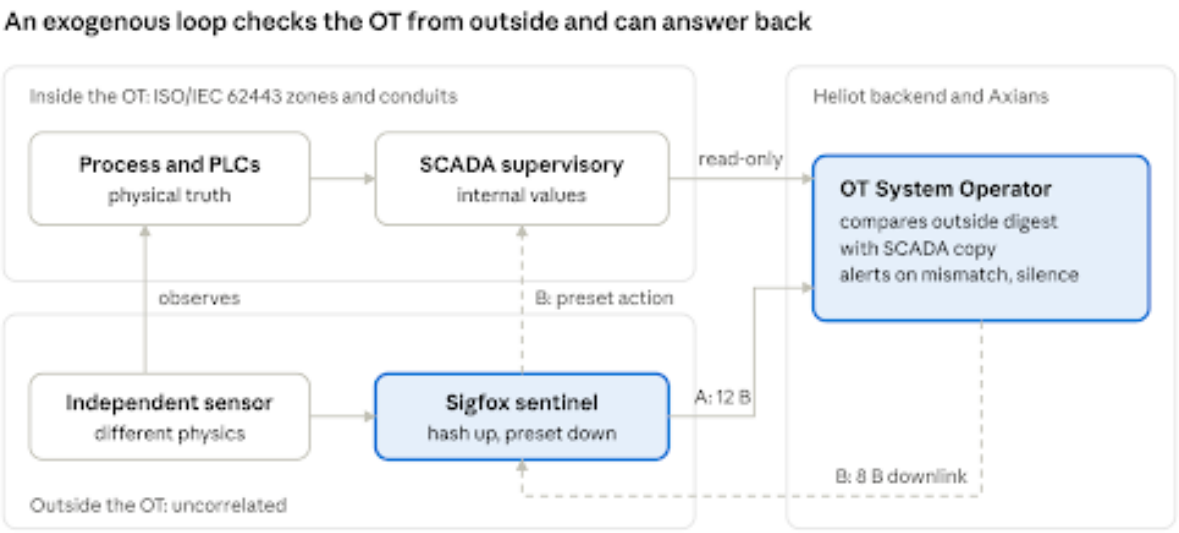
Out-of-Band Telemetry in OT Systems

ISO/IEC 62443 Security Level 3 & 4 System Requirements
Sigfox 0G as an Exogenous Guardrail for Industrial Control Systems

Architectural Diversity, Cybernetics, and Out-of-Band Physical Validation for High-Assurance Industrial Environments

October 2026

1. Executive Summary 2
2. System Requirements for Security Levels 3 and 4 (ISO/IEC 62443) 3
3. Systems-Cybernetic Analysis of Internal Security Controls 6
4. Sigfox 0G as an Exogenous, Uncorrelated Guardrail 7
5. Regulatory Positioning, Compliance, and Deployment Architectures 12
6. Operational Boundaries & Addressing Expert Objections 15
7. Conclusion & Strategic Roadmap 19



1. Executive Summary

Modern industrial automation relies on the convergence of Information Technology (IT) and Operational Technology (OT). While this integration enables real-time data analytics, enterprise resource optimization, and automated remote management, it exposes physical infrastructure to sophisticated cyber threats. Industrial Cybersecurity Management Systems (ICMS) built around standards such as ISO/IEC 62443 enforce multi-layered defenses. However, a fundamental architectural vulnerability remains: every security measure mandated by traditional frameworks lives inside the system it protects.

When an Industrial Control System (ICS) relies exclusively on internal controls—such as firewalls, intrusion detection systems (IDS), deep packet inspection (DPI), and cryptographic key infrastructure—it creates a single point of epistemic failure. If an advanced persistent threat (APT) or an autonomous, self-propagating AI worm compromises the underlying operating systems, hypervisors, or identity providers, the defense mechanisms are compromised alongside the operational processes.

This white paper presents a systems-cybernetic framework for securing critical OT infrastructure at ISO/IEC 62443 Security Levels 3 and 4 (SL 3 and SL 4). It introduces Sigfox 0G ultra-narrowband (UNB) technology as an exogenous, structurally uncorrelated guardrail. Operating outside the IP stack, software supply chains, and local network infrastructure, Sigfox 0G establishes an independent, out-of-band telemetry verification mechanism. Functioning as an exogenous diagnostic safeguard layer and structural risk treatment addressing the immanence trap, 0G couples out-of-band physical reality checks (Exogenous Upstream Verification) with optional, highly constrained downstream configuration profile updates. This allows industrial operators to achieve true architectural diversity and defend against zero-day exploits, insider threats, and machine-speed lateral movement without introducing operational latency, regulatory non-compliance, or dangerous remote control overrides.

