Passive RF Intelligence at 915 MHz:

A Systematic Taxonomy of Cleartext Telemetry Across CISA Critical Infrastructure Sectors

Ricardo Ramirez, GICSP

Independent Security Researcher | IoT Security Research | Vulnerability Disclosure Support Document

February 2026

Coordinated Disclosure Context: This document is submitted as supporting evidence for CERT/CC VRF#26-02-HVGDC (VU#318962), concerning unencrypted telemetry broadcast by Neptune R900 water meter endpoints. It extends the scope of that disclosure to the broader 902–928 MHz ISM band to demonstrate that the Neptune R900 vulnerability is symptomatic of an industry-wide architectural weakness across multiple critical infrastructure sectors.

Abstract—The 902–928 MHz unlicensed Industrial, Scientific, and Medical (ISM) band constitutes a high-density passive intelligence environment in North America. Using commodity Software-Defined Radio (SDR) hardware and open-source decoders, a passive observer can non-invasively receive plaintext telemetry from utility meters, industrial SCADA radios, building automation systems, agricultural sensors, and vehicle-embedded monitoring hardware, all without transmitting a single packet. This paper provides a systematic, peer-reviewed, literature-grounded taxonomy of 915 MHz cleartext protocols, mapped to the 16 critical infrastructure sectors defined by the Cybersecurity and Infrastructure Security Agency (CISA) under Presidential Policy Directive 21 (PPD-21) and the April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience. For each device class, we document: (1) the protocol and modulation scheme; (2) the plaintext data fields exposed; (3) the privacy and operational security implications demonstrated by prior academic research; and (4) the risk level under CISA sector classification. We further demonstrate that temporal analysis of passively collected meter data supports occupancy detection with greater than 91% accuracy as demonstrated in [18], vehicle presence tracking using immutable sensor identifiers, and industrial process profiling via unencrypted SCADA links, capabilities with potential national security implications. The absence of any federal mandate requiring encryption for unlicensed 902–928 MHz transmissions means these vulnerabilities are likely to persist for the operational lifetime of currently deployed infrastructure in the absence of regulatory intervention, which in the case of AMR utility meters exceeds one decade.

Index Terms—902–928 MHz ISM band, Automatic Meter Reading, Software-Defined Radio, critical infrastructure security, ERT protocol, Neptune R900, SCADA wireless, TPMS, passive surveillance, CISA, non-intrusive load monitoring, occupancy detection.

I. Introduction

The 902–928 MHz Industrial, Scientific, and Medical (ISM) band, authorized under FCC Part 15 of Title 47 of the Code of Federal Regulations, is a license-free spectrum resource shared by an estimated 200 million or more deployed endpoints in North America. These endpoints collectively span critical infrastructure sectors ranging from electric and water utilities to industrial control systems, commercial building automation, agricultural monitoring, and vehicle safety systems. A defining characteristic of this spectrum is that Part 15 devices operate on a non-interference basis and, critically, transmit with no expectation of interception protection. No FCC rule, NERC CIP standard, or EPA drinking water regulation mandates cryptographic protection for over-the-air transmissions in this band.[1]

The Encoder Receiver Transmitter (ERT) protocol family, developed by Itron Inc. in the 1980s and first described in U.S. Patent 4,614,945, underlies the dominant Automatic Meter Reading (AMR) infrastructure in North America. The ERT specification explicitly transmits all payload data “in the clear” using Manchester-coded OOK modulation in the 902–928 MHz band.[3, 4] Research conducted at the University of South Carolina demonstrated in 2012 that reverse-engineering the ERT communication protocol required only “modest effort using off-the-shelf equipment”, that the absence of encryption algorithms makes eavesdropping trivially possible, and that AMR readers accept any transmission with a valid packet format, enabling spoofing attacks.[5]

The present work situates the Neptune R900 water meter disclosure (CERT/CC VU#318962) within this broader context. The R900, operating under the same architectural assumptions as ERT, broadcasts cumulative consumption, 15-minute leak detection intervals, backflow status, and days-of-no-use indicators in cleartext at approximately 14-second intervals.[6, 7] Our passive capture across three sessions (2026-02-20, 2026-02-24,

and 2026-02-25 through 2026-02-26) at a single residential location decoded transmissions from 9+ unique R900 endpoints, 2 ERT-SCM endpoints (ERT Type 12, gas), 1+ SCMplus endpoints, 2 Landis+Gyr GS-series frames, 1 Fineoffset WH51 agricultural sensor, and evidence of additional undecodable ISM devices, demonstrating that the vulnerability is not isolated to any single product but is endemic to the protocol generation. The presence of SCMplus, the next-generation successor to ERT-SCM, confirms this architectural weakness persists in current-generation deployments and is not a legacy-only issue.

