FERC and the Office of Electric Reliability

Priorities and Current Focus Areas

Deepak Ramlatchan,
Deputy Director, Office of Electric Reliability
Federal Energy Regulatory Commission

MRO Summit May 2026

Federal Energy Regulatory Commission

Overview

- Intro and OER Key Focus Areas
- Challenges and Solution Opportunities
  - Evolving BPS
  - Extreme Weather
  - Cyber Security
  - Load Growth: Large Loads

Office of Electric Reliability

Responsible for protecting and improving the reliability of the Bulk Power System

Oversight of NERC Reliability Standards development and enforcement

Engineering support for other FERC filings and rules

Leadership Team

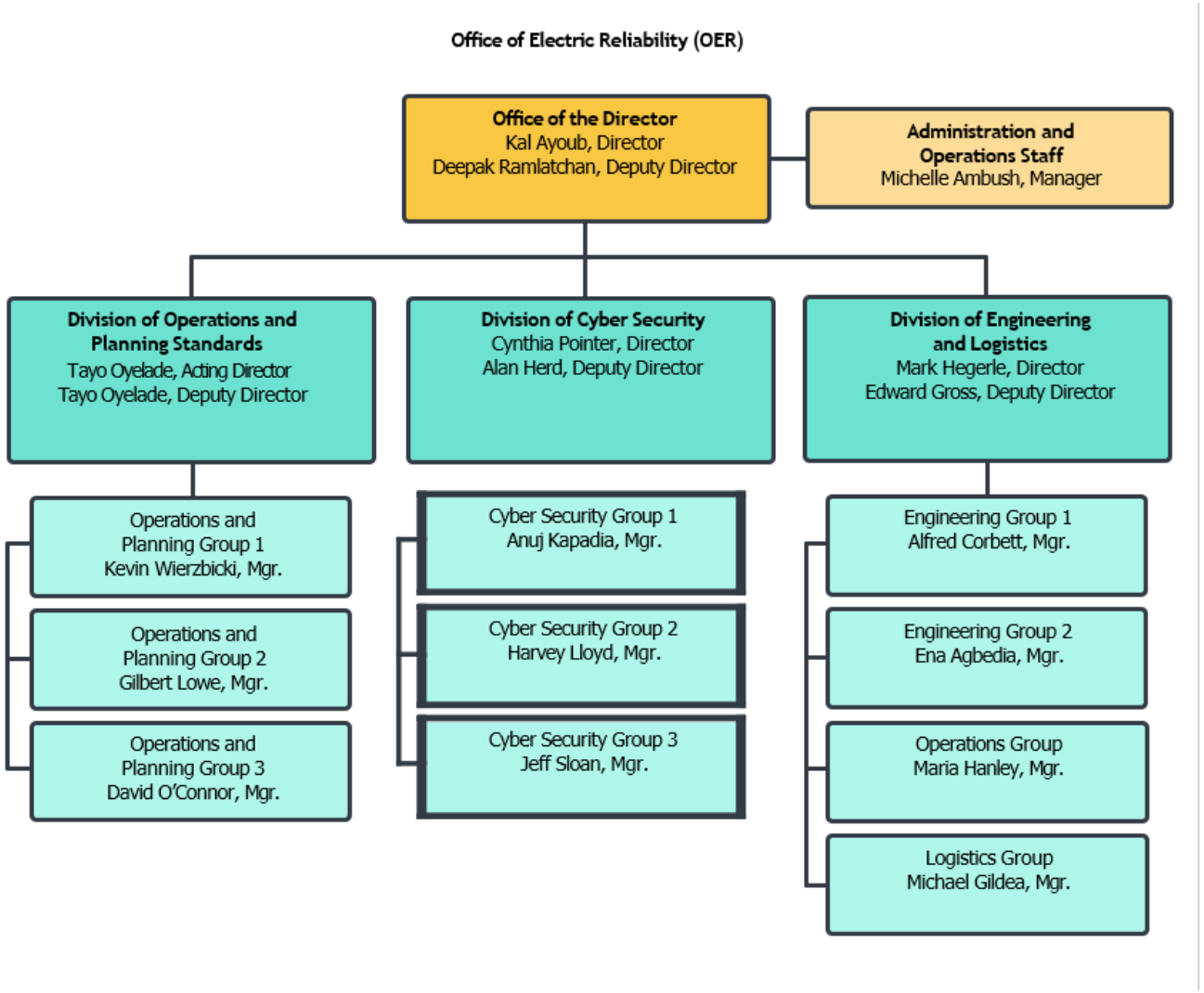
Kal Ayoub

Director

Deepak Ramlatchan

Dep. Director

All opinions are my own and do not reflect the views of the Commission or any individual Commissioner



Office of Electric Reliability

FEDERAL ENERGY REGULATORY COMMISSION

OER Functions and Responsibilities

- Review NERC-proposed penalties
- Provide technical support on tariff filings and rulemakings, focusing on system engineering and reliability impacts
  - Review over 500 FPA section 205/206 filings per year
- Analyze and issue reports on blackouts and major grid events with recommendations to mitigate recurrence
- Monitor the bulk-power system 24/7 to ensure the Commission is informed of major and evolving system events
- Perform seasonal energy market and electric reliability assessment

OER Priorities

Cyber and Physical Security

- Supply Chain Compromise
- Protections for Low Impact Assets
- Physical Security

Rapidly Evolving BPS

- Inverter Based Resources (IBR)
- Resource/Energy Adequacy, Load Growth
- Priority System Attributes (e.g., quick start, ramping)

Extreme Weather

- Asset Hardening (e.g., generator freeze protection)
- System Planning and Design

Office of Electric Reliability

OER is the Commission's lead reliability office under section 215 of the FPA. OER performs the oversight role for electric reliability, approving and enforcing reliability standards developed by NERC

- Advise on whether to approve, remand or require changes to reliability standards proposed by NERC
  - Monitor or process 10-30 new or revised reliability standards per year
- Oversee compliance with approved standards by users, owners, and operators of the Bulk-Power System (BPS)