2. System Requirements for Security Levels 3 and 4 (ISO/IEC 62443)

2.1 Overview of ISO/IEC 62443 Framework & Security Level Definitions (SL 1 to SL 4)

The ISO/IEC 62443 series provides a comprehensive framework designed specifically to address the unique availability, safety, and operational constraints of Industrial Automation and Control Systems (IACS). Unlike general IT cybersecurity frameworks centered on data confidentiality, ISO/IEC 62443 prioritizes physical safety, operational availability, and process integrity.
The standard is organized into four core categories:

- **General (Part 1-x):** Defines foundational concepts, terminology, metrics, and reference models.
- **Policies & Procedures (Part 2-x):** Outlines requirements for establishing an Industrial Cybersecurity Management System (ICMS), patch management, incident response, and third-party risk management.
- **System (Part 3-x):** Defines system-level technical security requirements, risk assessment methodologies, and the Zone and Conduit architecture.
- **Component (Part 4-x):** Specifies secure product development lifecycles (Part 4-1) and technical security requirements for individual IACS components like PLCs, RTUs, and HMIs (Part 4-2).

ISO/IEC 62443 defines four discrete Security Levels (SL) representing the resilience of a system against specific threat capabilities:

Security Level	Threat Capability & Motivation	Technical Focus & Operational Context
SL 1	Protection against casual or coincidental violations.	Basic access control, hygiene, and resistance to opportunistic, unguided errors.
SL 2	Protection against intentional violations using simple means with low resources.	Standard perimeter defenses, basic user authentication, and network segmentation.
SL 3	Protection against intentional violations using sophisticated means with moderate resources.	Multi-factor authentication, cryptographic verification, zone isolation, and active intrusion monitoring.
SL 4	Protection against intentional violations using sophisticated means with extended resources (e.g., state actors, AI worms).	Comprehensive defense-in-depth, zero-trust micro-segmentation, physical isolation, and resilient out-of-band controls.

2.2 Technical and Architectural Requirements for SL 3 and SL 4 Defense-in-Depth

Achieving compliance at SL 3 and SL 4 requires rigorous implementation of seven Foundational Requirements (FRs) set forth in ISO/IEC 62443-3-3:

1. **Identification and Authentication Control (IAC):** Mandatory multi-factor authentication (MFA) for all human users and cryptographic device-level identity verification for all hardware nodes (e.g., IEEE 802.1AR 802.1X certificates).
2. **Use Control (UC):** Strict role-based access control (RBAC) enforcing least privilege across human operators, software applications, and automated supervisory scripts.
3. **System Integrity (SI):** Cryptographic verification of software and firmware binaries, secure boot mechanisms, and continuous monitoring of operating memory to prevent unauthorized execution.
4. **Data Confidentiality (DC):** Encryption in transit and at rest in non-trusted segments.
5. **Restricted Data Flow (RDF):** Strict enforcement of network segmentation through physical air-gaps, stateful firewalls, and deep packet inspection (DPI) conduits.
6. **Timely Response to Events (TRE):** Continuous logging, real-time Security Information and Event Management (SIEM) integration, and automated anomaly detection.
7. **Resource Availability (RA):** Redundant hardware control loops, denial-of-service (DoS) protection, and degraded-mode operating capability to preserve physical safety

2.3 Zone & Conduit Segmentation, Cryptographic Controls, and Access Management

The structural core of ISO/IEC 62443-3-3 is the **Zone and Conduit model**. Assets with shared operational functionality and risk profiles are grouped into logical or physical Zones. Communication between different Zones must pass exclusively through designated **Conduits**, which inspect, filter, and authorize traffic flows.

In SL 3 and SL 4 environments, Conduits must enforce cryptographic protection. Data passing across conduits relies on the following mathematical primitives:

- **Asymmetric Cryptography:** Elliptic Curve Cryptography (ECC, such as ECDSA or Ed25519) and RSA for identity verification, digital signatures on control frames, and key exchange.
- **Symmetric Encryption:** Advanced Encryption Standard (AES) in Galois/Counter Mode (AES-GCM-256) or ChaCha20-Poly1305 to ensure confidentiality and payload integrity.
- **Cryptographic Hashing & MACs:** SHA-256, SHA-3, and Hash-based Message Authentication Codes (HMAC) to prevent message tampering and replay attacks.
- **Key Exchange Protocols:** Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) for perfect forward secrecy during session initialization.

