high-level guidance, but they do not explicitly encode these OT-specific constraints as auditable advancement criteria.

In this paper, we present **PS-CAMM** (Power Systems Crypto-Agility Maturity Model), an OT-oriented maturity model for substation systems. PS-CAMM makes level advancement conditional on quantitative real-time KPIs, requires hardware-in-the-loop (HIL) test evidence for safety validation, and specifies operational procedures for redundancy-aware transition in PRP/HSR environments. By incorporating firmware constraints and IEC 61850/62351 compliance considerations, PS-CAMM provides a practical basis for assessing and planning crypto-agility in substation automation under real-time and resource constraints.

II. Background, Gap Analysis, and OT Constraints

This section reviews prior crypto-agility maturity models and highlights why their criteria do not directly transfer to substation automation. We summarize the relevant gaps and the OT constraints that motivate PS-CAMM.

A. Existing Crypto-Agility Maturity Models

Hohm et al. [1] proposed CAMM, a five-level maturity model (L0–L4) in which a system's level is determined by strict satisfaction of all requirements up to that level. Alnahawi et al. [3] surveyed crypto-agility across multiple dimensions, including algorithms, hardware, APIs, and quality management, and discussed practical challenges such as composability and migration modalities. FS-ISAC [2] provides an operational view of migration through phases such as inventory, testing, cutover, and post-change verification, emphasizing process discipline at the organizational level.

These frameworks establish useful baseline principles, but they are largely shaped by IT deployment assumptions. In particular, their criteria are typically qualitative and do not explicitly encode tail-latency requirements or jitter tolerance under time-critical messaging. They also provide limited guidance for environments where devices are firmware-locked or resource constrained, and where verification must rely on OT test infrastructure (e.g., hardware-in-the-loop validation) rather than software-only test suites. Finally, they do not directly address redundancy-aware orchestration during migration, such as coordinated cutover and rollback across dual networks, nor time-synchronization considerations that affect measurement and scheduling in substations.

B. PS-CAMM's OT-Specific Extensions

PS-CAMM follows the same general approach as prior maturity models—deriving requirements from published guidance and expert practice—but tailors the assessment to substation automation constraints. Specifically, PS-CAMM (i) makes

level advancement conditional on quantitative, standards-aligned real-time KPIs, (ii) treats hardware-in-the-loop (HIL) results and regression evidence as mandatory verification artifacts, and (iii) specifies operational procedures for redundancy-aware transition, including coordinated cutover, rollover, and rollback under PRP/HSR. These extensions are intended to capture practical conditions in substations where protection messaging operates under hard time bounds, devices may have restricted update paths, and cryptographic transitions must remain consistent across redundant paths.

III. Proposed Maturity Model: PS-CAMM

This section describes PS-CAMM and the assessment logic used for level advancement. We summarize the substation constraints that drive the model, then present level requirements, KPI gates, and the associated verification evidence.

A. Substation Automation Constraints

Substation automation operates under constraints that are not explicitly captured by IT-oriented maturity models. Protection messaging on IEC 61850, particularly Type-1A GOOSE, is subject to a tight end-to-end latency bound on the order of a few milliseconds [4]. In addition, time synchronization via IEEE 1588 PTP is commonly required at sub-microsecond accuracy [5], and cryptographic transition must not degrade timing stability or introduce harmful jitter.

For protection behavior, average latency is not a sufficient indicator. Rare tail events can violate the protection time budget and lead to misoperation during fault conditions, even when the mean remains stable. Accordingly, PS-CAMM uses p_{95} and p_{99} end-to-end GOOSE latency as primary real-time KPIs, computed over fixed measurement windows with hardware timestamps. These percentiles characterize typical worst-case behavior (p_{95}) and extreme delay events (p_{99}) that are most relevant during cutover.

Substations also impose practical deployment constraints. IEDs are often firmware-locked and resource constrained, which limits update paths and the ability to accommodate large PQC key material. Hardware acceleration support for lattice-based cryptography may be limited or absent [6]. Finally, redundancy protocols such as PRP/HSR require coordinated operation across dual networks during migration, including consistent key management and standards-compliant negotiation under IEC 62351, as well as operational readiness for scenarios such as black-start and islanded operation [7].

