Cyber Security Stack

Cyber Security Stack:

Resonance Protocol

The Resonance Protocol for Critical National Infrastructure (CNI): Securing SCADA and Utility Control Environments Against Physical and Logical Tampering

Executive Summary

Critical national infrastructure (CNI) such as electricity, water, and gas networks depend on highly distributed supervisory control and data acquisition (SCADA) systems that bridge information technology (IT) and operational technology (OT). These environments, while operationally resilient, remain vulnerable to tampering, particularly when an adversary gains physical or engineering access to control assets.

The Resonance Protocol (RP) introduces a cryptographic integrity framework that allows systems within such environments to self-attest, verify peers, and autonomously isolate compromised components without relying on heuristic or behavioural indicators. Originally conceived as a universal model for digital trust across system layers, the protocol's layered hive architecture, Merkle-based integrity chains, and trust contract mechanism make it uniquely applicable to the challenges faced by national grid operators.

By embedding RP within substations, gateways, and control centres, operators gain a deterministic, verifiable view of their entire operational topology. Each device, whether a programmable logic controller (PLC), intelligent electronic device (IED), or SCADA master, cryptographically validates its internal state and forms time-bound, conditional trust relationships with adjacent systems. When a device's configuration, firmware, or logic changes (whether through authorised update or tampering), its cryptographic signature alters, automatically revoking its trust status and quarantining its network privileges until re-attested.

This whitepaper outlines how the Resonance Protocol can be applied within national grid and SCADA environments to protect against both remote and physical manipulation, aligning with cyber resilience objectives under frameworks such as the NCSC Cyber Assessment Framework (CAF), IEC 62443, and NIST 800-82.

Background Reading: Core Concepts from Existing Whitepapers

The Resonance Protocol has been detailed extensively in three preceding technical papers:

1. **Whitepaper 1: Overall Architecture** – Introduced the foundational model of system self-attestation, layered Merkle integrity, and scoped trust negotiation between systems.
2. **Whitepaper 2: Subsumption Hive** – Described how each system internally validates its component layers to build a cryptographic chain of integrity from the hardware upward.
3. **Whitepaper 3: Adjacent Hive** – Outlined the inter-system trust contract mechanism, where systems exchange signed state proofs and automatically revoke trust upon any integrity divergence.

The following summarises these principles as they apply to the utilities sector.

Overview of the Resonance Protocol

The RP model treats every digital system as a hive composed of nested layers, hardware, firmware, kernel, process, and application. Each layer generates a cryptographically signed hash of its immutable components. These are combined into a Merkle tree, producing a unique root hash that represents the entire system's state. Any change, however minor, propagates through the tree and invalidates the root, immediately signalling an integrity deviation.

Subsumption Hive Model

A subsumption hive represents this internal structure. Each layer attests to the one below it, creating an ascending chain of trust from hardware to application. The relationship is recursive, allowing any compromised layer to be detected deterministically. This design ensures that no single layer can falsify its state without detection by its parent.

Adjacent Hive Model

Separate systems, or adjacent hives, establish communication through trust contracts, signed, scoped, and time-bound digital agreements containing verified Merkle roots, allowed boundaries, and communication policies. Contracts expire or are revoked when either party's root hash changes, guaranteeing that only verified systems can maintain operational trust.

These mechanics form the foundation of RP's self-healing, self-isolating security paradigm, crucial for environments where downtime and false positives carry national-scale consequences.

Sector Context: SCADA and Nation Grid Landscape

National grids rely on SCADA environments that integrate field devices, substations, and central control rooms into a unified operational ecosystem. While segmented and layered by design, the convergence of IT and OT domains introduces new threat surfaces:

- Physical access to substation systems or remote cabinets enables configuration tampering, firmware swaps, or relay mis-settings.
- Engineering laptops with dual connectivity (corporate and OT) can introduce malicious updates or altered project files.
- Legacy devices often lack secure boot, cryptographic signing, or integrity verification mechanisms.
- Low-bandwidth and air-gapped systems limit traditional endpoint monitoring and detection capabilities.

Traditional security models, focused on network segmentation, whitelisting, and anomaly detection, do not prevent a trusted device from becoming malicious once compromised. RP directly addresses this limitation by embedding trust as a measurable and revocable state within the control fabric itself.

Applying the Resonance Protocol to Utilities Environments

Hive Representation for SCADA Assets

Each asset within the SCADA ecosystem is represented as an independent hive:

Asset Types	Hive Layers	Integrity Scope
IEDs / Relays / PLCs	Bootloader → Firmware → Logic → Configuration	Settings, binaries, communication tables
RTUs / Gateways	OS → Drivers → Protocol Stacks → Routing Rules	Network policies, serial/Ethernet mappings
HMIs / Engineering Workstations	OS → Runtime → Project Files → User Profiles	Visualisation, control logic, and access layers
Control Centre Servers	OS → Applications → Data Stores → Service Configs	SCADA, EMS/DMS, historian services

Each hive performs local hashing and produces a Merkle root signature. This signature is stored and optionally transmitted to peer systems or a control controller for verification.