2.4 The Four Critical Attack Surfaces in Modern IT/OT Converged Environments

Despite stringent ISO/IEC 62443 controls, modern converged industrial environments exhibit four primary attack vectors where internal defenses are vulnerable to advanced threats:

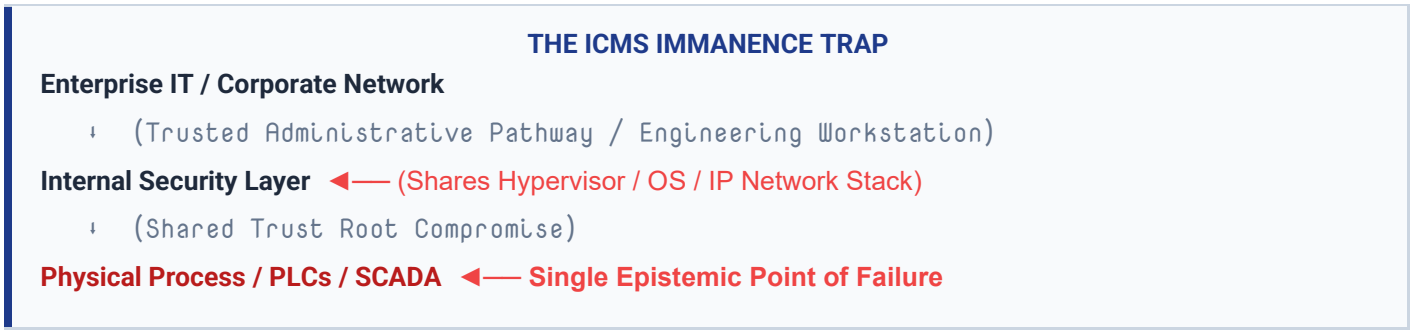
THE FOUR CRITICAL ATTACK SURFACES	
1. IT/OT Boundary & EWS	Software supply chain risks, administrative session hijacking, trusted conduits.
2. Encapsulated Legacy Protocols	Modbus TCP, PROFINET wrapped in TCP/IP; unauthenticated application layer.
3. Vendor Access & Portals	Cellular IoT gateways, remote VPNs, maintenance backdoors bypassing perimeters.
4. Edge IIoT & Smart Sensors	Low-power field hardware lacking heavy TLS/X.509 cryptographic validation.

1. **IT/OT Convergence Boundary & Engineering Workstations:** Engineering Workstations (EWS) run programming suites capable of pushing logic updates directly to Programmable Logic Controllers (PLCs). An automated AI worm infiltrating the corporate IT environment can hijack legitimate, pre-authenticated EWS sessions to modify control logic while bypassing firewalls.
2. **Ethernet-Encapsulated Legacy Protocols (The "Envelope vs. Letter" Gap):** Legacy industrial fieldbuses (e.g., Modbus, Profibus) have been adapted for modern IP networks by encapsulating industrial commands within standard Ethernet and TCP/IP frames (e.g., Modbus TCP, PROFINET). Standard network security inspects the TCP/IP "envelope," but the underlying "letter" (the application command) lacks native authentication. Once inside the conduit, an attacker can send unauthorized write commands that PLCs execute without verification.
3. **Third-Party Vendor Access & Maintenance Portals:** Original Equipment Manufacturers (OEMs) often require dedicated remote access (VPNs or cellular modems) for diagnostics and maintenance. Compromising a third-party vendor network grants direct access to internal OT conduits, bypassing perimeter controls.
4. **Edge IIoT Devices & Smart Sensors:** Resource-constrained edge sensors and Internet of Things (IoT) gateways frequently lack the memory and compute capacity needed to execute full TLS handshakes or x.509 certificate checks at line rate. Attackers can compromise these edge nodes to spoof operational telemetry, feeding manipulated data to SCADA historians.

3. Systems-Cybernetic Analysis of Internal Security Controls

3.1 The Immanence Trap of Industrial Cybersecurity Management Systems (ICMS)

From a systems-cybernetic perspective, traditional ICMS architectures suffer from an **immanence trap**. An immanent system is one whose governance mechanisms rely on the same internal structures, trust models, and execution pathways as the processes they regulate.



In an industrial plant, the intrusion detection software, log collectors, security agents, and core SCADA software share the same host hardware, hypervisors, and TCP/IP network interfaces. When a sophisticated adversary gains root-level privilege or exploits zero-day vulnerabilities in the hypervisor or network hardware, the security monitoring layer loses its integrity. The system cannot evaluate its own state because the observer is compromised alongside the observed process.