NERC RISK Priorities Report, 2025

- Grid Transformation (including demand growth and large loads)
- Resilience to Extreme Events
- Critical Infrastructure Interdependencies
- Security
- Energy Policy

https://www.nerc.com/comm/RISC/Related%20Files%20DL/2025_RISC_ERO_Priorities_Report.pdf

Actions to Address Reliability Challenges

- Resource Transition
  - Order No. 901 – directives for new or revised reliability standards covering IBR data sharing, model validation, planning and operational studies, and performance requirements
  - IBR Registration Orders (RD22-4, RR24-2) – Issued June 2024, requires NERC to determine which IBRs are required to comply with relevant reliability standards by May 2026

Actions to Address Reliability Challenges

- Order 901
  - Three batches of standards due November 2024, 2025, and 2026
  - Second batch November 4, 2025: Data sharing, data and model validation for registered IBRs, unregistered IBRs, and IBR-DERs in the aggregate. Approved February 2026
  - Third batch November 2026: Planning and operational studies for registered IBRs, unregistered IBRs, and IBR-DERs in the aggregate.
  - Effective Date of New or Revised Standards: all new or modified IBR-related Reliability Standards must be effective and enforceable "well in advance of 2030."

Actions to Address Reliability Challenges

- Cybersecurity

- **Summer 2025**
  - **Internal Network Security Monitoring**: issued Order No. 907 (June 2025) and Order No. 907-A (August 2025) approving Reliability Standard CIP-015-1 that requires INSM inside an entity's electronic security perimeter and directing modifications to extend protections to access control systems outside of the electronic security perimeter (RM24-7).

- **March 2026:**
  - **Final Rule on Virtualization Reliability Standards, Docket No. RM24-8-000**
    - secure use of virtualization technologies
  - **Final Rule on CIP Reliability Standard CIP-003-11, Docket No. RM25-8-000**
    - baseline cybersecurity for low impact bulk electric system (BES) Cyber Systems

Actions to Address Reliability Challenges

- Extreme Weather
- TPL-008-1 (Transmission System Planning Performance Requirements for Extreme Temperature Events), filed in response to Order No. 896, approved February 2025
- EOP-012-3 (Extreme Cold Weather Preparedness and Operations), the revised generator winterization reliability standard, effective October 2025
  - Commission previously accepted and directed further revisions to address concerns pertaining to generator cold weather constraints and corrective action implementation

Large Loads

CHAIRMAN SWETT

Top Priority:

"Connect and power …as quickly and durably as possible…"

Large Loads

NERC

- Large Load Working Group
  - Whitepapers, Guidelines, Alerts
- Project 2026-02 "Computational Loads"
  - SAR comment period, SDT

FERC Proceedings

DOE ANOPR

Industry Whitepapers etc.

Large Load Issues

Resource Adequacy

Unexpected, simultaneous loss

Protection System Failures (co-located)

- Sudden appearance of load
- Sudden appearance of the generator

Oscillations

- Sub-synchronous
- Forced

Power Quality Issues

- Harmonics

Load Growth: Large Loads

- Forced Oscillations: the rapid, synchronized power demands of AI workloads (like GPU clusters) create fluctuating loads that can resonate with the power grid's natural frequencies, potentially causing widespread instability, equipment damage (like turbines), and blackouts. These rapid fluctuations (tens to hundreds of MW in milliseconds) act as "forcing signals," unlike steady industrial loads, demanding new grid management strategies for grid operators to maintain stability.
- Sub-synchronous Oscillations: These oscillations are usually caused by the load's own fast-acting control systems interacting with grid impedance or nearby generators.

Megapack

"Today's problem is dealing with extreme power jitter…

We are having some power fluctuation issues, when you do synchronized training it's like having an orchestra and it can go loud to quiet very quickly, at the sub-second level. The electrical system freak out about that – with 10-20 MW shifts several times per second."

- Elon Musk
  August 2024 in conversation with Lex Fridman about xAI Memphis data center

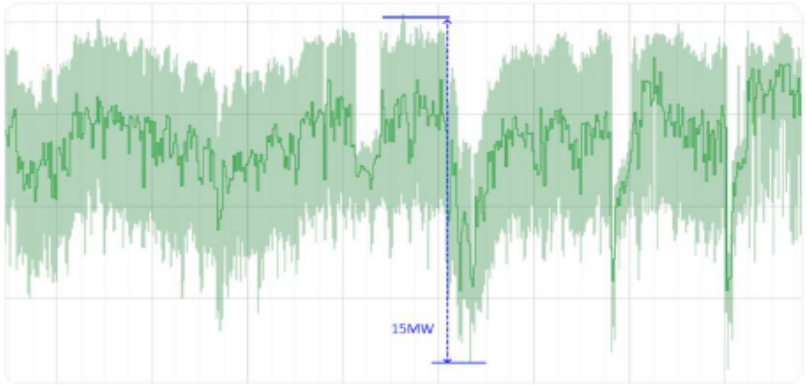


Fig. 1. Large power fluctuations observed on cluster level with large-scale synchronized ML workloads

"In our latest batch-synchronous ML workloads running on dedicated ML clusters, we observed power fluctuations in the tens of megawatts"

- Google Technical Lead Manager and VP, Engineering
  February 2025, Blog Post

Large Load Issues: Power Swings

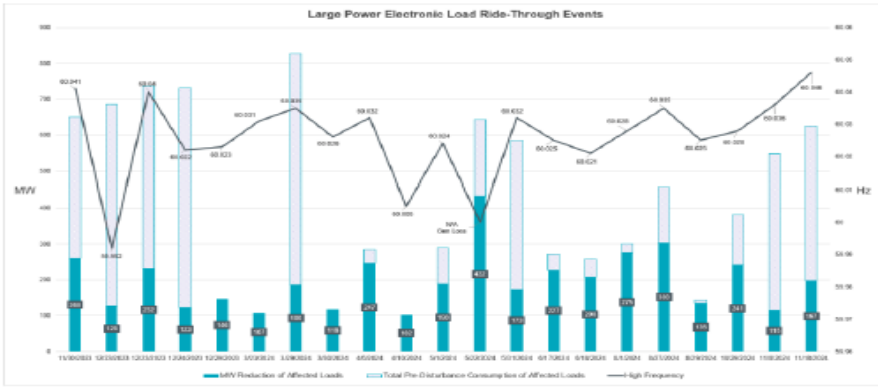
Megapack

Challenge: Low Voltage Ride Through (LVRT) of data centers

Dominion: 1.5 GWs across 60 data centers

July 2024 – due to reclosing attempts on faulted 230 kV system

ERCOT: Many events of 100s of MWs



Grid Operator Perspective

- Challenging to manage load drops at this scale
- Over frequency and voltage concerns

