Secure Industrial Radio (SIR) Certification

Whitepaper

Executive Summary

Radio-based control systems are widely used to power critical infrastructure across water, energy, and transport. Yet, unlike modern IT networks, these systems often lack enforceable cybersecurity baselines—leaving them vulnerable to replay attacks, signal spoofing, and unauthorised access.

The **Secure Industrial Radio (SIR) Certification**, developed by **Spotcom Ltd**, closes this gap. It provides a **unified, open, and testable cybersecurity assurance framework** specifically tailored to **long-range, low-bandwidth, and legacy industrial radio systems**.

SIR introduces a **three-tier certification model**—from Basic to Advanced protection—helping operators verify and improve the resilience of both legacy and modern deployments that underpin the critical infrastructure we all rely on.

Wireless Solutions and Support Services
www.SpotcomLtd.co.uk
+44 (0)1329 448161

Everyday Insecurity, High-Stakes Consequences

Radio signals are everywhere. From the devices that open our **garage doors** to the **key fobs unlocking vehicles**, the **RFID tags granting gated access**, and the **Bluetooth sensors embedded in homes and workplaces**, wireless convenience is part of everyday life.

But convenience often comes at a cost:

- **Garage doors** – vulnerable to brute-force and replay attacks, especially older static-code models.
- **Vehicle key fobs** – pre-2015 designs are still exposed to replay and relay theft.
- **Gated access systems** – often unencrypted, enabling signal cloning or brute-force entry.
- **Bluetooth devices** – susceptible to spoofing, hijacking, and keylogging if weak pairing is used.
- **RFID tags** – easily cloned or duplicated with basic consumer hardware.

These vulnerabilities are widely documented, regularly demonstrated with readily available hardware, and, in many cases, remain unresolved.

While certain consumer systems now fall under fragmented standards (e.g. ISO/SAE 21434 for automotive, ISO/IEC 14443 for RFID, Bluetooth LE Secure Connections), they are **inconsistently applied** and often focused on **safety and emissions rather than cybersecurity**. For example, many garage doors and gate controllers still rely on **fixed or outdated rolling codes** that can be bypassed with minimal effort.

Meanwhile, **industrial radio systems controlling far more critical processes**—such as chlorine dosing in water treatment plants, floodgate and sluice operations, emergency turbine shutdowns in energy facilities, railway signalling switches, and even remote activation of fuel pumps or chemical injection valves—**often operate without any enforceable security baseline.**

SIR Certification directly addresses this gap, offering a **practical, scalable framework** to secure the radio infrastructure that underpins critical sectors such as **water, energy, and transport**.

Applications in Critical Infrastructure

Radio remains a prime choice for critical infrastructure because it can operate in **complete isolation from public or third-party networks**. Unlike cellular systems (3G/4G/5G) that rely on external base stations and shared infrastructure, licensed or license-free industrial radios are **fully operator-controlled**—providing resilience against outages and upstream dependencies.

Private Industrial Radio

Operator Controlled – No dependency on external providers.
Fully Isolated – Operates even if public networks fail.
Deterministic Latency – Predictable response times for safety-critical systems.
Licenced or Licence-free Spectrum – Dedicated and less congested.
Proven for Decades – Widely deployed in Water, Energy and Automation.
Security – Military-grade Encryption, repeat/replay attack protection. (model /manufacturer specific)

Range Limitations – Typically 40 miles per hop (terrain dependant); repeaters may be needed.
May be Susceptible to Local Jamming – Though usually limited to line-of-sight attackers.

Cellular (3G/4G/5G)

Broad Coverage – Works anywhere with carrier service.
Quick Deployment – No need for Custom RF planning.
Wide Ecosystem – Many IoT-ready modems and hardware options.
Initial Costs - Cellular Modems are relatively inexpensive to purchase.

Relies on External Networks – Outages or carrier issues can disrupt service.
Shared Infrastructure – Competes with public users, can suffer congestion.
Variable Latency – Can spike unpredictably under load.
Service Lifecycle Changes – 3G withdrawal, spectrum reallocation risks.
Higher Costs – Ongoing SIM and Carrier fees exceed simple radio licence.
Security – Internet-connected, globally interceptable and, also vulnerable to local jamming.

This makes radio ideal for applications where **deterministic, low-latency control** is required: relatively

- **Water & Wastewater**
  - Pump controls, chemical dosing, flow and level monitoring, leak detection, smart metering.
- **Energy & Utilities**
  - Substation automation, emergency turbine shutdowns, transformer monitoring, renewable energy telemetry.
- **Transport & Signalling**
  - Rail signalling, traffic lights, bridge/tunnel sensors, public transit communications.
- **Oil, Gas & Environmental**
  - Pipeline monitoring, wellhead control, tank farm management, gas leak detection.