3.2 The Asymptotic Cost and Latency of Internal Reinforcement

To address the immanence trap, traditional security engineering adds more internal controls: deeper packet inspection, heavier endpoint detection and response (EDR) software, encrypted conduits, and continuous logging. However, this internal reinforcement strategy hits diminishing returns:

- **Computational Latency:** Real-time industrial automation requires deterministic performance, with control loops executing in sub-millisecond windows. Running deep packet inspection or heavy cryptographic handshakes on resource-constrained embedded PLCs introduces jitter and latency, impacting operational reliability.
- **Expanded Attack Surface:** Adding complex security software increases code volume and deployment complexity. Security platforms themselves become targets for zero-day exploits, administrative credential theft, and supply chain contamination.
- **Operational Friction:** Stricter internal controls increase management overhead, making maintenance, patch updates, and emergency interventions more complex.

3.3 Epistemological Asymmetry: Distinguishing Nominal Operation from False/Confirmed Deviations

An internal security layer must evaluate process data against internal baselines. This introduces an epistemological burden where the system must classify all state observations into four distinct operational quadrants:

	REALITY: NOMINAL	REALITY: COMPROMISE
OBSERVATION: NOMINAL	**CONFIRMED POSITIVE** System correctly validated nominal state.	**FALSE POSITIVE** Operational friction; misidentified normal operation.
OBSERVATION: ANOMALOUS	**FALSE NEGATIVE** Stealth vector bypasses internal detection.	**CONFIRMED NEGATIVE** Known attack successfully identified.

1. **Confirmed Positive (Nominal Operation):** The physical process is running within normal parameters, and security tools correctly report nominal operation.
2. **False Positive (Operational Friction):** A legitimate process adjustment or temporary load surge is flagged as an attack, causing unnecessary plant trips, alarm fatigue, and lost production.
3. **False Negative (Stealth Attack Vectors):** An attacker or AI worm tampers with physical setpoints while altering telemetry sent to the SCADA display. The internal monitor reports nominal operation while physical damage occurs.
4. **Confirmed Negative (Detected Attacks):** The system accurately identifies an attack and blocks it.

Relying exclusively on internal telemetry creates epistemic fragility. If the internal monitoring network is blinded, the system cannot distinguish between a Confirmed Positive state and a stealthy False Negative exploit.

4. Sigfox 0G as an Exogenous, Uncorrelated Guardrail

4.1 Conceptual Architecture: Breaking the Immanence Loop with Architectural Diversity

To overcome the immanence trap, industrial architectures require an **exogenous guardrail**—a control layer that operates outside the system's internal network stack, identity providers, and software supply chains.

EXOGENOUS 0G GUARDRAIL ARCHITECTURE

Physical Process / Equipment

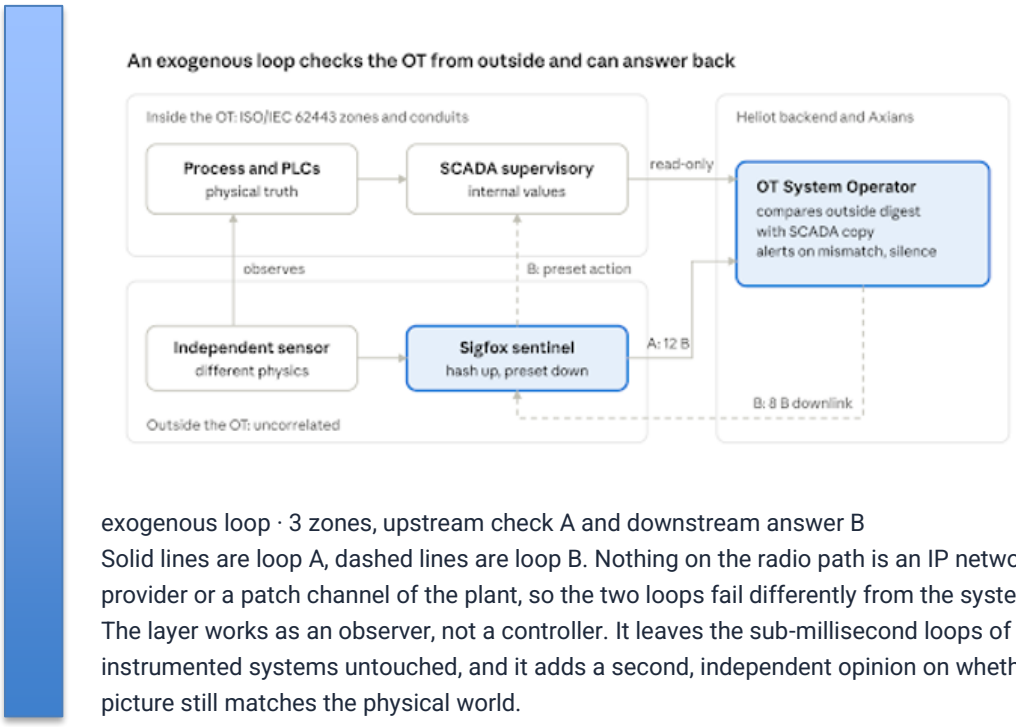
Primary Path (Internal)	**Guardrail Path (Out-of-Band)**
Internal Bus / Modbus / IP	Physical Sensor Layer
SCADA / Internal ICMS	**Sigfox 0G Sentinel Hardware**
↓ (Read-Only State Copy)	↓ (12-Byte Uplink / UNB Radio)