Data Center Perspective

- UPS systems working as intended
- Protecting our expensive and reliability critical equipment from utility system faults

Large Load Issues: sudden loss

Questions

- FERC and OER Priorities and Focus Areas

2025 Lessons Learned Report

Commission-led CIP Reliability Audits

Alan T. Herd
Deputy Director, Division of Cyber Security
Office of Electric Reliability
Federal Energy Regulatory Commission

MRO Summit May 2026

Overview

- This anonymized summary staff report informs the regulated community and the public of lessons learned from the Commission's FY2025 CIP Audits.
  - Provides information and recommendations to NERC, Regional entities, and registered entities for use in their assessments of risk and compliance, and to improve overall cyber security.
  - The information may be generally beneficial to the utility-based cyber security community to improve the reliability and security of the Bulk-Power System.

Background

- The Commission initiated its Reliability Standards audit program for registered entities in FY2016, and the Commission has conducted non-public CIP Audits each year since.
- Staff identifies emerging cybersecurity and compliance risks from the prior year CIP Audits that it believes will be most beneficial to share publicly.
- Reports have been issued annually beginning in 2017, with a total of 81 lessons between 2017 – 2025.

2025 Lessons Learned Report

1. Ensure that BES Asset Identification and Categorization Procedures consider Distributed Energy Resources (DERs) when determining Control Center impact rating.
   - CIP-002-5.1a, Requirement R1
2. Perform due diligence when relying on third parties to perform compliance duties.
   - CIP-003-8, CIP-006-6 and CIP-010-4
3. Registered entities should consider the compliance risk when using Cloud Services.
   - CIP-004-7 and CIP-010-4

Lesson 1

CIP-002-5.1a, Requirement R1: Ensure that BES Asset Identification and Categorization Procedures consider Distributed Energy Resources (DERs) when determining Control Center impact rating.

- When identifying their Control Centers, registered entities should assess and document generation resources holistically, including DERs.
- When these resources are being operated from the same Control Center, and aggregated capacity exceeds 1,500 MW in a single interconnection, the Control Center must be categorized as Medium Impact under Attachment 1, Section 2.11.

Lesson 2

CIP-003-8, **CIP-006-6**, **CIP-010-4**: Perform due diligence when relying on third parties to perform compliance duties.

- Registered entities are ultimately responsible for compliance with the applicable Reliability Standards, even when using third parties for their compliance obligations.
  - Document and track the security and compliance risks posed by outsourcing functions and processes to a third-party in their supply chain risk management plan.
  - Implement compensating controls to reduce the compliance and security risk of using third parties.

Lesson 3

CIP-004-7, **CIP-010-4**: Registered entities should consider the compliance risk when using cloud services.

- It is a strong cyber security practice to consider both benefits and risks when deciding whether to use cloud services.
- Registered entities should understand the current limitations of the CIP standards when operating high and medium impact BES cyber systems in the cloud.
- Registered entities with low impact BES cyber systems can use cloud services but should understand that a change in designation to medium impact will have commensurate CIP compliance consequences.

Questions

- 2025 Lessons Learned Report from Commission-led CIP Reliability Audits

Reliability Risk with an Internal Control Focus

May 12, 2026

MIDWEST RELIABILITY ORGANIZATION

Agenda

- ERO Internal Controls
- Opportunities to Gather Internal Controls
- Assessment of Internal Controls

ERO Internal Controls Frameworks

- COSO
- GAGAS/Yellow Book
  - Includes discussion on assessment of Internal Controls
- GAO Green Book
  - Sets the standard for organizational roles and effective Internal Control systems
  - Defines principles supporting effective design, implementation, and operation of IC

ERO Internal Controls

- Maturity Model assessment
  - Focuses on the global program
  - Questions available in the ICP_ICM Questionnaire moving to the ERPQ
- Specific Risk Category information
  - Format available in Risk and Internal Controls Workbook
- Both files available on the MRO audit website in the templates zip file

ERO Internal Controls

- Risk determination
  - Inherent Risk
    - This is the information that comes from the Enforcement department based on what is owned
  - Residual Risk
    - This information then incorporates what internal control information MRO has about the registered entity
    - Can include information from other departments

ERO Internal Controls

- **Focus is on risk**
  - Preoccupation with failure. Attention on close calls and near misses (“being lucky vs. being good”); focus more on failures rather than successes
  - Reluctance to simplify interpretations. Solid “root cause” analysis practices.
  - Sensitivity to operations. Situational awareness and carefully designed change management processes.
  - Commitment to resilience. Resources are continually devoted to corrective action plans and training.
  - Deference to expertise. Listen to your experts on the front lines (ex. authority follows expertise).

CIP Best Practice identified for CIP-004 R4.3

Requirement language: For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.

Example internal controls:

- Review access on a quarterly basis
- Automated software to scan for accounts
- Group reviews for privileged access

CIP Best Practice identified

For a small registered entity: Reviewing access on a quarterly basis may be acceptable depending upon how many employees and reviews need to occur. This may not be an effective control for a larger registered entity as the reviews could be over 10 pages for a specific role

For a medium registered entity: Having software that gathers the information about accounts and then having an individual review that information may be sufficient.