B. PS-CAMM Structure and Assessment Dimensions

Figure 1 summarizes PS-CAMM's level advancement logic, and Table I enumerates the corresponding requirements and evidence expected at each level. PS-CAMM assesses crypto-agility along four dimensions: (i) *Technical/Architecture* (e.g., algorithm modularity and PQC deployment options), (ii) *Operations/Governance* (e.g., policies, roles, and change control), (iii) *Real-time/KPI* (quantitative performance bounds), and (iv) *Verification Evidence* (mandatory test artifacts and documentation). Based on these dimensions, PS-CAMM defines five maturity levels:

- **L0 (Initial):** Hard-coded algorithms with no update mechanism and no crypto asset management.
- **L1 (Possible):** Basic enablement through updatability, versioned configurations, and baseline performance measurement.
- **L2 (Prepared):** Hybrid design with PQC applied to control and key-management planes, formalized policies, and predefined acceptance bounds $(\delta_{95}, \delta_{99}, \epsilon)$.
- **L3 (Practiced):** Operational transition supported by KPI validation, HIL evidence of zero protection misoperations, and redundancy-aware dual-path operation under PRP/HSR.
- **L4 (Sophisticated):** Policy-driven automation with PTP-aware scheduling, cross-vendor interoperability, and sustained p_{99} non-inferiority within planned cutover windows.

Table I also sketches an optional AI-assisted assessment component (non-scoring). This component supports evidence collection and consistency checks. Examples include SCD/SSD–Crypto-BOM alignment (SCD/SSD: System Configuration Description / Substation Specification Description; Crypto-BOM: Cryptographic Bill of Materials), policy compliance extraction, KPI trend monitoring, and log-based evidence retrieval. Final maturity determination remains criteria-based and human-auditable.

C. KPI-Gated Advancement

Levels 0–2 establish the organizational and architectural prerequisites for migration. Level 3 introduces quantitative gates that must be satisfied during cutover:

$$\mathrm{GOOSE}_{\mathrm{E2E}} \le 3\,\mathrm{ms}, \quad \Delta p_{95} \le \delta_{95}, \quad \Delta p_{99} \le \delta_{99}, \quad \mathrm{loss} \le \epsilon.$$

Here, Δp_{95} and Δp_{99} denote the change in end-to-end GOOSE latency percentiles relative to the pre-cutover baseline. The bounds $(\delta_{95}, \delta_{99}, \epsilon)$ are defined at Level 2 and are used for one-sided non-inferiority checks. Level 4 requires sustaining these gates within planned cutover windows under cross-vendor interoperability conditions. The gates are chosen to preserve protection semantics and are grounded in the relevant timing and redundancy requirements in IEC 61850-5, IEEE 1588, and IEC 62439-3.

D. Illustrative Assessment

We illustrate PS-CAMM with a digital substation testbed that includes firmware-locked IEDs and PRP redundancy. At Level 1, the operator establishes a crypto asset inventory and measures baseline GOOSE latency percentiles (p_{95}, p_{99}). At Level 2, the system adopts a hybrid design that applies PQC to control and key-management planes, defines the acceptance bounds $(\delta_{95}, \delta_{99}, \epsilon)$, and approves a test plan. At Level 3, the operator validates that the end-to-end GOOSE bound is met, the p_{95}/p_{99} percentiles satisfy the non-inferiority checks, HIL testing shows no protection misoperations, and PRP and PTP remain stable during the cutover window. If the required artifacts and logs support these checks, the system qualifies for Level 3.