However, the **same isolation that makes radio attractive also means it's overlooked by mainstream IT security standards**—creating a blind spot that SIR Certification is designed to address.

SIR Certification Framework

The Hidden Radios in Your Network

Many operators are unaware they even have radios embedded in their infrastructure. Often installed by contractors decades ago, these devices silently connect pumps, valves, and sensors to control rooms, operating “out of sight and out of mind.”

In one UK water utility, a routine SCADA upgrade revealed **UHF telemetry radios from the 1990s** still controlling chlorine dosing pumps. They were completely undocumented, unencrypted, and absent from asset registers—yet critical to the site’s operation.

This is why SIR Certification begins with a simple **Level 1 self-assessment**, helping operators first identify what radios they have before addressing their security posture.

The SIR Certification Framework is a progressive three-tier model, from basic protections for legacy systems to advanced assurance for critical deployments:

Level 1 Basic Protection	• Unique Device IDs • Default Password Change • Basic Access Control • Fail-safe Defaults
Level 2 Intermediate Protection	• AES-128/256 Encrypted RF Payloads • HMAC Integrity Checks • OTA Firmware Updates • Replay Mitigation
Level 3 Advanced Protection	• Full Origin Authentication with Digital Signatures • Automated Key Rotation/Revocation • Whitelisting & ACLs • Secure OTA Updates

This tiered approach ensures **even legacy systems can make incremental improvements**, while modern deployments can reach **advanced assurance levels**.

Wireless Solutions and Support Services
www.SpotcomLtd.co.uk
+44 (0)1329 448161

Alignment with ELPRO Radios

ELPRO's Quantum Edge, 415U-2-Cx, and 925U-2 radios have been benchmarked against SIR Certification criteria and meet or exceed **Level 3 compliance**.

They include:

- AES-256 encryption with WPA2-PSK
- Over-the-air key rotation and firmware updates
- IP/MAC/Serial whitelisting
- Modbus/DNP3/MQTT support with logging and diagnostics
- Secure provisioning and centralised management

These radios are **actively deployed in thousands of sites globally**, across sectors including water, energy, and transport, making them ideal candidates for **SIR-certified industrial deployments**.

Governance & Openness

SIR Certification is owned and operated by **Spotcom Ltd**, and is:

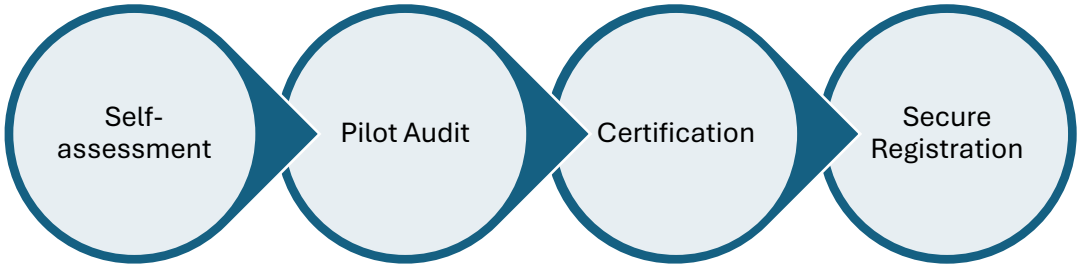
- **Open** – any vendor may certify products and systems.
- **Transparent** – criteria and test methods are fully published.
- **Vendor-neutral** – despite Spotcom's role as an ELPRO supplier, the certification applies to all industrial radios.
- **Expandable** – designed to evolve with emerging threats and new technologies.

Spotcom's mission in establishing SIR Certification is simple: **to protect the people and critical infrastructure of the UK** by creating a practical cybersecurity framework for industrial radio systems.

Roadmap & Next Steps

- **Pilot programs** are in development, with utility partners being engaged for early assessments.
- A **public registry of certified devices** will launch alongside the first audits.
- A **SIR Certified Installer whitelist** will be introduced in 2026, required for Level 2/3 certifications.
- **Regulator engagement** with NCSC, DWI, and Ofcom is planned for Q3 2025.

How SIR Certification Works



Achieving SIR Certification follows a clear, step-by-step pathway. Organisations start with a **self-assessment** to understand their current radio security posture. From there, a **pilot audit** validates key controls in a real-world environment. Once compliance is confirmed, the deployment is issued an official **SIR Certification**, and the product or system is listed in the **secure registry of certified devices**, ensuring transparency and trust for operators and regulators alike.