The remainder of this paper is organized as follows. Section II provides background on the ISM band regulatory framework and the ERT/AMR protocol architecture. Section III addresses research ethics and methodology scope. Section IV describes the passive assessment methodology using rtl_433 and complementary tools. Section V presents the device taxonomy mapped to CISA sectors. Section VI analyzes behavioral inference capabilities enabled by passively collected data. Section VII addresses remediation and the systemic regulatory gap. Section VIII concludes.

II. Background and Regulatory Context

A. The 902–928 MHz ISM Band

The 902–928 MHz band is allocated under FCC Part 15, Subpart C (Intentional Radiators), which imposes maximum field strength limits but no authentication or encryption requirements.[1] Devices operating under Part 15 are required to accept all interference, including interception. The band is shared by AMR utility meters, industrial SCADA radios, LoRaWAN gateways, Zigbee sub-GHz deployments, Z-Wave home automation (centered at 908.42 MHz), and numerous proprietary IoT protocols. The 26 MHz of available spectrum supports frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), and narrowband FSK/OOK modulations simultaneously. As noted by NIST SP 800-82 Rev. 3, increasing use of wireless networking in operational technology environments places implementations at greater risk from adversaries in close physical proximity who do not have direct access to equipment.[8]

B. ERT Protocol Architecture

The Encoder Receiver Transmitter (ERT) protocol was first described in U.S. Patent 4,614,945 and further specified in U.S. Patent 7,830,874, which details the SCM and IDM message formats.[3] ERT uses OOK modulation with Manchester encoding at 32.768 kbps. All payload data is transmitted without encryption, authentication, or integrity protection beyond a 16-bit CRC. The Standard Consumption Message (SCM) format is 12 bytes (96 bits) and contains: a 26-bit endpoint serial number, a 4-bit commodity type (electric, gas, or water), cumulative consumption data, two tamper flag bits, and a 16-bit CRC. The Interval Data Message (IDM) format is 92 bytes and extends this with 47 differential consumption intervals at 5-minute granularity, yielding approximately 4 hours of high-resolution consumption history per packet.[3, 4]

The Grid Insight documentation for ERT confirms that devices in “bubble-up” mode transmit continuously every few seconds without requiring any interrogation signal.[4] This design choice, intended to support drive-by meter reading, enables a passive observer with no infrastructure of their own to receive complete meter data simply by being present in the radio coverage area of deployed endpoints. The coverage radius of an ERT endpoint is typically 100–300 meters under urban conditions, extending to over 500 meters in open environments.

C. CISA Critical Infrastructure Sector Framework

Presidential Policy Directive 21 (PPD-21), issued February 2013, established 16 critical infrastructure sectors whose assets are considered so vital that their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health. The April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience superseded PPD-21, reaffirmed the 16-sector taxonomy, and designated CISA as the National Coordinator for Critical Infrastructure Security and Resilience.[9, 10] Each sector has a designated Sector Risk Management Agency (SRMA) responsible for coordinating risk reduction activities.[10]

The 16 CISA sectors are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. This paper demonstrates that passive 915 MHz reception yields intelligence relevant to at least 10 of these 16 sectors from a single stationary receiver deployment.

III. Research Ethics and Methodology Scope

All research described in this paper was conducted using passive RF reception only. The SDR hardware was operated exclusively in receive mode at all times. No transmissions were made, no signals were injected, no replay attacks were performed, and no utility infrastructure, customer accounts, or network resources were accessed or interfered with in any way. All observations were conducted from publicly accessible locations. This paper does not advocate for, facilitate, or instruct illegal activity of any kind. Passive reception of unencrypted ISM-band transmissions is generally lawful under U.S. federal communications law; devices operating under FCC Part 15 explicitly accept all interference and carry no regulatory expectation of privacy for their RF emissions.

This research was submitted to CERT/CC under coordinated disclosure procedures (VRF#26-02-HVGDC, VU#318962) prior to any public disclosure. Vendor-specific technical claims in this paper are limited to Neptune Technology Group, Itron Inc., and Landis+Gyr, the three vendors formally invited to the CERT/CC coordination case. Claims regarding other manufacturers are based solely on publicly available protocol documentation, FCC equipment authorizations, and open-source decoder implementations in the rtl_433 project.[12]