For a large registered entity: Having the software as well as reviewing in a group/multiple reviewers is something that may make an effective control

O&P Best Practice identified for EOP-012-3 R5

Requirement language: Each Generator Owner, in conjunction with its Generator Operator, shall identify the entity responsible for providing generating unit-specific training, and that identified entity shall provide annual training to the maintenance and operations personnel, as applicable, responsible for implementing the cold weather preparedness plan(s) developed pursuant to Requirement R4.

Example internal controls:

- Spreadsheet tracking
- Software tracking
- Multiple department reviews

O&P Best Practice identified

For a small registered entity: Reviewing training on a spreadsheet on an annual basis or when an individual is hired could be an effective control. This would not be effective for an entity that has 500 employees to track.

For a medium registered entity: Depends on the number of employees. This could be a spreadsheet with multiple departments reviewing on a quarterly basis as well as when an individual is hired. May be a software program that tracks the information with a dashboard for easy reporting.

For a large registered entity: Most likely is going to be a software program that includes automated notifications and tracking for the training.

Opportunities to Provide Internal Controls

- During any CMEP activity
  - Audits
  - Spot Checks
  - Self-Certifications
  - Self-Reports
  - Mitigation Plans
  - Events

Assessment of Internal Controls

- How does this drive the Compliance Oversight Plan
  - Still restricted by the Rules of Procedure based on registration functions
- JMA project
  - Driving change to have discussions earlier and have impacts to audit scope and sampling
  - This is a multi-year project

COP Performance Considerations

- Compliance History
- Culture of Compliance
- Events
- Misoperations
- Internal Controls
- Generation
- Transmission

Assessment of Internal Controls

- What should an entity provide for internal controls?
  - Provide documentation of the design and implementation of the internal controls
  - Initial information is provided as part of the Internal Compliance Questionnaire
    - This will be transitioning to the ERPQ functionality in Align

Assessment of Internal Controls

- Information provided as part of the internal controls workbook
  - Want to provide the design information
    - Documented information such as processes, procedures, etc. . .
  - Want to provide evidence of the implementation of the internal control
    - Technical controls
      - Example: Reoccurring meeting invites or configuration of software
    - Automation
      - Handled via automation of the task such as testing that software is functioning as intended

Assessment of Internal Controls

20YY XXXX Audit
Risk and Internal Controls Workbook

Background:
The Standard(s) and Requirement(s) listed in the row(s) below are for Internal Control(s) inquiry which is performed as part of a monitoring engagement. Understanding the extent to which an entity contemplates risk and designs/implements Internal Control(s) to help reduce inherent risk(s) is an integral part of the monitoring objective.

Instructions:
1) Please review the question(s) in Row 3 and provide a response(s) and/or operational risk(s) your organization has identified, as well as any designed and implemented Internal Control(s) which help reduce the inherent risk(s).

2) Please add rows as necessary to list any additional identifi

3) For Columns F through I, please provide a brief insight that ...ate/how example instance(s) demonstrating that each attribute has been defined, developed, and/or performed. This may include, but not limited to, process document(s)/steps, evidence such as screenshot(s) of applications, meeting agendas and minutes, calendar items, tracking document(s) (r... , and so forth.

4) Upload this completed workbook along with any reference

Entity's Global Risk Management Question:

Does your organization have a formal Risk Identification and/or Risk Management program that contemplates your organization's extent of compliance and/or operational risks? If so, please provide a description of the extent of your program (such as a brief narrative) and an example of how risks are identified, categorized, and prioritized (such as a screenshot of a portion of a Risk Matrix or Risk Register so the MRO reviewer(s) can see how it works - do not send entire documents showing all risks).

Global Risk Management

Standard	Requirement	Purpose of Standard	Requirement

Example Only (Shaded in light green):

Risk Assessment	Control Objective	Control Design	Implementation	Effectiveness
[EXAMPLE]		For the determination of System Operating Limits.	determining its Facility Ratings.		audit and subsequent updates to the FR database when inconsistencies are found.	Program Process Steps.docx" for control design details.	which was prepared to help the reviewer understand how the control was designed and how it is being implemented.	

Assessment of Internal Controls

Risk Assessment

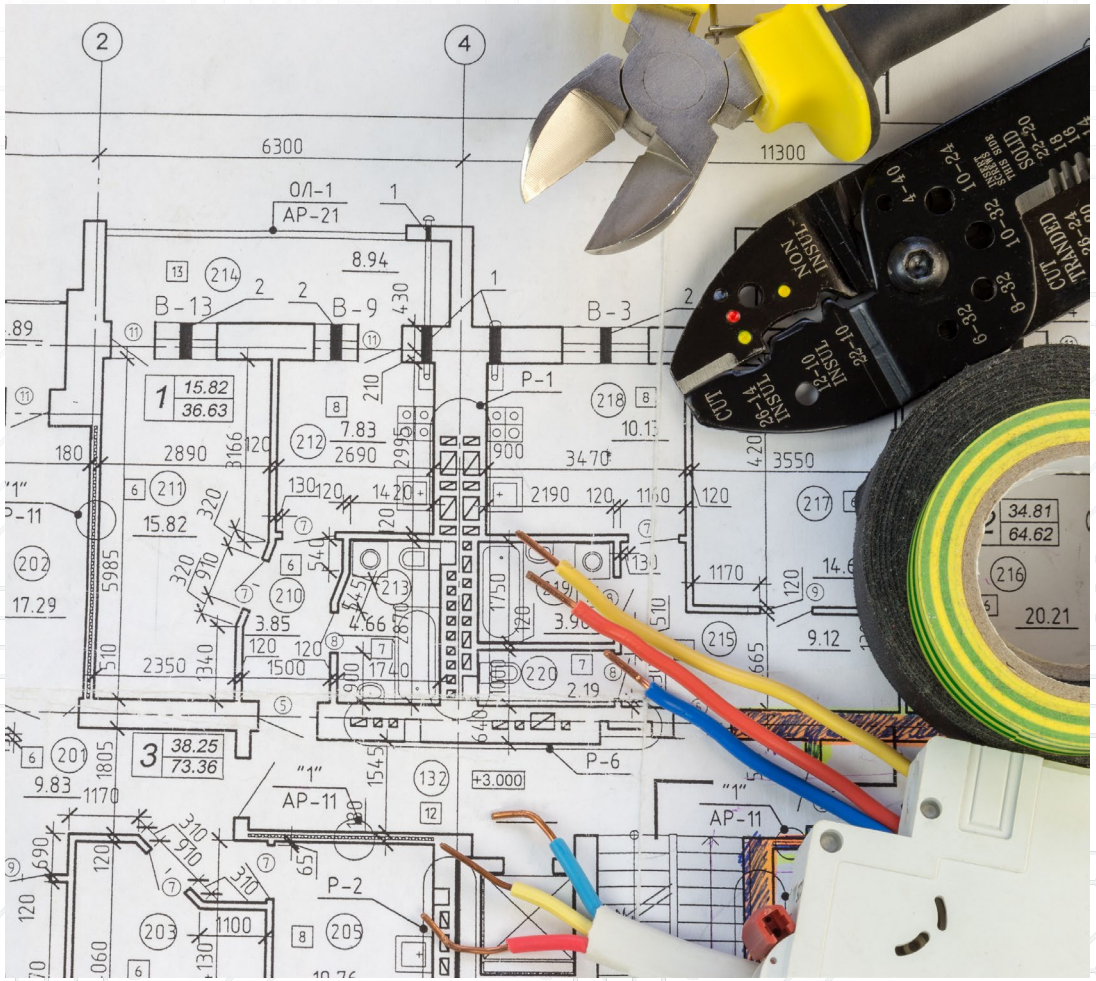
- Description of Compliance and/or Operational Risk(s)