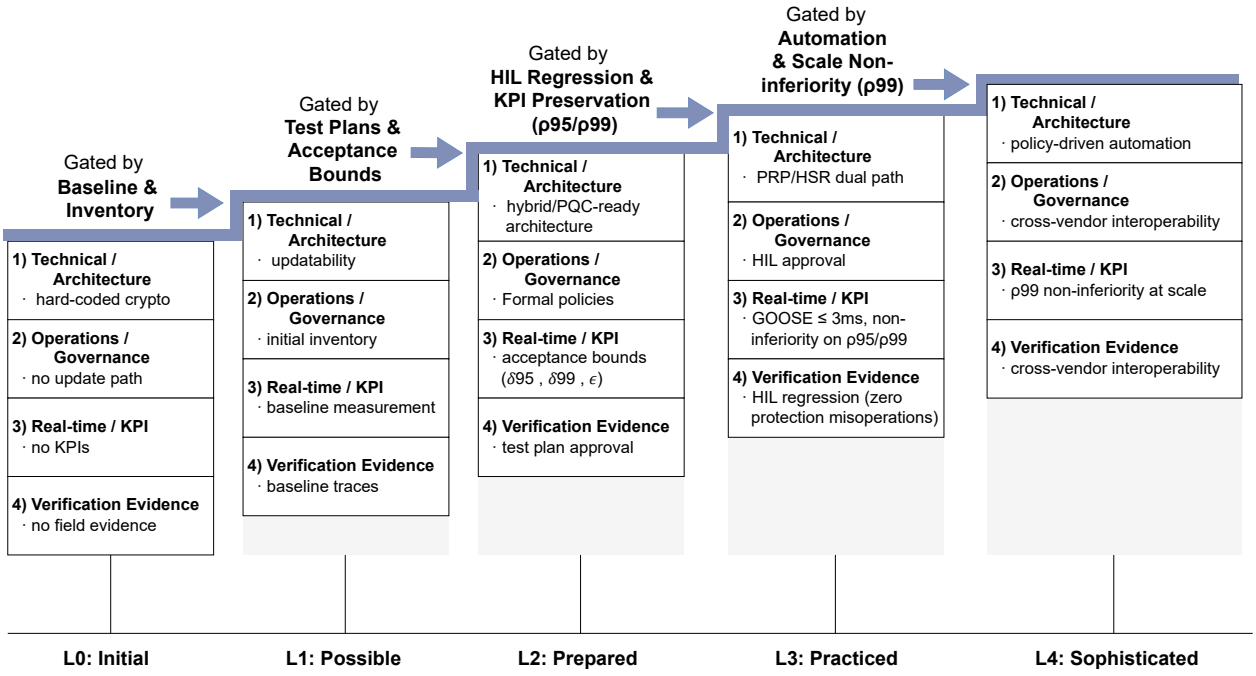

Fig. 1. PS-CAMM Level Advancement Based on KPI Satisfaction and Verification Evidence

IV. Evaluation Methodology and Process Mapping

A. Scoring and Assessment

PS-CAMM follows CAMM's strict advancement rule. A system attains level X only when it satisfies all requirements from Levels 0 through X. In practice, assessment combines document review, architecture inspection, performance measurement, test-log analysis, and operational drills to verify that the required KPI gates and evidence are met. Table I sketches an optional AI-assisted component that can support evidence collection and consistency checks. Final level assignment remains criteria-based and auditable, relying on the KPI inequalities and the relevant normative requirements.

B. Mapping FS-ISAC Ten Phases to OT Operational Windows

Figure 2 summarizes the cryptographic transition workflow used in PS-CAMM. The workflow is adapted from FS-ISAC [2] and adds OT-specific safety gates and rollback considerations for substation operation.

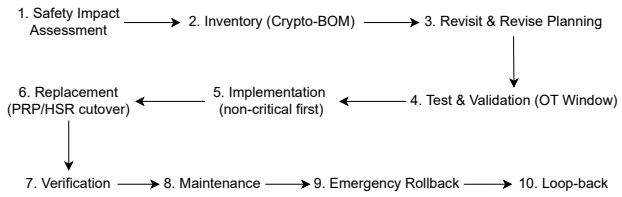

Fig. 2. PS-CAMM workflow for substation migration

The workflow consists of ten phases grouped into planning, deployment, and maintenance. Planning covers safety impact assessment (Phase 1), Crypto-BOM inventory of algorithms and device capabilities (Phase 2), and schedule revision driven by vendor and operational constraints (Phase 3). Deployment requires HIL verification without regression (Phase 4), staged rollout (Phase 5), redundancy-aware dual-network rollover under PRP/HSR (Phase 6), and post-cutover validation against the real-time KPI gates (Phase 7). Maintenance monitors cryptographic health and certificate lifecycle (Phase 8), supports coordinated emergency rollback across redundant paths (Phase 9), and feeds operational findings back into the planning process (Phase 10).

V. Conclusion

This paper presented PS-CAMM, an OT-oriented crypto-agility maturity model for substation automation. PS-CAMM extends CAMM by introducing quantitative real-time KPI gates, requiring HIL-based verification evidence, and specifying redundancy-aware operational procedures for migration. These elements are intended to make maturity assessment actionable and auditable under substation constraints and standards. Future work includes pilot studies and implementation of supporting tools for Crypto-BOM consistency checking and evidence collection.

