Durand Porter

CRITICAL INFRASTRUCTURE RESILIENCY & SCADA OPTIMIZATION

GRANT PROPOSAL

Strengthening operational technology resiliency, cybersecurity, and energy independence for a more secure and reliable future.

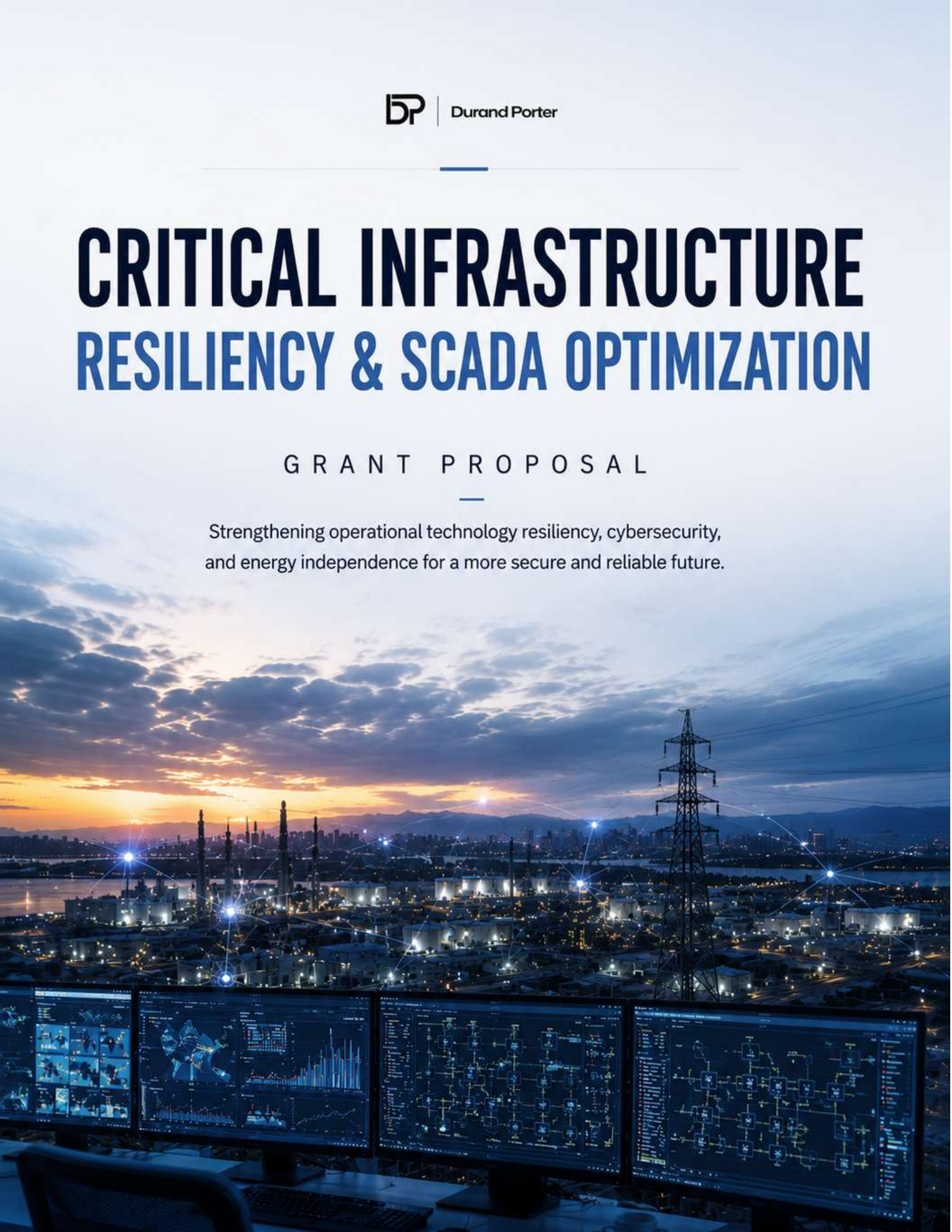

Table of Contents

1. Executive Summary

Modern industrial control environments face escalating cyber-physical vectors targeting legacy telemetry infrastructure. This proposal details an engineering roadmap to transition vulnerable, unencrypted Supervisory Control and Data Acquisition (SCADA) environments into a hardened, high-availability operational technology (OT) framework. By integrating cryptographic protections, physical network isolation, and resilient backup energy systems, the initiative reduces single points of failure and strengthens operational continuity during cyber disruptions or environmental emergencies.

The proposed modernization effort enhances infrastructure resiliency through secure telemetry communications, segmented network architectures, and advanced operational security measures designed to support uninterrupted industrial operations. The initiative also improves recovery readiness, infrastructure reliability, and long-term operational stability across mission-critical energy, utility, and industrial environments.