SUPERVISORY VERIFIER

Compares primary SCADA digest against 0G exogenous digest

↓ Optional Downlink (8 Bytes -> Profile Selector)

Sigfox 0G provides this exogenous layer. It operates as an independent, ultra-narrowband (UNB) wireless network using sub-GHz license-free ISM bands. Because Sigfox 0G does not use standard IP routing, cellular network cores, or shared local Ethernet infrastructure, it remains completely uncorrelated from the plant's internal IT/OT environment. A total compromise of the plant's corporate network, domain controllers, and internal security gateways leaves the Sigfox 0G radio path unaffected.



exogenous loop · 3 zones, upstream check A and downstream answer B

Solid lines are loop A, dashed lines are loop B. Nothing on the radio path is an IP network, an identity provider or a patch channel of the plant, so the two loops fail differently from the system they watch. The layer works as an observer, not a controller. It leaves the sub-millisecond loops of PLCs and safety instrumented systems untouched, and it adds a second, independent opinion on whether the supervisory picture still matches the physical world.

4.2 Exogenous Upstream Verification (Out-of-Band State Validation) & Optional Profile Updates
The Sigfox 0G guardrail centers entirely on out-of-band physical status monitoring, with optional downstream configuration tuning completely decoupled from critical control loops:

- **Exogenous Upstream Verification (Out-of-Band State Validation):**
    a. An independent sentinel device is attached directly to the physical process using sensors that operate on different physical principles than the main SCADA instrumentation (e.g., optical counters, external current transformers, acoustic sensors).
    b. The sentinel collects raw sensor values and hashes them into a 12-byte status digest.
    c. This digest is transmitted over the Sigfox 0G network directly to a cloud or local private verifier.
    d. The verifier compares the exogenous digest with a read-only copy of the telemetry reported by the primary SCADA system.
    e. If a discrepancy is detected between physical state measurements and internal SCADA reports, an alert is triggered immediately.
- **Optional Downlink Parameter Tuning (Profile Selector):**
    a. To prevent the systemic safety and security risks associated with remote interdiction mechanisms or killswitches, downstream communication is strictly optional and explicitly forbidden from executing direct physical overrides or plant trips.
    b. If downstream capabilities are utilized, an 8-byte downlink frame is transmitted exclusively during scheduled windows following an uplink transmission.
    c. The 8-byte payload contains a preset profile selector and dynamic verification token, serving solely to update pre-programmed sentinel configuration parameters or reporting behavior profiles (e.g., threshold sensitivity or heart-beat cadence).
    d. By restricting downstream data to passive profile configuration updates, the system guarantees process safety and preserves strict operational autonomy at the physical edge.

4.3 Payload Budget as a Security Primitive (12 Bytes Uplink / 8 Bytes Downlink) & Cyber-Inertia

The payload structure of Sigfox 0G acts as a core security feature. Strict message size limits enforce functional simplicity, ensuring Exogenous Upstream Verification remains lightweight while ruling out broad categories of cyber attacks:

UPLINK FRAME ARCHITECTURE (12 BYTES TOTAL)			
Byte 0 Profile / Msg Type	**Byte 1** Status Flags (Pass/Fail)	**Bytes 2–3** Epoch Counter	**Bytes 4–11** Truncated Hash Digest (State Signature)
DOWNLINK FRAME ARCHITECTURE (8 BYTES TOTAL)			
Byte 0 Command ID	**Byte 1** Profile Selector	**Bytes 2–7** Dynamic Verification Token (Binds Command to Epoch)	

This structural constraint provides inherent **Cyber-Inertia**:

- **No IP Stack:** The sentinel device does not support TCP/IP, UDP, HTTP, SSH, or Telnet protocols.
- **No Remote Code Execution:** An 8-byte downlink payload cannot deliver executable binaries or complex control scripts. It can only select a pre-programmed command ID from a fixed local lookup table.
- **No Over-the-Air Software Supply Chain Attacks:** Firmware cannot be updated over the Sigfox 0G radio channel. Malicious firmware updates via remote access are impossible.
- **Initiated Downlink Only:** The device cannot be called or polled externally. The radio receiver activates briefly only after an uplink transmission, closing the attack window.