Why SIR Certification Goes Beyond Spectrum Regulation

In the UK, Ofcom regulates and manages the radio spectrum, ensuring critical services like water and energy utilities have access to reliable, licensed frequencies. They monitor for interference and investigate illegal jamming, but **their remit stops at spectrum integrity—not cybersecurity.** Ofcom does not enforce encryption, authentication, or replay protection on the data carried over those frequencies.

SIR Certification fills this gap. It focuses on the *cybersecurity of the radio payload itself*, introducing layered protections like AES encryption, key rotation, and command authentication—controls that go far beyond spectrum licensing. Where Ofcom ensures the airwaves are "clean," **SIR ensures the signals are secure.**

RF Attacks: Real-World Lessons

Radio-frequency attacks on critical infrastructure are no longer theoretical—they've already caused real-world disruption.

In Australia, 2000, the Maroochy Shire sewage attack became one of the first known RF-based cyber incidents on water infrastructure. A disgruntled ex-contractor used stolen radio equipment to impersonate legitimate controllers on the utility's wireless SCADA network. By sending spoofed commands over the air, he repeatedly disabled pumps and alarms, ultimately releasing **800,000 litres of raw sewage** into local parks and rivers. The root cause? Unauthenticated, unencrypted radio signals that could be replayed and spoofed without detection.

In the United States, 2021, the Oldsmar water facility hack showed how easy it is to tamper with treatment processes. An attacker gained remote access and tried to increase sodium hydroxide dosing in the drinking water supply 100-fold. While that breach came via IT systems rather than RF, it highlighted how simple pump and dosing commands are—and how **vulnerable wireless telemetry would be to replay or spoofing attacks.**

In the energy sector, 2016–2022, European researchers warned of unencrypted radio control signals used for grid load balancing. An attacker with a high-powered SDR could theoretically spoof commands to activate or deactivate millions of devices simultaneously, risking large-scale grid instability. Similarly, the **Ukraine power grid attacks** in 2015–2016 showed how attackers can combine cyber intrusions with wireless sabotage—firmware on substation radios was deliberately wiped to block operator control during the blackout.

In Germany, 2022, a satellite RF cyberattack disrupted 5,800 wind turbines by wiping remote access modems, cutting operators off from their control links. Though the turbines failed safely, the incident proved how wireless disruption—even at the satellite layer—can cascade into energy outages.

What ties all these cases together is the same weakness: **unauthenticated, unprotected radio signals controlling critical processes.** From sewage pumps to power substations, if a signal can be intercepted or spoofed, it can be weaponised.

In the UK, this gap still exists. Much of the water and energy infrastructure continues to rely on legacy radio systems installed decades ago, long before cybersecurity was a consideration. While Ofcom regulates spectrum usage and investigates interference, there is **no national standard that enforces encryption, authentication, or replay protection on industrial radio links.**

That's why **SIR Certification exists**. It sets a measurable benchmark for securing radio commands with encryption, authentication, and key management—closing the hidden security gap that has already been exploited elsewhere in the world.

Selected References

- **Maroochy Shire Sewage Attack (Australia, 2000)** – Case study of an RF-based insider attack on wireless SCADA, causing 800,000 litres of raw sewage to spill. Documented in the Queensland Criminal Code and multiple ICS security reports.
- **Oldsmar Water Facility Hack (Florida, 2021)** – Remote access breach where attackers attempted to poison the water supply by altering chemical dosing. Covered by BBC, Reuters, and ICS-CERT advisories.
- **Ukraine Power Grid Blackouts (2015–2016)** – State-backed hackers combined cyber intrusions with sabotage of substation communications, leading to large-scale outages. Detailed in ESET's Industroyer report and SANS ICS analysis.
- **European Grid Load Control Vulnerabilities (2020–2025)** – Research on spoofable long-wave radio signals controlling up to 60 GW of demand in Central Europe. Presented at Black Hat EU and industry white papers.
- **ViaSat Wind Turbine Disruption (Germany, 2022)** – Satellite modem attack that cut remote access to 5,800 wind turbines during the Ukraine conflict, reported by Reuters and BSI Germany.
- **UK Utility Cyber Resilience Warnings (2022)** – NCSC and DEFRA bulletins highlighting outdated radio telemetry in UK water and energy sectors, urging modernization and encryption.

Get Involved

Utilities, system integrators, and OEMs are encouraged to: - Request a free Level 1 self-assessment pack - Participate in pilot audits - Contribute to the open controls framework

Visit www.spotcomltd.co.uk/SIR or contact sir@spotcomltd.co.uk to register interest.

Together, we can secure the invisible layer that powers critical infrastructure.