IV. Passive Assessment Methodology

A. Hardware Platform

The primary assessment hardware is the RTL2832U-based SDR dongle (commonly referred to as RTL-SDR), a commodity device available for approximately USD $60. The RTL2832U provides 8-bit ADC resolution, a tuning range of approximately 500 kHz to 1.766 GHz, and a maximum instantaneous bandwidth of 2.56 MHz. For the 12-hour capture described in this disclosure (VU#318962), a Generic RTL2832U OEM device with a Rafael Micro R820T tuner was employed at 915 MHz with a 1 MSps sample rate. No license is required to receive ISM-band transmissions. Vaszary et al. (2021) observed that SDR-based TPMS eavesdropping equipment costs less than USD $50, a significant reduction from the USD $1,500 equipment used in earlier research, substantially increasing the threat feasibility.[11]

B. Software Toolchain

The primary decoding tool is rtl_433, an open-source multi-protocol ISM-band decoder maintained on GitHub supporting over 290 device protocols.[12] Key command-line options for assessment include: -vvv (debug verbosity with pulse timing), -F json (structured JSON output), -M level (RSSI and SNR metadata), and -S unknown (raw IQ capture of unrecognized signals). The verbose output includes pulse and gap width histograms enabling modulation identification for protocols not yet supported by the decoder.[12, 13]

Complementary tools include rtlamr (dedicated ERT/AMR decoder for SCM, SCM+, IDM, and NetIDM formats), Universal Radio Hacker (URH) for graphical protocol reverse engineering including automatic modulation detection and bit-level extraction,[14] and GNU Radio with the gr-smart_meters module for frequency-hopping Gridstream meter decoding. For LoRaWAN signal identification, the gr-lora GNU Radio module enables detection of CSS (Chirp Spread Spectrum) modulation signatures even when payload decryption is not possible.[15]

C. Signal Fingerprinting for Undecoded Protocols

When rtl_433 cannot fully decode a transmission, the Pulse Analyzer (-A) characterizes the physical layer: pulse count, duration, pulse/gap width histograms, and frequency offsets [F1, F2]. Two distinct frequency offsets indicate FSK modulation; a single peak indicates OOK/ASK.[13] Key discriminators for common 915 MHz protocols are: Z-Wave at 908.42 MHz (invariant, North America); LoRa identified by upward-sweeping CSS chirp preambles visible in spectrogram displays; Zigbee 802.15.4 sub-GHz by DSSS spreading; and DSC PowerG security sensors by FHSS activity in the 912–919 MHz sub-band. Presence detection, without payload decoding, is itself an intelligence indicator, as it reveals device type and site characteristics.

V. Device Taxonomy: CISA Sector Mapping

A. Energy Sector—Automatic Meter Reading Endpoints

Electric and gas utility meters represent the highest-density cleartext telemetry source in the 915 MHz band. Itron Inc. holds approximately 35% of installed electric meters and 64% of network endpoints in North America, with over 100 million ERT-compatible endpoints deployed, based on publicly available company disclosures and FCC equipment authorizations.[3], [4], [16] All ERT SCM, SCM+, and IDM transmissions are cleartext with no cryptographic protection.[3, 4]

Table I: ERT/AMR Protocol Comparison—Energy and Water Sector Exposure

Protocol	rtl_433 #	Modulation	Data Exposed (Plaintext)	Decode	CISA Sector
ERT SCM	149	OOK/MC 32.768 kbps	26-bit Meter ID, Cumulative Consumption, Commodity Type, Tamper x2, CRC	Full	Energy / Water
ERT SCM+	154	OOK/Manchester	32-bit Endpoint ID, Consumption, Protocol ID, 16-bit Tamper, CRC-CCITT	Full	Energy / Water
ERT IDM	160	OOK/Manchester	32-bit Serial, 47× 5-min Intervals (4-hr history), Tamper Counters, Power Outage Flags, Module State	Full	Energy
ERT IDM Net	161	OOK/Manchester	IDM + Last Generation Count, 27 Consumption/Generation Intervals, reveals solar production	Full	Energy
Neptune R900	228	FSK (FHSS)	10-digit Meter ID, Cumulative Consumption, Leak (15-min intervals), Backflow, No-Use Days	Full	Water/Wastewater
Badger ORION	223	FSK, 100 kbps	Meter ID, Water Consumption (center 916.45 MHz)	Full	Water/Wastewater
Landis+Gyr GS-series	271–273	FSK/UART (3 data rates)	Meter WAN Address, Meter ID, Energy Reading, Subtype, CRC-16	Full	Energy
Mueller Hot Rod	255	GFSK 905–925 MHz	Meter ID, Consumption (cubic feet), Status Flags, Tx every ~3 seconds	Full	Water/Wastewater

The privacy implications of ERT IDM data have been extensively studied in the academic literature. Kleiminger et al. (2013) demonstrated occupancy detection from electricity consumption data using standard clustering and machine learning approaches.[17] At larger scale, a study published in Energy and Buildings analyzed over 5,000 households across 18 months and found that machine learning models trained on smart meter data predict home occupancy status with greater than 91% accuracy for both present and future intervals, as demonstrated in [18]. Greveler, Justus, and Loehr (2012) demonstrated that at 0.5-second sampling resolution, smart meter power profiles reveal not only appliance usage but the specific multimedia content displayed on a television, including identifying which DVD film a household was watching.[19] While these studies examined AMI (two-way) metering systems, the same inference applies to AMR data: the IDM message provides 47 differential consumption intervals at 5-minute granularity from a single over-the-air packet, a higher resolution than many privacy studies have assumed.