4.4 Direct Mapping: How Sigfox 0G Addresses the Four Core Attack Surfaces

The exogenous guardrail directly mitigates vulnerabilities across all four primary attack surfaces:

Attack Surface	Threat Vector / AI Worm Mechanics	Sigfox 0G Exogenous Countermeasure
1. IT/OT Boundary & EWS	Compromises EWS via IT network; hijacks administrative credentials to push malicious logic directly to PLCs.	**Physical State Validation:** Unauthorized setpoint changes create an immediate mismatch between physical sensor outputs and SCADA logs. Sentinel is unreachable from EWS.
2. Ethernet Legacy Protocols	Injects unauthenticated Modbus TCP/PROFINET write commands into trusted conduits.	**Out-of-Band Process Monitoring:** Telemetry manipulation is detected at physical layer regardless of network arrival vector.
3. Vendor Access Portals	Exploits misconfigured cellular modems or remote access VPNs to enter OT network.	**Independent Air-Gap Path:** Uses dedicated radio path with zero IP routing or inbound services, preventing lateral movement.
4. Edge IIoT & Sensors	Spoofs low-level sensor telemetry sent to historians due to weak embedded cryptography.	**Dual-Measurement Verification:** Injected telemetry is caught by comparing primary sensor data against an independent physical sensor.

5. Regulatory Positioning, Compliance, and Deployment Architectures

5.1 Alignment with ISO/IEC 62443 Framework and Exogenous Guardrail Architecture

Under ISO/IEC 62443, organizations often struggle with the limitations of internal security controls. It is critical to clarify that Sigfox 0G operates entirely outside the formal System Requirements (SRs) of an ISO-compliant ICMS. Rather than functioning within the software boundary to replace or substitute standard SRs, Sigfox 0G acts as an exogenous, structurally uncorrelated guardrail. Consequently, it does not need to comply with the ISO standard itself—directly reflecting the systems-cybernetic principle of avoiding the "immanence trap" by remaining completely external to the internal system governance structures and network stacks it observes.

OT system operators formally justify and capture 0G guardrail layering across several key regulatory and engineering frameworks:

- **Security Risk Assessment & Residual Risk Treatment (ISO/IEC 62443-3-2):** During the threat modeling and risk assessment phases mandated by ISO/IEC 62443-3-2, operators evaluate high-consequence threat scenarios (such as hypervisor compromise or EWS hijacking). Sigfox 0G is documented in the risk treatment plan as an exogenous structural risk treatment that mitigates common-mode vulnerabilities across Zone and Conduit boundaries without introducing secondary software attack surfaces.
- **Independent Protection Layer (IPL) and Diagnostic Safeguard (IEC 61508 / IEC 61511):** In Layer of Protection Analysis (LOPA) and functional safety assessments, 0G is classified as an independent diagnostic safeguard layer. By utilizing distinct physical measurement principles and completely separated communication paths, 0G satisfies IPL requirements for independence, diversity, and non-interference relative to the primary basic process control system (BPCS) and safety instrumented systems (SIS).
- **Audit Scope Boundary and Exogenous Non-Interference:** Because the sentinel operates strictly as an exogenous observer outside the internal IP network stack, it provides out-of-band physical verification without expanding the auditable ICMS software boundary. Compliance auditors evaluate the primary IACS against standard SRs while recognizing 0G as an external physical validation mechanism.
- **NIS2 and CRA Alignment:** 0G provides OT operators with continuous out-of-band monitoring and supply chain risk mitigation required under the EU NIS2 Directive, while adhering to secure-by-design and minimal attack surface principles under the Cyber Resilience Act (CRA).

5.2 Supporting NIS2 Directive and Cyber Resilience Act (CRA) Compliance

The Sigfox 0G guardrail directly aligns with evolving European regulatory frameworks:

- **EU NIS2 Directive:** NIS2 requires operators of essential and important entities to implement supply chain risk management, continuous monitoring, and effective incident response. Sigfox 0G provides an independent audit trail of physical process state, proving process integrity during regulatory reviews and incident investigations.
- **EU Cyber Resilience Act (CRA):** The CRA mandates secure-by-design development and rapid vulnerability management for products with digital elements. Because Sigfox 0G sentinels use fixed firmware with no IP stack or remote code execution capability, they present a minimal attack surface and significantly reduce long-term vulnerability management overhead.

