QUANTUM COMPUTING THREAT MODEL

Energy Sector Cryptographic Infrastructure

Report Type:	**STRIDE-Based Threat Model with Data Flow Diagrams**
Methodology:	**STRIDE Framework + Attack Trees + Risk Matrix**
Target System:	**Energy Grid Control Systems & Infrastructure**
Classification:	**CRITICAL INFRASTRUCTURE**
Report Date:	**November 27, 2025**
Group:	**Group 19**
Authors:	**Ali Al Said, Zixuan Shan, Erica Belcena, Anmol Vats**

■ WARNING: This report identifies CRITICAL quantum computing threats to energy infrastructure. Immediate action required for Harvest Now, Decrypt Later (HNDL) attacks currently in progress. Migration window: 2025-2031.

EXECUTIVE SUMMARY

This threat model analyzes quantum computing risks to energy sector cryptographic infrastructure using the STRIDE methodology. The analysis identifies 18 distinct threats across six categories, with particular emphasis on quantum-enabled attacks that could compromise grid operations, data confidentiality, and system integrity.

Key Findings:
• **CRITICAL:** Harvest Now, Decrypt Later (HNDL) attacks are **ACTIVE NOW**, targeting strategic infrastructure data with 20-50 year relevance
• **CRITICAL:** Certificate Authority compromise could collapse entire trust infrastructure
• **HIGH:** VPN authentication vulnerable to quantum attacks by 2030-2036
• **HIGH:** ICS command channels susceptible to tampering via quantum decryption

Timeline:
• **2025 (NOW):** Immediate hybrid PQC deployment required
• **2028-2031:** Critical migration window for core infrastructure
• **2030-2036:** Cryptographically Relevant Quantum Computer (CRQC) expected
• **2036:** All classical cryptography assumed broken

Regulatory Drivers:
• EU NIS2 Directive & DORA mandating operational resilience
• US Presidential Executive Order requiring PQC by 2035
• UK NCSC roadmap with 2028-2035 migration phases
• NIST PQC standards finalized (Kyber, Dilithium, Falcon, SPHINCS+)

This report provides comprehensive threat analysis with Data Flow Diagrams (DFDs), attack trees, risk matrices, and detailed mitigation strategies aligned with a four-layer defense framework.

THREAT INVENTORY

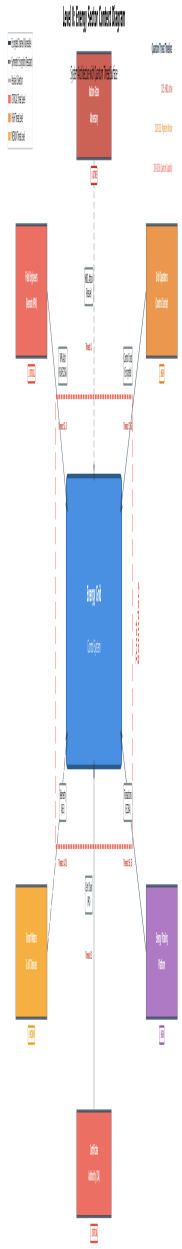
ID	Category	Threat Name	Priority	Timeline
I1	Info Disclosure	HNDL Attacks	CRITICAL	NOW
E1	Elevation	CA Compromise	CRITICAL	2028-2036
S1	Spoofing	VPN Auth Forgery	HIGH	2028-2036
T1	Tampering	ICS Manipulation	HIGH	2030-2036
I3	Info Disclosure	Credential Exposure	HIGH	2028-2036
E2	Elevation	Privilege Escalation	HIGH	2028-2036
S2	Spoofing	PMU Spoofing	MED-HIGH	NOW
T3	Tampering	Firmware Tampering	MED-HIGH	2028-2036
D1	Denial of Service	PQC Performance	MED-HIGH	NOW
S3	Spoofing	Blockchain ID Spoof	MEDIUM	2030-2036
T2	Tampering	Data Modification	MEDIUM	2030-2036
I2	Info Disclosure	Real-time Exposure	MEDIUM	2030-2036
D2	Denial of Service	Quantum DDoS	MEDIUM	2030-2036
E3	Elevation	Smart Contract	MEDIUM	2030-2036
R1	Repudiation	Trading Repudiation	LOW-MED	2030-2036
R2	Repudiation	Audit Repudiation	LOW-MED	2030-2036
I4	Info Disclosure	Smart Meter Privacy	LOW-MED	2032+
D3	Denial of Service	Time Sync Denial	LOW-MED	NOW

Summary Statistics: 18 total threats identified | 2 CRITICAL | 4 HIGH | 3 MED-HIGH | 5 MEDIUM | 4 LOW-MED | 3 threats ACTIVE NOW requiring immediate action