2. Purpose and Scope

2.1 Purpose

The purpose of this proposal is to enhance the resiliency, security, and operational continuity of critical infrastructure systems through the modernization of SCADA and operational technology (OT) environments. This initiative is designed to strengthen infrastructure reliability against cyber threats, operational disruptions, and environmental hazards while supporting secure, uninterrupted industrial operations.

The proposed effort focuses on improving infrastructure survivability, protecting industrial control systems, and establishing resilient operational frameworks capable of sustaining mission-critical services during adverse conditions. Through strategic modernization and systems hardening, the initiative aims to reduce operational risk, improve recovery readiness, and support long-term infrastructure stability.

2.2 Scope

This proposal encompasses the planning, modernization, deployment, and validation of resilient SCADA and operational technology infrastructure across designated critical infrastructure environments.
The project scope includes:

- SCADA and OT modernization
- Industrial cybersecurity enhancement
- Secure telemetry communications
- Operational continuity and resiliency planning
- Infrastructure recovery and failover readiness
- System validation and resiliency assessment

The initiative supports operational environments requiring secure, reliable, and continuously available infrastructure systems, including energy, utility, industrial, and mission-critical operational facilities.

3. SCADA Architecture Overview

The proposed SCADA architecture establishes a segmented, high-availability operational technology framework designed to support secure telemetry transmission, resilient infrastructure communications, and deterministic IT/OT boundary protection. The architecture integrates layered security controls, encrypted communications, redundant operational systems, and field-level resiliency mechanisms to support continuous mission-critical operations.