5.3 Deployment Models: Public Network Access vs. Standalone Local Private Bubbles for KRITIS

Sigfox 0G guardrails can be deployed using two distinct operational models:

DEPLOYMENT MODEL ARCHITECTURAL COMPARISON	
PUBLIC NETWORK ACCESS Distributed Public Infrastructure	**LOCAL PRIVATE BUBBLE** Air-Gapped KRITIS Installation
Sentinel Node ↓ UNB Radio Transmission **Public Base Station (Heliot Macro-Net)** ↓ Cloud API Callback **OT Verifier / Enterprise Cloud**	**Sentinel Node** ↓ Local RF Link **Private On-Premises Base Station** ↓ Isolated Local Bus **Air-Gapped Local Plant Verifier**

Deployment Feature	Public Network Access Model	Standalone Local Private Bubble
Infrastructure	Public Sigfox 0G coverage managed by Heliot.	On-premises private base stations and local backend.
Network Interface	No inbound open firewall ports or corporate VPN tunnels.	Fully air-gapped; zero connection to external networks.
Primary Target	Distributed infrastructure, municipal utilities, logistics.	Critical Infrastructure (KRITIS), military facilities, nuclear.
Geofencing	Zone-level location validation via base station reception.	High-precision indoor geofencing using local stations.
Operational Control	Managed network service delivered by Heliot.	Customer or OT provider maintains full local control.

6. Operational Boundaries & Addressing Expert Objections

6.1 Scope, Latency, and Operational Limits

To maintain technical integrity, the operational limits of the Sigfox 0G guardrail must be explicitly defined:

- **Bounded Reporting Cadence:** Sigfox 0G operates on periodic transmission schedules (typically ~140 uplinks and 4 downlinks per day). Transmission frequency is suited for process trend verification rather than continuous real-time streaming.
- **Latency Profile:** Message transmission and processing take several seconds. Downlink execution occurs during the subsequent scheduled receive window.
- **State Fingerprinting:** Loop A provides a cryptographic digest verifying state consistency. It does not replace full local forensic data logging.
- **Jamming Visibility:** While jammers can disrupt radio frequencies, the verifier expects messages on a set schedule. A missing heartbeat triggers an immediate anti-jamming alert.

6.2 Overcoming the Availability-Safety Paradox

Expert Objection:*In high-speed processes (e.g., turbine control or multi-axis motion synchronization running on sub-millisecond loops), out-of-band radio monitoring is too slow to provide real-time trip execution.*

Architectural Resolution: Exogenous Upstream Verification is a supervisory guardrail, not a replacement for deterministic Safety Instrumented Systems (SIS) or local PLC interlocks. Sub-millisecond emergency shutdowns remain under the control of local hardwired SIS hardware, while 0G provides out-of-band validation of process state.

Sigfox 0G protects supervisory continuity. It detects stealthy manipulation where an attacker alters SCADA configuration parameters or setpoints over time while tricking operators with false telemetry.

Time Scale	Layer	Primary Role
< 10 ms	Safety Systems (SIS)	Hardwired physical trip execution.
10 ms – 1 sec	PLC Logic Control	Deterministic closed-loop control.
Minutes – Hours	**Sigfox 0G Guardrail**	Exogenous supervisory state check.

6.3 Resolving the Oracle Problem via Diverse Physical Measurement

Expert Objection: *If the exogenous sentinel relies on a sensor attached to the same process, an attacker can tamper with the sensor directly, corrupting the verification loop.*

Architectural Resolution: The sentinel must use an independent physical measurement principle completely separated from the primary SCADA instrument.

PHYSICAL MEASUREMENT DIVERSITY	
PRIMARY SCADA SYSTEM (Subject to Protocol & Software Exploits)	**EXOGENOUS 0G SENTINEL** (Independent Physical Vector)
In-Line Fluid Flowmeter Communicates via Modbus TCP	**Optical Cavitation Sensor** Reads Physical Pipe Vibration
Internal PLC Bus Shared Power & Data Bus	**Split-Core Current Transformer** Measures Raw External Magnetic Field

For example, if the primary SCADA system measures pump flow using an in-line digital flowmeter connected via Modbus TCP, the exogenous sentinel uses an external optical tachometer or current transformer to measure motor shaft speed. An attacker corrupting the PLC's protocol stack or software drivers cannot spoof the physical magnetic field or light reflections measured by the independent sensor.