1. SYSTEM ARCHITECTURE & DATA FLOWS

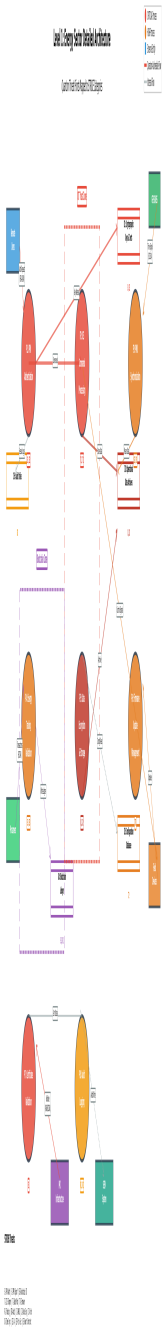
1.1 Level 0 Context Diagram

High-level system context showing external entities, trust boundaries, and quantum threat surface. Red dashed lines indicate trust boundaries separating trusted internal systems from external actors and untrusted zones.



1.2 Level 1 Detailed Architecture

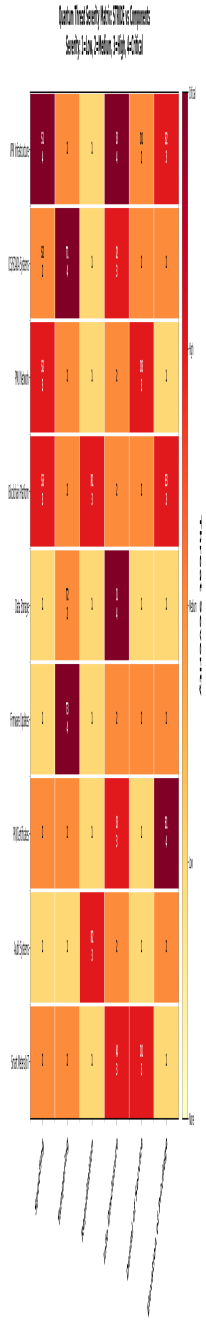
Detailed process decomposition showing data stores, processes, and data flows. Processes are numbered (P1-P8), data stores (D1-D5), and all quantum-vulnerable flows are annotated with STRIDE threat identifiers. Trust zones are marked with colored boundaries.



2. STRIDE THREAT ANALYSIS

2.1 Threat Severity Heatmap

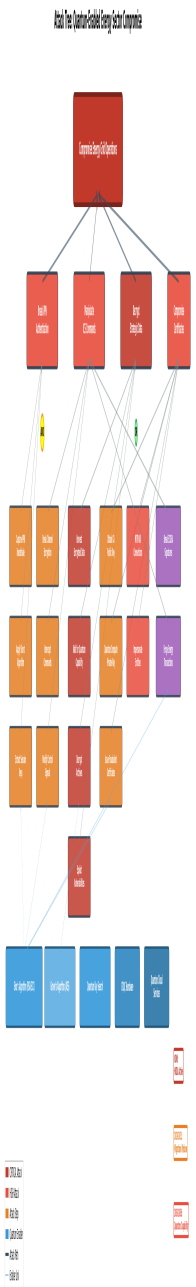
Matrix visualization showing threat severity (1=Low to 4=Critical) across STRIDE categories for each system component. Critical threats (red) require immediate attention. Each cell shows the threat ID and severity level.



3. ATTACK PATHS & KILL CHAINS

3.1 Quantum-Enabled Attack Tree

Attack tree showing progression from quantum computing capabilities (Shor's and Grover's algorithms) through attack steps to compromise of energy grid operations. AND gates require all sub-attacks to succeed; OR gates require only one path. Quantum enablers (blue) provide the foundation for higher-level attacks.



4. MITIGATION ROADMAP

MITIGATION FRAMEWORK

A four-layer defense-in-depth approach addresses identified quantum threats across immediate, medium-term, long-term, and ongoing timeframes.

LAYER 1: IMMEDIATE ACTIONS (2025-2028)

- Deploy hybrid classical/PQC encryption for high-value communications
- Conduct comprehensive cryptographic inventory across all systems
- Implement crypto-agile infrastructure for rapid algorithm updates
- Re-encrypt strategic data archives with quantum-resistant algorithms
- Enhanced monitoring for VPN anomalies and authentication failures

LAYER 2: MEDIUM-TERM TRANSITION (2028-2032)

- Migrate VPN infrastructure to post-quantum key exchange (Kyber)
- Upgrade PMU authentication to PQC-based signatures (Dilithium/Falcon)
- Implement quantum-safe blockchain signature schemes
- Replace ICS device certificates with PQC-based PKI
- Deploy hardware security modules (HSMs) with quantum-resistant capabilities