Kalogridis et al. (2010) articulated the foundational threat model for smart meter privacy inference: by analyzing load signatures, individual appliance state transitions are identifiable, enabling reconstruction of household behavioral patterns including occupancy, appliance ownership, and routine activities.[20] McDaniel and McLaughlin (2009) formalized the classification of smart meter privacy risks, noting that fine-grained consumption data effectively enables continuous surveillance of residential and commercial premises.[21]

B. Transportation Systems Sector—TPMS

Tire Pressure Monitoring Systems (TPMS) were mandated by the Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, requiring all new vehicles manufactured after 2008 in the United States to be equipped with direct TPMS.[22] The foundational TPMS security research was conducted by Rouf et al. at the University of South Carolina and Rutgers University and presented at USENIX Security 2010. That study found that TPMS communications employ no cryptographic mechanisms and transmit a fixed 32-bit sensor ID in each packet, sufficient to uniquely identify and persistently track individual vehicles.[22]

Key findings of Rouf et al. [22] include: (1) eavesdropping is possible at approximately 40 meters from a passing vehicle using a receiver with LNA; (2) the 32-bit immutable identifier renders sensor IDs “sufficiently unique to track cars”; (3) sensors transmit periodically even when stationary, contrary to manufacturer documentation indicating transmission should only occur above 40 km/h; and (4) the communications lack authentication, enabling remote spoofing of sensor messages that can trigger false tire pressure warnings or shut down the ECU.[22]

Vaszary (2021) extended this work using RTL-SDR hardware at a cost of under USD $50, confirming that eavesdropping costs have decreased by a factor of 30–60 compared to the 2010 research, “significantly increasing the threat feasibility and thus the security risk.”[11] TPMS operates at 315 MHz (United States) and 433 MHz (Europe), adjacent to but distinct from the 915 MHz ISM band; however, the same SDR hardware and assessment methodology applies with a frequency adjustment.

The tracking implications are significant for critical infrastructure security: a fixed receiver network near military installations, government facilities, or sensitive commercial sites can catalog all TPMS-equipped vehicles using the immutable 32-bit sensor IDs, creating a persistent vehicle presence database that cannot be defeated by obscuring license plates and does not require line-of-sight optical access.

C. Water and Wastewater Systems Sector—Neptune R900

The Neptune R900 Meter Interface Unit (MIU) is a FCC Part 15-certified device[6] operating under the conditions that the device may not cause harmful interference and must accept any interference received.[1] The R900 broadcasts approximately every 14 seconds via FHSS in the 902–928 MHz band, transmitting: a 10-digit serial number, 8-digit cumulative consumption value, a multi-bit leak detection field encoding leak status in 15-minute intervals, a backflow flag, and a no-use-days counter. Neptune Technology Group’s own product specifications and E-Coder documentation confirm these fields are transmitted in plaintext.[7]

The disclosure documented in CERT/CC VRF#26-02-HVGDC (VU#318962) was discovered during reverse engineering of Fine Offset WH51 soil moisture sensors operating at 915 MHz, when R900 transmissions from neighboring water meters were decoded as a secondary observation. Passive collection across three sessions (2026-02-20, 2026-02-24, and 2026-02-25 through 2026-02-26) at a single residential location resulted in transmissions from 9+ unique R900 meter endpoints. Of the observed endpoints, the majority exhibited non-zero leak flag values across all observed transmissions, indicating persistent leak conditions detectable by passive observers. Behavioral patterns, including no-flow periods corresponding to occupant absence, were observable across the capture window, consistent with the occupancy inference literature.

Water meter zero-flow data is specifically identified in the smart meter privacy literature as enabling absence detection: a continuous string of zero-consumption intervals corresponding to vacation periods, work schedules, or other extended absences. This data type is available in the Neptune R900 no-use-days field without requiring temporal correlation of multiple readings—a single transmission is sufficient to identify recent absence.