Assessment of Internal Controls

Control Objective

- What is the overall objective of the control?
- An explanation of how the identified risk is being addressed

Assessment of Internal Controls



Control Design

- Summarization of the activities and/or actions performed to achieve the objective of the control

Assessment of Internal Controls

Implementation

- Evidence of the action taking place
- Frequency of the action taking place

Assessment of Internal Controls

Effectiveness

- Assessment of whether the control is effective in helping to reduce the risk
- What did this assessment look like?

Assessment of Internal Controls

- Risk Category selection
  - Discussions from the workbook are going to drive discussions of any concerning residual risks

Questions

ASK AWAY!

QuSecure

May 2026

Artificial Intelligence and Quantum Computing

Agenda

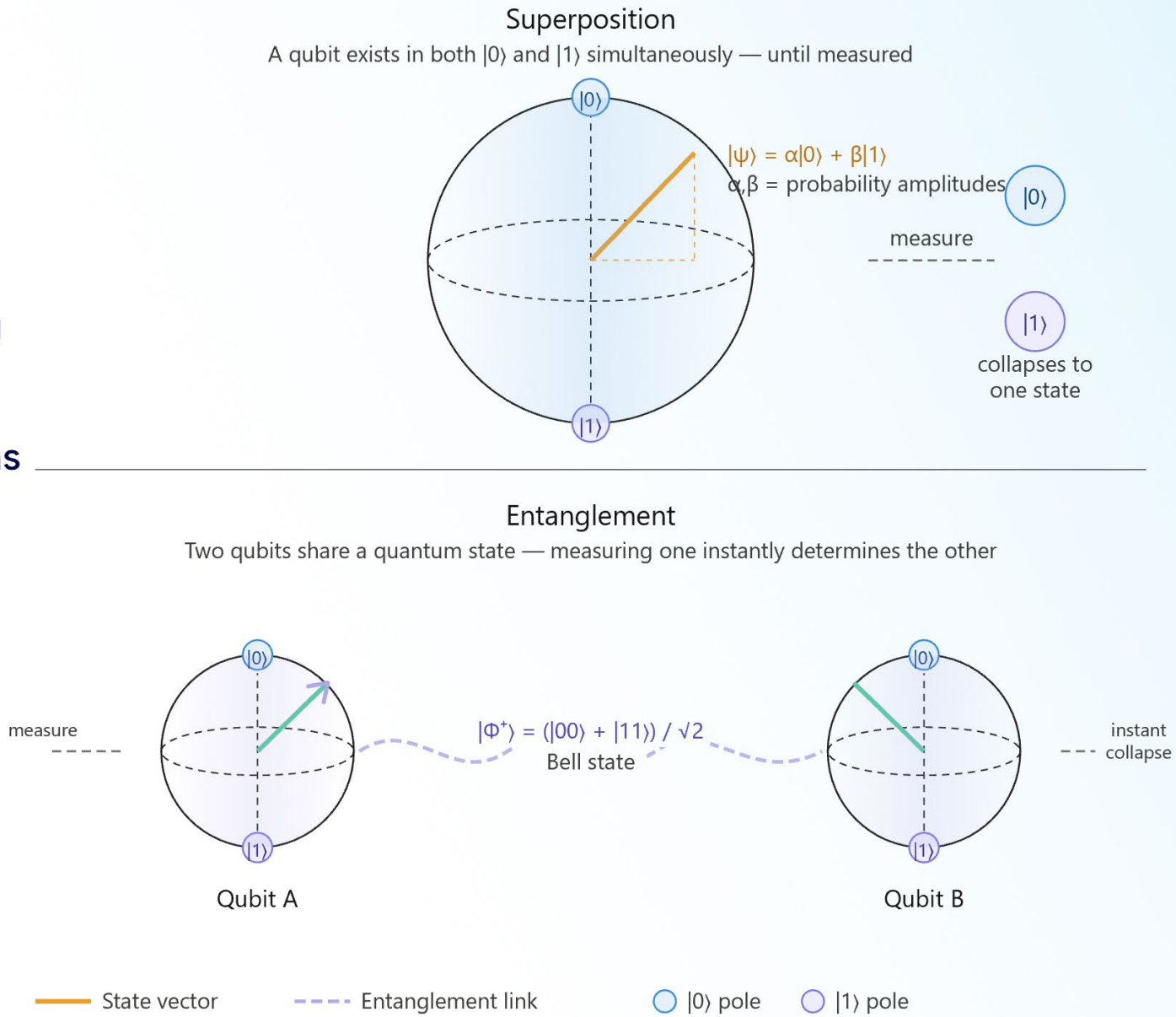
- Background and Problem
- Quantum and Artificial Intelligence
- QuantumAI, Cybersecurity, Operational Technology
- AI Augmented Attacks
- The Problem
- OT vs IT The Core Challenge
- The OT Attack Surface
- Critical Infrastructure at Risk
- Implementation Strategy for Post Quantum Cryptography for CI
- Conclusions and Call to Action