LAYER 3: LONG-TERM HARDENING (2032-2036)

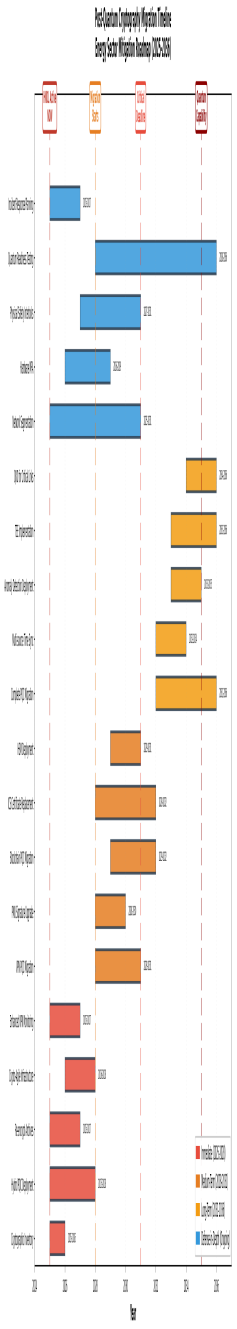
- Complete migration of all cryptographic systems to PQC standards
- Multi-source time synchronization with quantum-safe authentication
- Physics-based anomaly detection for operational validation
- Trusted execution environments (TEEs) for smart contract validation
- Quantum key distribution (QKD) for highest-security connections

LAYER 4: DEFENSE-IN-DEPTH (ONGOING)

- Network segmentation and zero-trust access controls
- Hardware-based multi-factor authentication
- Physical safety interlocks for impossible operational states
- Regular quantum readiness assessments and penetration testing
- Incident response plans for quantum compromise scenarios

4.1 Post-Quantum Cryptography Migration Timeline

Gantt-style timeline showing PQC migration activities from 2025-2036. Vertical dashed lines mark critical quantum threat milestones. Activities are color-coded by layer: Red (Immediate), Orange (Medium-term), Yellow (Long-term), Blue (Defense-in-Depth).



5. IMMEDIATE RECOMMENDATIONS

1. CRITICAL - Address HNDL Threat (Within 30 days)

- Implement hybrid PQC encryption for all external communications
- Identify and re-encrypt archived strategic data using NIST PQC algorithms
- Establish quantum-safe key management infrastructure
- Deploy network traffic analysis to detect data harvesting

2. HIGH PRIORITY - VPN Infrastructure (Within 90 days)

- Audit all VPN configurations for quantum-vulnerable protocols
- Begin pilot deployment of post-quantum VPN solutions
- Implement certificate pinning and hardware-based authentication
- Enhanced logging and anomaly detection for VPN access

3. HIGH PRIORITY - ICS/SCADA Systems (Within 180 days)

- Complete cryptographic inventory of all control systems
- Implement network segmentation between IT and OT
- Deploy physical safety interlocks independent of cryptography
- Establish incident response procedures for quantum scenarios

4. ONGOING - Organizational Readiness

- Establish PQC migration governance and steering committee
- Allocate budget for multi-year migration program
- Engage with vendors on PQC roadmaps and timelines
- Conduct tabletop exercises for quantum compromise scenarios
- Regular briefings to executive leadership on quantum risk posture

6. CONCLUSION

This STRIDE-based threat model identifies significant quantum computing risks to energy sector cryptographic infrastructure. The analysis reveals that 18 distinct threats span all six STRIDE categories, with two CRITICAL-priority threats requiring immediate action: Harvest Now, Decrypt Later (HNDL) attacks currently in progress, and the potential for Certificate Authority compromise.

The window for migration to post-quantum cryptography is narrowing. With conservative estimates placing Cryptographically Relevant Quantum Computer (CRQC) capability between 2030-2036, and given the 3-5 year timeline for infrastructure migration, organizations must begin implementation **now** to meet the 2028-2031 critical migration window.

Key Takeaways:

- Nation-state adversaries are actively collecting encrypted energy sector data for future quantum decryption
- VPN, ICS, PKI, and blockchain infrastructures all require PQC upgrades
- Regulatory frameworks (NIS2, DORA, NCSC guidance) mandate PQC adoption
- NIST-standardized algorithms (Kyber, Dilithium, Falcon) are ready for deployment
- Four-layer mitigation framework provides structured approach to quantum resilience

Organizations that delay PQC migration risk catastrophic compromise of critical infrastructure, long-term competitive disadvantage, and regulatory non-compliance. The quantum threat is not theoretical—it is happening now, and the time to act is immediate.

Next Steps: Establish executive sponsorship, allocate resources, conduct cryptographic inventory, and begin hybrid PQC deployment for highest-value assets within 30 days.