6.4 Regulatory & Audit Integration Strategies

6.5 Detailed Structural Advantages of 0G Architecture

The fundamental security and operational resilience of Sigfox 0G rests on several intrinsic physical and network-level properties that set it apart from traditional wireless technologies and IP-based infrastructure:

- **Anti-Jamming & Robustness:** Ultra-Narrowband (UNB) signals operate at extremely high spectral power density across license-free sub-GHz bands. Combined with spatial diversity and frequency hopping across multiple transmissions, attempting to jam a 0G signal across wide geographic areas requires infeasible amounts of RF power. Furthermore, missing scheduled heartbeats immediately convert potential RF jamming into a detected alarm condition.
- **Anti-Spoofing & Cryptographic Binding:** Transmissions use sequence-numbered payload digests bound to device-unique secret keys. Combined with physical network-level triangulation and timestamping, off-air replay attacks or message spoofing by unauthorized transmitters are inherently mitigated.
- **Cyber-Inertia:** The absolute absence of an IP stack, local network listeners, operating system layers, or over-the-air firmware updates renders sentinels immune to common remote exploits, executable injections, memory corruption, and lateral propagation vectors.
- **No Local Client Network Access Required:** 0G sentinels extract critical process and telemetry data directly over long distances indoors and outdoors without touching local client LANs, Wi-Fi, or corporate firewalls, ensuring zero expansion of the client's digital attack surface.
- **Self-Powered Autonomous Operation:** Ultra-low power consumption enables sentinels to operate completely independently of the client system's power grid for years using small coin cells, energy-harvesting capacitors, or internal batteries, guaranteeing guardrail functionality during plant power failures or intentional blackouts.
- **Public Network Macro-Diversity (2x to 4x Coverage Overlap):** Public 0G deployments feature an overlapping network topology where a single uplink frame is typically received simultaneously by 2 to 4 independent base station masts. This macro-diversity eliminates reliance on any single cell tower or hardware mast, ensuring high message delivery resilience against physical mast failures or local attacks.

When presenting Sigfox 0G to compliance auditors, organizations should follow three formal integration rules:

1. **Read-Only Verification Configuration:** Configure Exogenous Upstream Verification as a purely passive, read-only observer that pulls no power and sends no data back into the PLC bus.
2. **Strict Downlink Isolation:** If optional downstream profile updating is implemented, document that connection as a isolated configuration channel with explicit guards preventing any access to physical actuator interlocks or safety switches.
3. **Risk Treatment Documentation:** Position the system within the ICMS risk assessment framework as an exogenous structural guardrail and diagnostic safeguard that addresses common-mode failure risks, supporting overall resilience for ISO/IEC 62443-3-2, NIS2, CRA, and KRITIS without introducing internal dependencies.

7. Conclusion & Strategic Roadmap

Relying exclusively on internal security controls creates structural vulnerabilities in industrial control systems. Stacking additional security software on internal OT networks increases operational complexity, introduces computational latency, and expands the total attack surface.

Sigfox 0G offers an exogenous, uncorrelated guardrail that breaks the immanence loop. Operating outside the IP stack and internal network infrastructure, Exogenous Upstream Verification validates physical process states out-of-band without creating risks associated with remote control switches.

IMPLEMENTATION ROADMAP	
STEP 1	**Target Scenario Selection** Identify high-risk OT assets (e.g., critical pumps, remote substations).
STEP 2	**Diverse Sensor Integration** Pair SCADA nodes with sensors using distinct physical measurement principles.
STEP 3	**Digest & Behavior Catalog Specification** Define the 12-byte status digest and 8-byte action lookup table.
STEP 4	**Compliance & Legal Clearance** Document the architecture as an exogenous structural risk treatment and diagnostic safeguard.
STEP 5	**Dual Pilot Deployment** Deploy pilots on a public network site and a private bubble facility.

1. **Target Scenario Selection:** Select two high-risk operational scenarios: one public-sector distributed infrastructure site and one air-gapped critical infrastructure facility.
2. **Diverse Sensor Integration:** Specify independent sensors that measure physical realities using mechanisms distinct from primary SCADA instruments.
3. **Digest & Behavior Catalog Specification:** Define the 12-byte uplink hash structure, baseline versioning rules, and the exact lookup table of pre-authorized 8-byte downlink commands.
4. **Compliance & Legal Clearance:** Finalize regulatory positioning under ISO/IEC 62443-3-2, NIS2, and the Cyber Resilience Act, documenting the system as a formal exogenous risk treatment and independent diagnostic safeguard.
5. **Dual Pilot Deployment:** Execute pilot installations across a public network deployment and a standalone private bubble to validate heartbeat reliability, anti-jamming alerts, and anomaly detection.