Background and Problem

- Power grids are rapidly evolving from isolated systems into interconnected, digitally driven "smart grids" that enable two-way communication, renewable energy integration, and real-time consumer control.
- Major investments — including an $8 billion U.S. Department of Energy program — have accelerated this transformation globally, with countries like Germany, China, and South Korea leading adoption.
- This increased connectivity comes at a cost: smart grids are now exposed to a wide range of cybersecurity threats that endanger national security, economic stability, and public safety.
- The merging of Operational Technology (OT) and Information Technology (IT) creates unique vulnerabilities that traditional security measures can no longer adequately address.

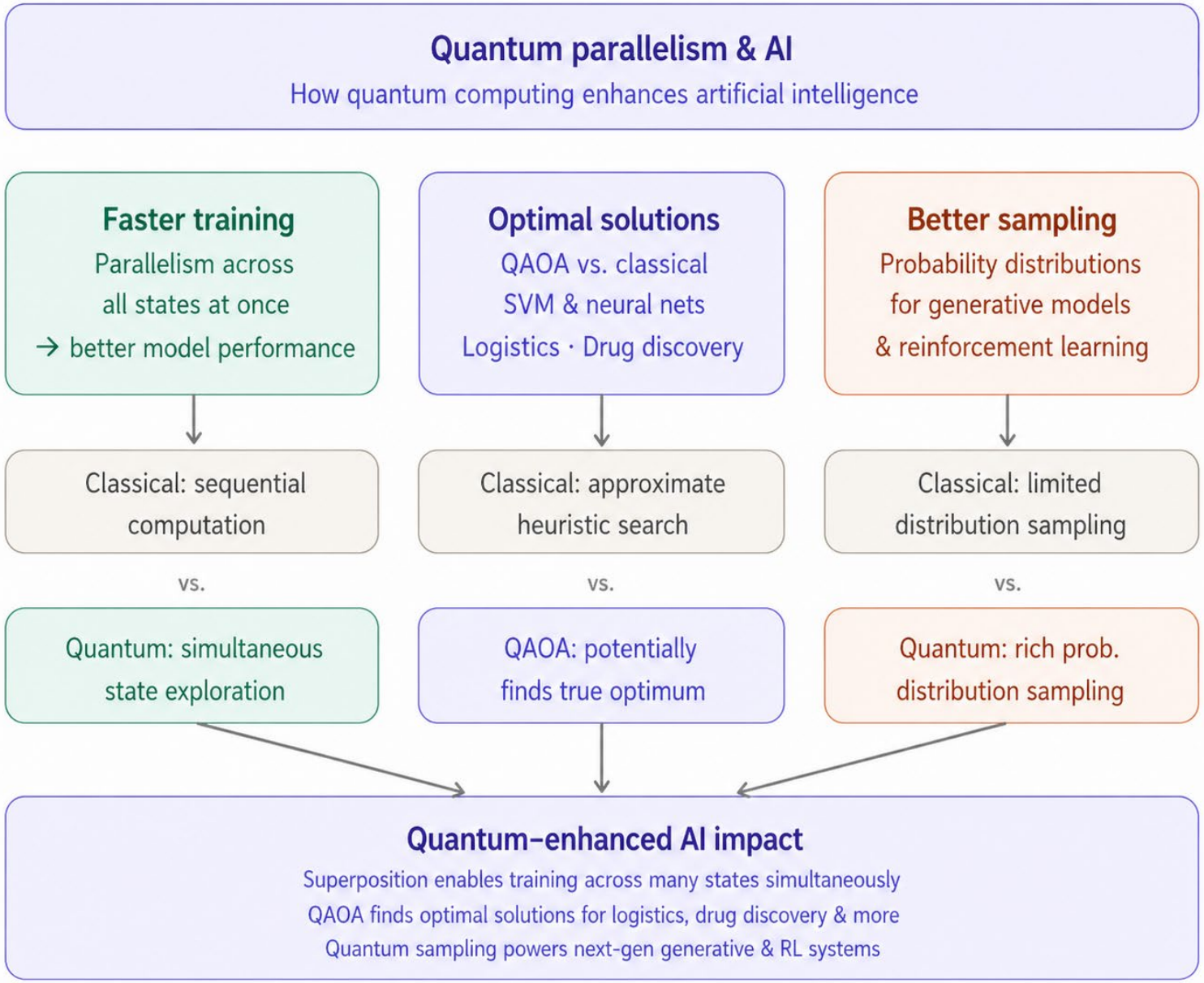
Quantum and AI

- Interdisciplinary field that merges Quantum Mechanics and AI concepts
- Leverages Superposition and Entanglement to enhance AI algorithms and models by exploiting qubits
- Quantum Computing attempts to solve problems that are difficult for classical computers by:
  - Use of qubits speeds up processing times
  - Improving computational efficiency
- Parallelism
  - Allows for faster computation on larger datasets in parallel unlike classical computation
  - Optimization, Classification, and Clustering can be done more efficiently



Quantum and AI

- Quantum Approximation Optimization Algorithm (QAOA)
- Quantum Support Vector Machines (QSVM)



Quantum and AI

- Quantum Monte Carlo methods allow for rapid sampling enabling AI systems to make better predictions based on complex distributions leading to:
  - Better predictions especially in uncertain environments