Substation-Level Subsumption

At the substation level, all device hives form part of a parent (subsuming) hive. The substation's Merkle root is derived from its constituent devices, relays, IEDs, gateways, and HMIs.

If any device's integrity shifts, the substation's root automatically changes, enabling high-level visibility of localised tampering without direct polling of every asset.

Establishing Adjacent Hive Trust Across the Grid

Adjacent hives represent communication between substations, control centres, or regional grid nodes. Each connection is governed by a trust contract containing:

- Signed Merkle roots from both parties
- Connection scope and permitted command types
- Time-to-live (TTL)
- Revocation policy

When either party's Merkle root changes (indicating possible tampering or authorised maintenance), the trust contract is invalidated and all associated communication ceases until both sides re-attest.

This model guarantees that only verified systems participate in operational control, eliminating reliance on external intrusion detection or heuristic monitoring.

Physical Access Tamper Response and Deterministic Isolation

A defining strength of the Resonance Protocol in SCADA environments is its ability to counter physical manipulation.

Scenario:
An attacker gains physical access to a protection relay or PLC within a substation and uploads modified logic or changes a protection setting.

RP Response:

1. The device recalculates its layer hashes and detects a root mismatch.
2. The hive's integrity state changes to *Unhealthy*.
3. Any active trust contract between the device and its parent gateway or controller is automatically revoked.
4. The device's control communication channels are blocked, while read-only telemetry may continue to ensure grid stability.
5. A tamper report is generated locally and synchronised upstream when connectivity resumes.
6. Restoration requires re-attestation and signature approval from an authorised engineer.

The process is deterministic and independent of behavioural analytics, eliminating the ambiguity that often hinders rapid decision-making in OT incident response.

Low Connectivity or Air-Gapped Operations

Utilities often operate with intermittent or minimal network connectivity. RP supports two complementary operational modes:

- **Passive Mode:** Devices operate autonomously, performing periodic self-attestation and storing tamper logs locally. These can be retrieved by an authorised gateway or maintenance tool.
- **Active Mode:** Connected devices maintain live trust contracts with peers or controllers, supporting immediate detection, isolation, and re-attestation events.

The transition between passive and active modes is seamless, preserving deterministic integrity assurance even when systems are isolated or temporarily disconnected.

Governance and Attestation Workflows

A core tenet of RP is to ensure that legitimate maintenance and updates do not trigger false isolation.

Authorised Change Windows

Before performing configuration or firmware updates, authorised engineers submit a signed update manifest defining expected state changes and validity period.

Re-Attestation

Once maintenance concludes, the affected hive recomputes its Merkle root. The controller verifies this against the manifest and, upon approval, reinstates trust contracts.

Immutable Audit Chain

Every Merkle root, signature, and attestation event is logged and chained cryptographically, producing a tamper-proof operational record. This enables forensic investigation, compliance auditing, and evidence for regulatory frameworks such as CAF.

Governance and Attestation Workflows

When trust contracts are revoked due to detected tampering, the response is policy-driven according to device criticality:

Asset Class	Isolation Policy	Recovery Path
Protective Relays / Safety IEDs	Freeze configuration; block writes; maintain trip logic	Re-attest post verification
RTUs / Gateways	Disable command traffic; maintain telemetry	Manual re-attestation
HMIs / Engineering Workstations	Disable network interface; revoke credentials	Reimage and re-attest
Control Servers	Segregate from orchestration plane; switch to read-only mode	Controller-approved re-attestation

This ensures safety and availability are prioritised while enforcing absolute integrity.

Integration with Security Operations

The RP model integrates naturally with a Cyber Defence Operations or SOC framework.

Tamper alerts, revoked trust contracts, and re-attestation logs can be ingested by SIEM platforms, correlating deterministic integrity events with broader network and endpoint telemetry.

Key advantages include:

- **Deterministic alerts:** Zero false positives from behavioural anomalies.
- **Autonomous isolation:** Devices self-contain before lateral propagation.
- **Cross-layer visibility:** SOC analysts can correlate cryptographic drift with process anomalies.
- **Forensic depth:** Immutable audit logs support post-incident verification and regulatory reporting.

By fusing RP telemetry with SecOps observability, utilities gain continuous assurance that their physical and digital control fabric remains uncompromised.

Conclusion

As the convergence of IT and OT continues to accelerate, the boundary between cyber and physical risk has become inseparable. Traditional defences, segmentation, monitoring, and patch management, address only symptoms. The Resonance Protocol introduces a first-principles approach, establishing cryptographic truth as the foundation of operational trust.

By applying the Resonance Protocol across SCADA and national grid environments, utilities can:

- Achieve deterministic detection of unauthorised change, whether remote or physical.
- Contain compromise automatically through self-revoking trust.
- Maintain operational safety while ensuring regulatory compliance and auditability.

The result is a measurable, enforceable trust fabric across all operational layers, where every device, from relay to control centre, proves its integrity before it participates in control.

This capability transforms CNI resilience from reactive monitoring to proactive, mathematically verifiable assurance, aligning the nation's most critical systems with the cyber-physical realities of modern threat landscapes.