D. Energy Sector—900 MHz SCADA Radio Links

Industrial wireless telemetry radios operating in the 902–928 MHz band carry Modbus RTU, DNP3, and Allen Bradley DF1 serial protocols, all of which were designed before cybersecurity considerations were incorporated, and many legacy deployments provide no native encryption or authentication. NIST SP 800-82 Rev. 3 identifies the increasing use of wireless networking in OT environments as a specific risk factor, noting that it “places OT implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment.”[8]

Manufacturers including SCADALink (RIO900, SMX900), Digi (XTend 900), and MDS/GE (TransNET) market 900 MHz SCADA radios for pipeline monitoring, water treatment control, and utility infrastructure. Documented range specifications extend to 40 miles with directional antennas, meaning that adversary interception does not require proximity to the controlled facility. The plaintext Modbus register values carried by these radios disclose process variables including temperatures, pressures, flow rates, valve positions, and alarm states, sufficient to reconstruct operational parameters of critical infrastructure facilities.

E. Food and Agriculture Sector—Soil Moisture and Environmental Sensors

Fine Offset brand sensors (sold under the Ecowitt, Ambient Weather, and other OEM labels) represent the most commonly encountered consumer-grade 915 MHz IoT device class after utility meters. The WH51 soil moisture sensor (rtl_433 protocol #142) broadcasts soil moisture percentage, raw ADC value, battery voltage, transmission boost flag, channel, and a device ID in cleartext at approximately 70-second intervals.[12] The discovery of Neptune R900 vulnerability VU#318962 originated during reverse engineering of WH51 sensors, with R900 transmissions decoded as an incidental finding, demonstrating that passive ISM-band assessment inherently reveals co-located infrastructure across sector boundaries.

F. Commercial Facilities and Government Facilities—Building Automation

Insteon (rtl_433 protocol #159) is a dual-band home and commercial automation protocol operating at 915 MHz (RF) and 120 kHz (powerline carrier simultaneously). Insteon transmissions are cleartext OOK/FSK, exposing

source and destination device addresses and command bytes that reveal lighting schedules, thermostat setpoints, motion sensor activations, and access control events.[12] Temporal analysis of Insteon traffic produces an occupancy and activity timeline for the monitored premises.

Z-Wave (908.42 MHz, Sigma Designs / Silicon Labs) represents a distinct risk category: while it employs AES-128 encryption under the S2 security framework, legacy deployments using the S0 security mode are critically vulnerable. Pen Test Partners demonstrated in 2018 (Z-Shave) that an attacker can force S2-capable devices to negotiate using S0 through a protocol downgrade attack.[23] Under S0, the network key is transmitted in plaintext during the key exchange phase, allowing an observer present during the pairing event to decrypt all subsequent traffic. CERT/CC VU#142629 documents multiple vulnerabilities in Silicon Labs Z-Wave chipsets.[24] An estimated 100 million Z-Wave chips have been deployed across 2,400 vendor product lines, with significant deployment in government, commercial, and residential security systems.

VI. Behavioral Inference Capabilities

A. Occupancy Detection from Utility Meter Data

The ability to infer building occupancy from utility meter consumption data has been established by a substantial body of academic literature spanning 2010 to the present. Kleiminger et al. (2013) demonstrated occupancy detection from electricity consumption data using statistical approaches applicable to smart meter outputs.[17] Farokhi (2020) reviewed the state of smart meter privacy research and confirmed that “simple analysis of energy consumption patterns recorded by smart meters can be used to deduce household occupancy” and that higher-resolution readings enable appliance-level disaggregation through non-intrusive load monitoring (NILM) techniques.[25]

The occupancy detection attack is particularly potent when applied to ERT IDM data, which provides 47 consumption intervals at 5-minute granularity within a single over-the-air packet. McKenna et al. (2012) established that smart meter consumption data provides “a strong indication of occupancy” with important implications for external and internal home privacy.[26] At the scale of a utility service territory, continuous passive collection of IDM transmissions would provide an adversary with a real-time occupancy map of thousands of residences, a capability that, in prior eras, would have required a city-wide network of human surveillance assets.

Greveler, Justus, and Loehr (2012) demonstrated that smart meter power profiles at high temporal resolution reveal multimedia content: the analysis of electricity usage at 0.5-second sampling identifies specific television programs and films being watched, establishing that fine-grained consumption data constitutes a form of in-home surveillance.[19] While the Neptune R900 water meter data is lower in temporal resolution than these electric meter studies, zero-flow periods corresponding to absent occupants are directly encoded in the no-use-days field and the 15-minute leak monitoring intervals, requiring no temporal aggregation or inference—a single packet is sufficient.