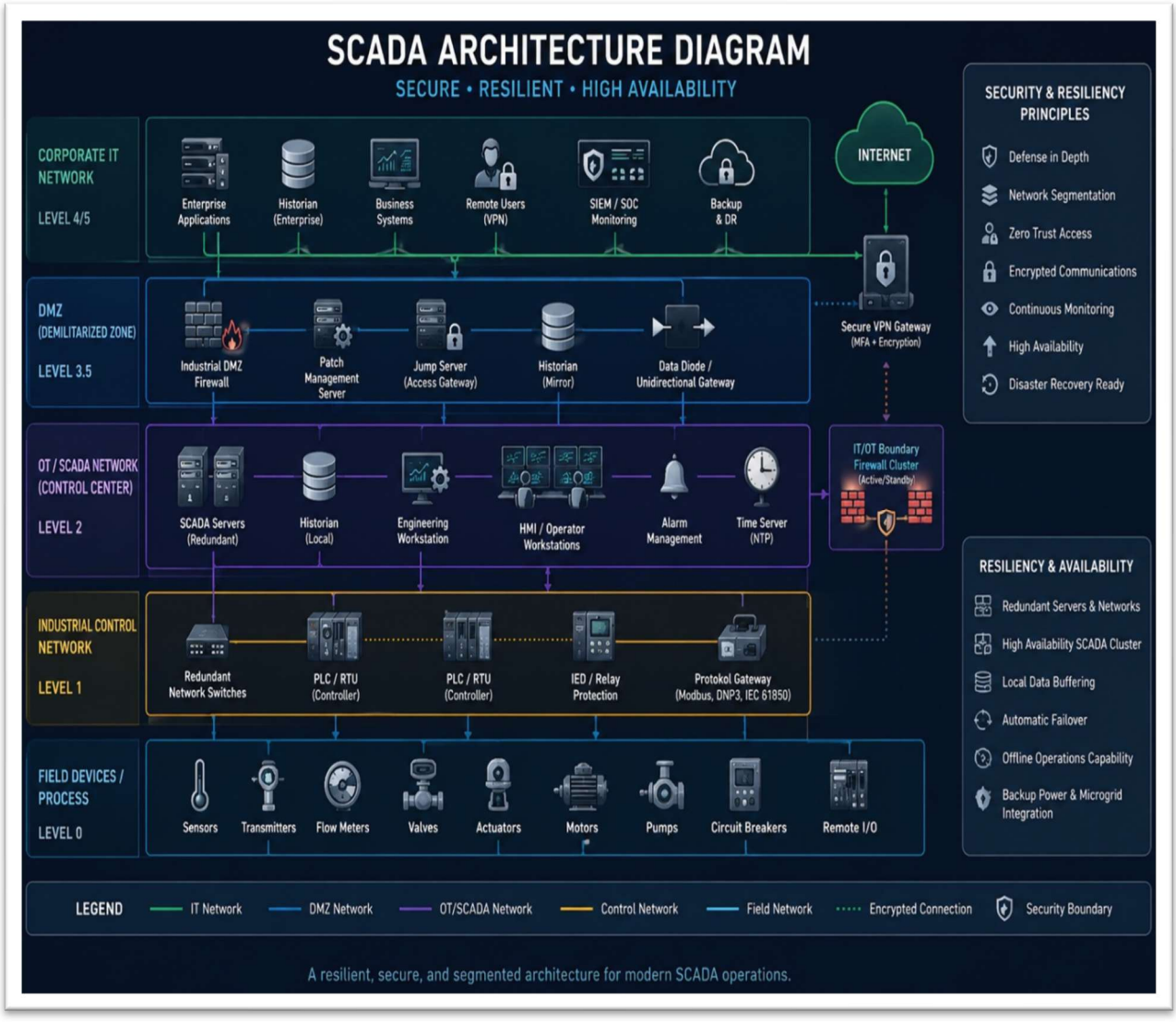

Figure 1. Proposed SCADA & Operational Technology Architecture Framework

4. Granular Technical Objectives

- **Cryptographic Protocol Encapsulation:** Replace vulnerable, clear-text protocols (e.g., standard Modbus, DNP3) with secure variations like DNP3 Secure Authentication (SAv5) and TLS-encapsulated Modbus TCP to prevent man-in-the-middle injection attacks.

- **Deterministic Boundary Protection:** Enforce unidirectional security gateways (data diodes) at critical IT/OT boundaries, allowing outbound telemetry to reach data warehouses while physically preventing inbound network traversal.

- **Autonomous Microgrid Survivability:** Field-deploy dedicated lithium-iron-phosphate (LiFePO4) industrial battery arrays paired with off-grid photovoltaic charging circuits at isolated remote terminal units (RTUs), ensuring 72 hours of complete telemetry independence.

- **Signatureless Behavioral Telemetry:** Deploy network-tap-based anomaly detectors executing unsupervised machine learning on raw packet streams to capture unauthorized register-writes or configuration deviations without relying on traditional, easily bypassed signature lists.

5. Four-Phase Execution Matrix

5.1 Phase 1: Deep Asset & Protocol Inventory (Months 1–3)
Perform passive traffic analysis to discover undocumented sub-networks, compile a complete hardware registry of aging programmable logic controllers (PLCs), and map baseline data-flow topologies.

5.2 Phase 2: Perimeter Boundary Isolation (Months 4–6)
Physically dismantle shared corporate-OT routing paths. Install hardware-enforced data diodes at essential boundaries and deploy multi-factor authentication (MFA) on micro-segmented, internal engineering workstation zones.

5.3 Phase 3: Cryptographic Hardware Field Deployment (Months 7–9)
Swap obsolete legacy controllers for modern, hardware-encrypted PLCs.

Mount ruggedized, inline encryption appliances to secure serial communication lines over long-distance radio or fiber links.

5.4 Phase 4: Adversarial Validation & Incident Drills (Months 10–12) Conduct controlled red-team physical and digital penetration testing to confirm boundary strength. Train field operators using live, simulated network-outage and failover recovery scenarios.

6. Itemized Strategic Budget

The comprehensive capital requirement for this complete system overhaul is structured below:

Structural Allocation	Investment	Exact Engineering Purpose
Cryptographic Edge Infrastructure	$320,000	Ruggedized PLCs supporting DNP3 SAv5, hardware security modules (HSMs), and secure edge communication gateways.
OT Network Engineering Specialists	$180,000	Dedicated third-party industrial control systems (ICS) architects to execute deterministic segmentation and firewall provisioning.
Physical Isolation & Microgrid Hardening	$150,000	Unidirectional data diodes, localized LiFePO4 battery enclosures, and weatherized solar recharging assemblies for remote field units.
Red-Team Auditing & Workforce Resiliency	$100,000	Independent verification testing, regulatory alignment mapping, and immersive operational sandbox simulation training for field technicians.
Total Grant Funding Requested	**$750,000**	**Total capital investment required for complete infrastructure transformation.**

7. Measurable Resilience Metrics

- **Zero Lateral Threat Contamination:** Eradication of potential IT-to-OT compromise vectors via deterministic, unidirectional physical boundaries.

- **Packet Invariance:** Absolute encryption of all command-and-control telemetry across internal networks, verified via deep-packet inspection auditing.

- **Uninterrupted Field Visibility:** 100% telemetry availability during major power infrastructure failures, sustained by self-contained microgrid elements.

8. Authoritative Sourcing & Regulatory References

- **CISA Infrastructure Resilience Planning Framework (IRPF):** National guidance utilized to establish baseline risk matrices and ensure a holistic defensive posture against multi-hazard events.
    - *Resource Guide:* https://cisa.gov

- **Claroty Industrial Cybersecurity Frameworks:** Industry-standard technical concepts referenced for optimizing OT-specific threat hunting, network micro-segmentation boundaries, and SCADA risk mitigation strategies.
    - *Technical Analysis:* https://claroty.com

DURAND PORTER


Salt Lake City, UT, US, 84107


durandmporter@gmail.com


+1 8056378355