- QC Algorithms with AI leads to faster:
  - Convergence
  - Training by rapidly evaluating model parameters
  - Improved performance with machine learning algorithms

- QAI is particularly relevant to better:
  - Feature selection
  - Hyperparameter tuning
  - Neural network training

Quantum and AI

- QC could speed up the **manufacturing process of devices** with properties such as **superconductivity, high strength or improve signal performance**

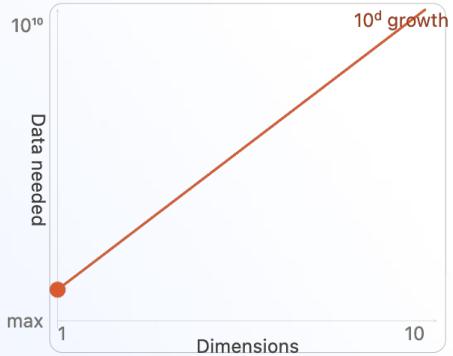
- Quantum K-nearest Neighbor **(QKNN), (QSVM)** and Quantum Principal Component Analysis **(QPCA)** offer novel ways to **handle high dimensional data**
  - *“Curse of Dimensionality” is significantly reduced*

- ***Patterns that are usually obscured to classical AI Algorithms can be discovered by Quantum algorithms***

Dimensions 1

Data points needed	Avg. nearest-neighbour dist.	Sparsity level
10	0.05	Low

1D line



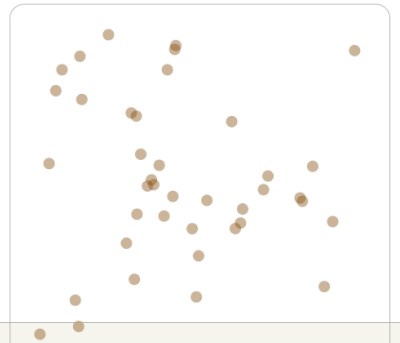
1D: Points sit on a line. A model needs ~10 samples to cover the space. Easy.

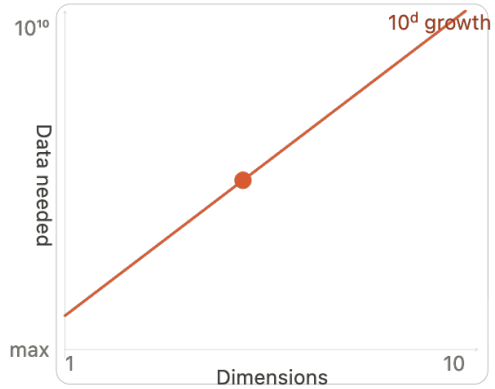
Dimensions 5

Data points needed	Avg. nearest-neighbour dist.	Sparsity level
100K	0.41	High

Curse of Dimensionality

1D line



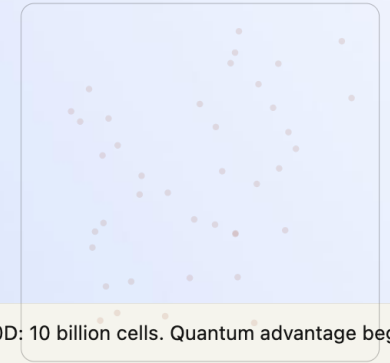


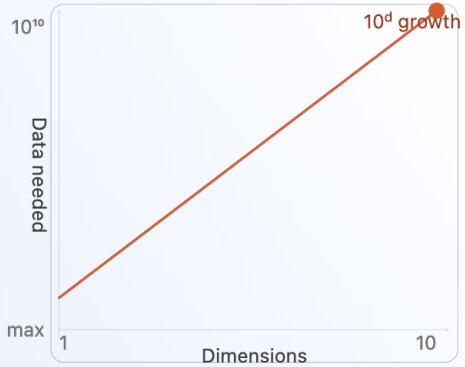
5D: 100,000 cells. Nearest neighbours are almost as far as farthest neighbours.

Dimensions 10

Data points needed	Avg. nearest-neighbour dist.	Sparsity level
10B	0.86	Critical

1D line





10D: 10 billion cells. Quantum advantage begins here — superposition explores all states simultaneously.

Quantum Advantage begins here

Quantum AI is still very nascent technology

QuSecure

Quantum AI, Cybersecurity and OT

AI-Augmented OT Attacks

Reconnaissance

1 AI scans OT networks, fingerprints devices, maps topology automatically

Vulnerability Discovery

2 ML models trained on CVE databases find zero-days in legacy OT firmware

Evasion & Persistence

3 Adversarial AI mimics normal SCADA traffic to bypass anomaly detection

Physical Impact

4 AI optimises attack payload timing to maximise damage to physical processes

60×
faster vulnerability scanning with AI vs manual

82%
of ICS/SCADA systems have unpatched known CVEs

3 min
median attacker dwell time before OT detection fails

AI dramatically lowers the barrier to sophisticated OT attacks — from nation-state to well-funded criminal groups.

The Problem

2,200+

Known cyberattacks per day (2022)

Every 39s

A business attacked by cybercriminals

4th

Industrial Revolution driven by AI & QC

The Threat Landscape

- Industrial environments connected to the internet to boost performance — but now highly vulnerable to cyberattacks
- Critical Infrastructures (CI) — electricity, water, transport — are prime targets with potential for massive economic and human casualties
- Modern cyberwar leverages hacking to disrupt production, degrade devices, or steal state and industrial secrets
- The Russo-Ukrainian conflict demonstrated active large-scale cyberwarfare targeting public, media, and financial sectors

OT vs IT: The Core Challenge

Operational Technology (OT)

- Legacy hardware, low compute power
- Non-standardized communication protocols
- Latency-critical — delays cause failures
- Long deployment lifetimes (20–30 years)
- Physical safety implications

VS

Information Technology (IT)

- Modern processors with high compute
- Standardized protocols (TCP/IP, TLS)
- Latency more forgiving
- Frequent updates and patching cycles
- Data confidentiality focus