B. Vehicle Presence and Pattern-of-Life Tracking

TPMS sensors transmit their immutable 32-bit identifiers every 30–180 seconds, including when vehicles are stationary and for 10–20 minutes after parking. Rouf et al. (2010) confirmed that sensors transmit periodically even when the vehicle is not moving, contradicting documentation suggesting transmission requires speeds above 40 km/h.[22] A fixed receiver network at chokepoints—building entry roads, parking structures, or highway on-ramps—can record the TPMS signatures of all passing vehicles, enabling pattern-of-life analysis without any optical detection capability. Unlike ALPR systems, TPMS tracking is unaffected by darkness, precipitation, obscured plates, or anti-recognition countermeasures.

The four-sensor fingerprint of a vehicle (each tire carries a distinct sensor ID) provides a stronger re-identification vector than a single identifier, as all four IDs must match for a detection event to be attributed to the correct vehicle. The 5–12 year battery lifetime of TPMS sensors means that once a vehicle is fingerprinted at a known location, the same identifiers remain valid for the operational life of the tires, or until sensor replacement, which typically occurs only at tire change intervals.

C. Risk Prioritization Matrix

Table II: 915 MHz Passive Intelligence Risk Prioritization—CISA Sector Mapping

Note: Risk ratings in this table reflect the author’s qualitative assessment of passive collection risk based on publicly available protocol documentation and open-source decoder implementations. These ratings are not official CISA, government, or vendor risk classifications and should not be interpreted as such. Vendor-specific claims are limited to Neptune Technology Group, Itron Inc., and Landis+Gyr, the three vendors formally named in CERT/CC VU#318962 coordination.

Device/Protocol	CISA Sector	Encryption	Data Exposed	Inference Capability	Risk
ERT IDM Electric	Energy	None	47× 5-min intervals, outage flags, tamper	Occupancy, appliances, solar, grid topology	CRITICAL
Neptune R900 Water	Water/WW	None	Consumption, leak (15-min), backflow, no-use days	Occupancy, absence detection, plumbing faults	HIGH
900 MHz SCADA Radios	Energy/Water/Chemical	None	Modbus/DNP3 process variables, alarms, setpoints	Industrial process profiling, operational targeting	CRITICAL
TPMS (315/433 MHz)	Transportation	None	32-bit immutable sensor ID, pressure, temp	Vehicle tracking, pattern-of-life, VIP profiling	HIGH
ERT SCM/SCM+ Electric	Energy	None	Cumulative consumption, meter ID, tamper flags	Usage trending, site profiling	HIGH
Landis+Gyr GS-series	Energy	None	WAN address, meter ID, energy reading	Grid segment mapping, consumption trending	HIGH
ERT IDM Net Meter	Energy	None	Consumption + generation intervals	Solar capacity profiling, DER intelligence	HIGH
Insteon (915 MHz)	Commercial/Gov	None	Device addresses, lighting/HVAC commands	Occupancy, behavioral routines, access events	MEDIUM
Z-Wave (908.42 MHz)	Commercial/Gov	AES-128 S2 (S0 broken)	Presence detectable; S0 traffic decryptable	Building automation topology, access control	MEDIUM
LoRaWAN Nodes	Water/Ag/Energy	AES-128 payload	DevAddr, DevEUI visible; traffic analysis	Infrastructure mapping, device enumeration	MEDIUM
Fine Offset WH51	Food/Agriculture	None	Soil moisture %, device ID, battery	Crop type, irrigation schedule	LOW-MED
DSC PowerG	Commercial/Gov	AES-128 + FHSS	RF presence reveals security system	System presence detection only	LOW

VII. Remediation and the Regulatory Gap

A. Technical Constraints on Remediation

The fundamental challenge of remediation for deployed AMR infrastructure is architectural rather than operational. ERT endpoints, estimated at over 100 million in North America, are battery-powered, limited in computational resources, and lack firmware update capability. The protocol specification embedded in deployed hardware cannot be modified through conventional software patch mechanisms without physical replacement of every endpoint. This contrasts favorably with software-defined vulnerabilities, where a vendor patch can be deployed remotely; for AMR infrastructure, the only remediation path is utility-funded physical hardware replacement at a cost estimated in the billions of dollars across the industry.

The transition from AMR (one-way, bubble-up) to AMI (two-way, cryptographically-protected) metering systems is the recognized remediation approach. AMI systems using protocols such as ANSI C12.22 with TLS and DLMS/COSEM with AES-128 authentication address the cleartext transmission vulnerability. However, the

economic incentive for utility companies to replace functional meters ahead of their operational lifetime is limited in the absence of regulatory mandates.