Acknowledgment

This work was partially supported by the Korea Evaluation Institute of Industrial Technology (KEIT) grant funded by the Korean government (MOTIR) (RS-2025-02634277, "Development of Human-AI Teaming-based Autonomous Security

TABLE I

PS-CAMM: Level-by-level checklist of OT crypto-agility requirements, real-time KPIs, and verification evidence

Level	Technical / Architecture	Operations / Governance	Real-time / KPI	Verification Evidence
L0 Initial	• Hard-coded algorithms; no update path • No algorithm ID / negotiation • Vendor lock-in; no key/cert lifecycle	• No crypto asset inventory or roles • No change management or vendor oversight	• No measurement baseline	• Known Answer Test (KAT)/compile logs only; no field data
L1 Possible	• Updatability, rollback, inventory established • Versioned keysets/configs; manual switchover	• Initial policy; crypto officer assigned • Asset scanning; initial inventory	• Baseline latency/throughput (testbed) • E2E instrumentation for GOOSE fast path	• Inventory report; baseline traces
L2 Prepared	• Modularity; hybrid/parallel design • Cipher-suite intersection; policy-driven partial automation • PQC on control & key mgmt (IEC 62351-3/9)	• Formal policies; mandatory inventory workflow • Third-party risk templates; dedicated team	• Acceptance bounds set: $\delta_{95}, \delta_{99}, \epsilon$ • Cutover window and Service Level Objectives (SLOs) defined	• Approved test plan and checklists • Supplier compliance artifacts
L3 Practiced	• Transition mechanisms operational; PRP/HSR dual path • Backward compatibility; HW modularity	• Training/drills; transparent change control • HIL/field sampling approval gates	• GOOSE E2E ≤ 3 ms; one-sided non-inferiority on p_{95}/p_{99} • Loss $\leq \epsilon$; jitter within bounds during cutover	• Before/after regression reports • HIL results (zero protection misoperations) • PRP duplicate-discard & sequence-gap logs • PTP offset/PDV time series within spec
L4 Sophisticated	• Policy-driven automation; PTP-aware scheduler • Cross-vendor interoperability at scale • Fast-path GOOSE/SV unchanged (IEC 62351-6)	• Continuous monitoring and audit • Rapid response to threat/standard changes • Black-start and islanded procedures embedded	• p_{99} non-inferiority in planned windows • Loss $\leq \epsilon$; zero protection misoperations	• Interop pass rate; seamless rollover demos • SCD/SSD–Crypto-BOM alignment audit trail
Future (non-scoring) AI assistance for assessment automation				
AI assist	• SCD/SSD–Crypto-BOM consistency checks • Algorithm/cipher-suite compatibility	• Policy compliance extraction and scoring • Supplier certification summarization	• KPI trend analysis; regression detection	• Evidence extraction from HIL/field logs • zero protection misoperations verification

Notes: p_{95}/p_{99} are computed over fixed windows using hardware timestamps; $(\delta_{95}, \delta_{99})$ and ϵ bound non-inferiority and loss, respectively. *Abbreviations:* SV = Sampled Values, PDV = Packet Delay Variation.

System for Future Cyber Threats") and by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (RS-2025-25457382, "Development of Operation and Deployment Technologies for Korean AI SoC based Micro Data Centers").

References

[1] J. Hohm, A. Heinemann, and A. Wiesmaier, "Towards a Maturity Model for Crypto-Agility Assessment," in *Proc. Int. Symp. Foundations and Practice of Security*. Springer, 2022, pp. 104–119.

[2] FS-ISAC, "Building Cryptographic Agility in the Financial Sector," Financial Services Information Sharing and Analysis Center, White Paper, May 2022.

[3] N. Alnahawi, N. Schmitt, A. Wiesmaier, A. Heinemann, and T. Grasmeyer, "On the State of Crypto-Agility," IACR Cryptology ePrint Archive, Report 2023/487, 2023.

[4] M. H. T. Essa and P. Crossley, "GOOSE Performance Assessment on an IEC 61850 Redundant Network," *The Journal of Engineering*, vol. 2018, no. 15, pp. 841–845, 2018.

[5] IEEE, "IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications," IEEE Standard C37.238-2017, 2017.

[6] T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, 2020.

[7] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, 2020.