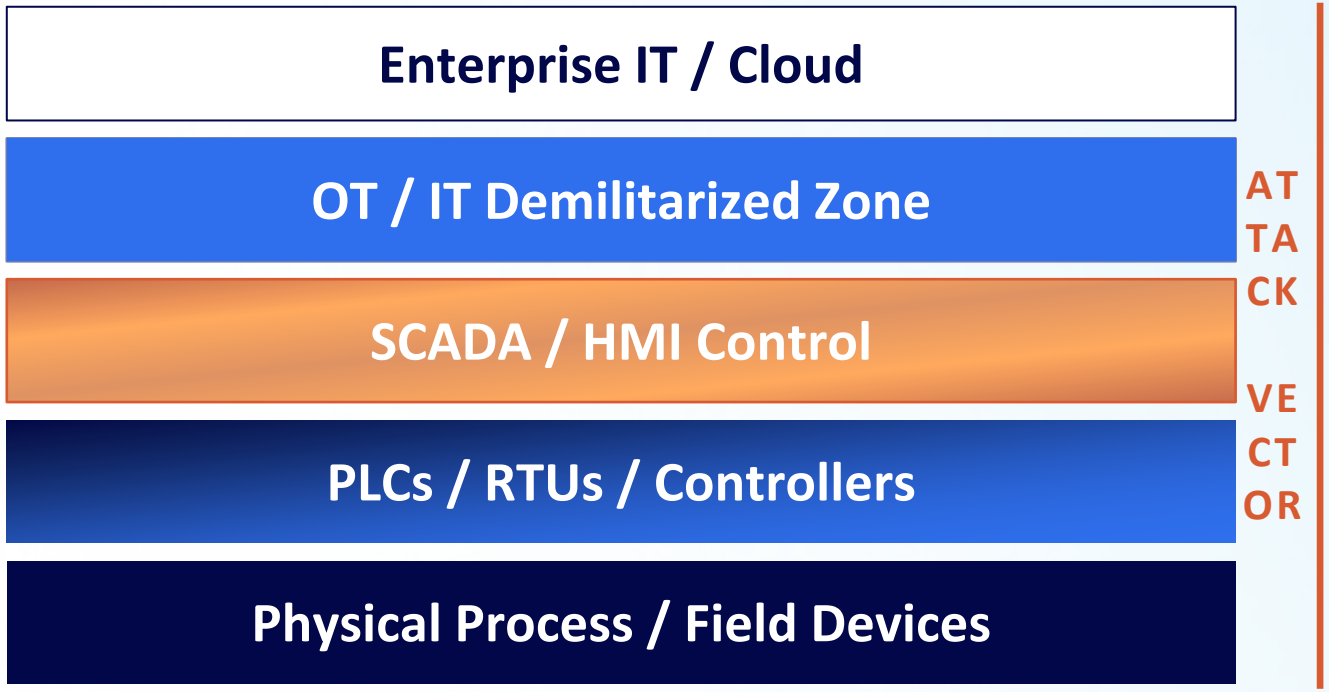
The OT Attack Surface

Why operational technology is uniquely vulnerable

OT environments — SCADA, ICS, PLCs, and industrial IoT — were designed decades ago for reliability, not security. They are now the prime target for quantum-accelerated and AI-driven attacks.

Key vulnerabilities:

- Legacy protocols with no encryption (Modbus, DNP3)
- Long asset lifecycles — 20–30 year systems
- Air-gap myth: 80% of OT now has IT connectivity
- Patching near-impossible without downtime



Convergence of IT/OT networks has dramatically expanded the OT threat surface.

Critical Infrastructure Sectors at Risk

⚡ Energy & Power — HIGH

Smart grids, SCADA systems, power generation control — outages affect millions

💧 Water & Utilities — HIGH

Treatment plants, distribution networks — tampering could cause public health crises

🚗 Transport — HIGH

Autonomous vehicles, traffic control, railway signaling — safety-critical real-time systems

🏭 Manufacturing — MED

Industrial robots, production lines — IP theft and sabotage risk

🏥 Healthcare — HIGH

Medical devices, hospital networks — lives depend on integrity and availability

💰 Finance — HIGH

Banking infrastructure, trading systems — quantum threatens transaction security

Implementation Strategy for Critical Infrastructure

1. **Crypto Agility:** Design systems that can **swap cryptographic algorithms without full infrastructure overhaul** — future-proof architecture
2. **Hybrid Schemes:** **Run classical + PQC algorithms in parallel during transition** — if one fails, the other holds; phased migration reduces risk
3. **Benchmarking First:** **Profile each OT device's compute and memory before selecting algorithms** — one size does not fit all in industrial networks
4. **Lightweight PQC:** **Prioritize lattice-based schemes** (Kyber, Dilithium) optimized for constrained devices — small code footprint, low latency
5. **Standards Alignment:** **Follow NIST PQC standards and coordinate with sector regulators (NERC CIP for energy, etc.) for compliance and interoperability**

The integration of PQC should be seamless, cheap, and non-disruptive to existing CI operations.

Conclusions & Call to Action

- 🔐 Quantum computers will break RSA and ECC — the transition to PQC is not optional
- ⚙ OT/CI environments face unique constraints that make PQC adoption non-trivial
- 📊 Lattice-based PQC (CRYSTALS-Kyber/Dilithium) shows the most promise for CI contexts
- 🔄 Crypto agility and hybrid schemes are essential during the transition period
- ⏰ Organizations must act now — before fault-tolerant quantum computers become reality

Oliva del Moral et al. | IEEE IoT Journal Vol.11 No.18 pp.30217–30244 | DOI: 10.1109/JIOT.2024.3410702

QuSecure

Help us secure the future.

Today.

CONTACT

Garfield Jones D. Eng

SVP Global Strategy & Research

Gjones@qusecure.com

www.qusecure.com

info@qusecure.com

Beyond the Floor: Building a Security-First Compliance Future

Robert M. Lee

CEO and Co-Founder, Dragos

Presentation at the MRO Reliability, Security, and CMEP Summit

May 2026

DRAGOS