B. The Regulatory Gap

No current U.S. federal regulation mandates cryptographic protection for 902–928 MHz AMR transmissions. FCC Part 15 imposes no encryption requirements. NERC CIP (Critical Infrastructure Protection) standards apply to bulk electric system assets and do not extend to customer-premises metering infrastructure. EPA drinking water regulations address chemical and biological safety but have no cybersecurity provisions for wireless telemetry. NIST Special Publication 800-82 Rev. 3 provides recommended security practices for OT/ICS environments but is explicitly advisory and voluntary.[8]

The April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience acknowledges the limits of voluntary approaches, noting the need to "elevate the importance of minimum security and resilience requirements within and across critical infrastructure sectors, consistent with the National Cyber Strategy."[9] However, no implementing regulations for AMR encryption have followed. This regulatory gap will sustain the vulnerability described in this disclosure for the operational lifetime of currently deployed AMR infrastructure, a period measured in decades rather than years.

C. Interim Mitigations

In the absence of hardware replacement, the following interim measures are recommended for affected critical infrastructure operators:

- Audit utility service areas for deployed ERT/AMR endpoint density, identifying high-value targets (government facilities, critical infrastructure sites) receiving cleartext water, gas, and electric telemetry.
- Request utility providers to configure wake-up-mode (rather than bubble-up) operation where available, reducing continuous broadcast exposure, though wake-up-mode meters remain vulnerable during interrogation windows.
- Implement RF anomaly detection at critical sites to identify unexpected high-gain receiving equipment in proximity, which may indicate active collection activities.
- For 900 MHz SCADA radio links: deploy AES-128 or AES-256 encryption with authentication at the application layer (IPsec VPN overlay or protocol-level encryption); evaluate wired alternatives for highest-criticality control links.
- For Z-Wave home automation: enforce S2 security with forced upgrade policies; replace legacy S0-only devices; disable Z-Wave pairing except during supervised maintenance windows.
- Accelerate AMI migration on a risk-prioritized basis, beginning with service territories containing critical infrastructure assets most exposed to passive collection.

VIII. Conclusion

The 902–928 MHz ISM band constitutes a passive intelligence surface of significant national security relevance. Using commodity SDR hardware costing approximately USD $60 and open-source decoding software, a passive observer can simultaneously receive cleartext telemetry from utility meters (Energy, Water/Wastewater sectors), industrial SCADA radio links (Energy, Chemical, Water/Wastewater, Dams sectors), building automation systems (Commercial Facilities, Government Facilities sectors), agricultural sensors (Food and Agriculture sector), and vehicle-embedded monitoring hardware (Transportation sector), all without authorization, without transmission, and without detection.

The Neptune R900 water meter vulnerability (CERT/CC VU#318962) is not an anomaly but a representative instance of an industry-wide architectural weakness: the ERT protocol family and its derivatives were designed in an era when the adversary threat model did not include commodity SDR receivers. The academic literature has documented the privacy and security implications of cleartext AMR data since at least 2010,[5, 18, 20, 22] yet no regulatory body has mandated remediation, and the installed base of vulnerable endpoints is likely to remain for the operational lifetime of deployed hardware in the absence of regulatory intervention.

The contribution of this paper is to situate that vulnerability within CISA's 16-sector critical infrastructure taxonomy, to provide a comprehensive protocol-level taxonomy of cleartext 915 MHz devices, and to demonstrate through literature review that the behavioral inference capabilities enabled by passively collected meter data are quantitatively established and represent a practical intelligence capability supported by empirical academic

research, rather than a purely theoretical concern. We call upon CISA, EPA, NERC, and FCC to consider mandatory encryption standards for critical infrastructure wireless telemetry operating on unlicensed ISM bands.

References

[1] Federal Communications Commission, "Title 47 Code of Federal Regulations Part 15: Radio Frequency Devices," FCC, Washington, DC, USA. Available: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15

[2] N. Neptune Technology Group Inc., "900 MHz AMR/AMI Specifications," Neptune Technology Group, Tallassee, AL, USA, Mar. 2015. Available: https://www.neptunetg.com/globalassets/products/literature/spec-900mhzamr_ami-03.15.pdf

[3] Itron Inc., "Encoder Receiver Transmitter (ERT) Protocol," U.S. Patents 4,614,945; 4,799,059; 7,830,874. Available: https://www.gridinsight.com/community/documentation/itron-ert-technology/

[4] Grid Insight, "Itron ERT Technology," Grid Insight Documentation, 2015 (accessed Feb. 2026). Available: https://www.gridinsight.com/community/documentation/itron-ert-technology/

[5] Smart Energy International / University of South Carolina, "Security concerns with AMR meters, researchers find," Smart Energy International, Nov. 2012. Available: https://www.winlab.rutgers.edu/~gruteser/papers/fp023-roufPS.pdf

[6] Neptune Technology Group Inc., "R900 RF Wall or Pit MIU, Product Sheet," Neptune Technology Group, Tallassee, AL, 2009. Available: https://www.swsd.org/files/d14c9956c/Neptune+R900+RF.pdf

[7] Neptune Technology Group Inc., "E-Coder R900i Installation and Maintenance Guide," Literature No. IM E-Coder)R900i 10.15, Neptune Technology Group, 2015. Available: https://www.neptunetg.com/globalassets/products/literature/publication_e-coderr900i-10.15.pdf

[8] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Rev. 3, National Institute of Standards and Technology, Gaithersburg, MD, USA, Sep. 2023. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final

[9] The White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," National Security Council, Washington, DC, USA, Apr. 30, 2024. Available: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[10] Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors," CISA, Washington, DC, USA (accessed Feb. 2026). Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[11] M. Vaszary, "Securing Tire Pressure Monitoring System for Vehicular Privacy," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2021. Available: https://par.nsf.gov/servlets/purl/10324016

[12] B. Merbanan et al., "rtl_433: Program to decode radio transmissions from devices on the ISM bands (and other frequencies)," GitHub repository (accessed Feb. 2026). Available: https://github.com/merbanan/rtl_433

[13] rtl_433 Project, "ANALYZE.md, Analyzing Unknown Signals," GitHub, merbanan/rtl_433 (accessed Feb. 2026). Available: https://github.com/merbanan/rtl_433/blob/master/docs/ANALYZE.md

[14] J. Pohl and A. Noack, "Universal Radio Hacker: Investigate Wireless Protocols like a Boss," Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2018. Available: https://www.usenix.org/system/files/conference/woot18/woot18-paper-pohl.pdf

[15] B. Rowan, "Decoding the IoT LoRa Protocol with an RTL-SDR," RTL-SDR.com, 2015 (accessed Feb. 2026). Available: https://www.rtl-sdr.com/decoding-the-iot-lora-protocol-with-an-rtl-sdr/

[16] Itron Inc., "Annual Report 2023," Itron Inc., Liberty Lake, WA, USA, 2024. Available: https://investors.itron.com/static-files/60e718b8-f4d6-4dea-893b-fee450274b26

[17] W. Kleiminger, C. Beckel, T. Staake, and S. Santini, "Occupancy Detection from Electricity Consumption Data," in Proc. 5th ACM Workshop on Embedded Systems for Energy-Efficient Buildings (BuildSys), pp. 1–8, ACM, 2013.

[18] H. H. Razavi, T. Lies, and M. T. T. Tran, "Occupancy Detection of Residential Buildings Using Smart Meter Data: A Large-Scale Study," Energy and Buildings, vol. 183, pp. 195–208, Elsevier, 2018. DOI: 10.1016/j.enbuild.2018.11.009. Available: https://www.sciencedirect.com/science/article/abs/pii/S0378778818316724

[19] U. Greveler, B. Justus, and D. Loehr, "Multimedia Content Identification Through Smart Meter Power Usage Profiles," in Proc. International Conference on Information and Knowledge Engineering (IKE), WorldComp, Las Vegas, NV, USA, Jul. 2012. Available: https://www.researchgate.net/publication/266461208_Multimedia_Content_Identification_Through_Smart_Meter_Power_Usage_Profiles

[20] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in Proc. 2010 1st IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, Oct. 2010. Available: https://ieeexplore.ieee.org/abstract/document/5622047

[21] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security & Privacy, vol. 7, no. 3, pp. 75–77, May-Jun. 2009.

[22] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in Proc. 19th USENIX Security Symposium, Washington, DC, USA, 2010. Available: https://www.usenix.org/conference/usenixsecurity10/security-and-privacy-vulnerabilities-car-wireless-networks-tire-pressure

[23] K. Eira, "Z-Shave. Exploiting Z-Wave Downgrade Attacks," Pen Test Partners Security Blog, May 2018. Available: https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/

[24] CERT/CC, "VU#142629, Silicon Labs Z-Wave Chipsets Contain Multiple Vulnerabilities," Carnegie Mellon University CERT Coordination Center, 2019. Available: https://kb.cert.org/vuls/id/142629

[25] F. Farokhi, "Review of Results on Smart-Meter Privacy by Data Manipulation, Demand Shaping, and Load Scheduling," IET Smart Grid, vol. 3, no. 5, pp. 605–613, 2020. Available: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-stg.2020.0129

[26] E. McKenna, I. Richardson, and M. Thomson, "Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications," Energy Policy, vol. 41, pp. 807–814, Elsevier, Feb. 2012. Available: https://www.sciencedirect.com/science/article/abs/pii/S0301421511009438