Vulnerabilità Critiche nelle Infrastrutture Municipali: Analisi delle Tecnologie RF, di Sorveglianza e di Metering

Stefano Rossi IU2UEI

1. Analisi del Panorama delle Minacce nelle Smart City

La rapida digitalizzazione delle infrastrutture municipali, spesso etichettata sotto l'egida della "Smart City", ha introdotto un livello di interconnettività senza precedenti nella gestione urbana. Le amministrazioni locali, spinte dalla necessità di ottimizzare le risorse energetiche, migliorare la sicurezza pubblica e fluidificare il traffico, hanno adottato massicciamente tecnologie IoT (Internet of Things). Tuttavia, questa transizione ha esposto le città a una superficie di attacco vasta e spesso mal protetta. L'analisi approfondita delle vulnerabilità sistemiche rivela un quadro preoccupante in cui l'obsolescenza dei protocolli, l'implementazione insicura di standard moderni e la fragilità fisica dei dispositivi sul campo convergono per creare rischi significativi per la privacy dei cittadini e la resilienza delle infrastrutture critiche.
La presente analisi si concentra sulle tre arterie principali della tecnologia municipale: l'infrastruttura di misurazione avanzata (Advanced Metering Infrastructure - AMI), i sistemi di sorveglianza pubblica (incluso il caso studio delle telecamere Flock Safety) e i sistemi di controllo del traffico. Attraverso l'esame di case study internazionali, strumenti di hacking disponibili su repository pubbliche come GitHub e discussioni tecniche su piattaforme come Reddit, emerge una realtà operativa in cui la sicurezza è stata frequentemente sacrificata in nome dell'efficienza energetica e della facilità di installazione.

1.1 La Convergenza Fisico-Cibernetica

A differenza dei sistemi IT tradizionali confinati nei data center, l'infrastruttura municipale risiede nello spazio fisico pubblico: armadietti stradali, pali della luce, contatori domestici e sensori di parcheggio. Questa esposizione fisica nega molti dei vantaggi della sicurezza perimetrale tradizionale. Come evidenziato dalle vulnerabilità scoperte nelle telecamere Flock Safety, l'accesso fisico a un dispositivo può tradursi in un accesso amministrativo completo (root), permettendo a un attaccante di trasformare un nodo periferico in un punto di ingresso verso la rete centrale dell'amministrazione o delle forze dell'ordine.
Inoltre, la dipendenza dalle comunicazioni a radiofrequenza (RF) crea un vettore di attacco invisibile ma pervasivo. Protocolli come Wireless M-Bus (wM-Bus), LoRaWAN e le trasmissioni proprietarie a 900 MHz o 169 MHz sono suscettibili a intercettazione, jamming e attacchi di replay se non rigorosamente protetti da crittografia end-to-end e meccanismi di autenticazione robusti. L'accessibilità di hardware a basso costo, come le radio definite via software (SDR) basate su chipset RTL2832U, ha democratizzato la capacità di intercettare e analizzare questi segnali, portando strumenti di livello militare nelle mani di hobbisti e attori malevoli.

2. Infrastruttura di Misurazione Avanzata (AMI): Lo Scandalo della Privacy e le Vulnerabilità RF

L'introduzione dei contatori intelligenti (smart meters) per elettricità, gas e acqua rappresenta forse la più vasta implementazione IoT al mondo. Questi dispositivi sostituiscono la lettura manuale con la trasmissione automatica dei dati di consumo. Tuttavia, la granularità di questi dati e le modalità di trasmissione hanno generato quello che ricercatori e attivisti definiscono "lo scandalo dei smart meter", una problematica che intreccia violazioni della privacy e rischi di sabotaggio infrastrutturale.

2.1 La Granularità del Dato e il Monitoraggio Non Intrusivo del Carico (NILM)

Il cuore della controversia sulla privacy risiede nella frequenza di campionamento dei dati. I moderni smart meter non si limitano a registrare il consumo totale mensile, ma inviano letture a intervalli brevi (tipicamente 15, 30 o 60 minuti, e in alcuni casi ogni pochi secondi). Questa alta risoluzione temporale abilita tecniche di analisi note come *Non-Intrusive Load Monitoring* (NILM).
Il principio alla base del NILM è che ogni apparecchio elettrico possiede una "firma" energetica unica. Il ciclo di accensione di un compressore frigorifero è distinguibile dalla resistenza di un tostapane o dall'alimentatore switching di un televisore moderno. Analizzando le variazioni di potenza reattiva e attiva, algoritmi sofisticati possono disaggregare il carico totale per identificare quali specifici elettrodomestici sono in uso in un dato momento.

2.1.1 Deduzione delle Abitudini di Vita e Privacy

Le implicazioni di questa capacità analitica sono profonde. Ricercatori come Dario Carluccio e Stephan Brinkhaus hanno dimostrato, intercettando dati non crittografati dal provider tedesco Discovergy, di poter determinare non solo quando gli occupanti erano in casa, ma anche quale programma televisivo stessero guardando, correlando le fluttuazioni del consumo energetico del televisore con i cambiamenti di luminosità del segnale trasmesso.
Questa capacità trasforma l'abitazione in una "casa di vetro". Le informazioni deducibili includono:

- **Pattern di Occupazione:** Sapere con precisione quando una casa è vuota aumenta il rischio di furti mirati. I ladri potrebbero utilizzare strumenti SDR per scansionare un quartiere e individuare le abitazioni con consumo basale (modalità vacanza).
- **Routine Quotidiane:** Orari di sonno e veglia, orari dei pasti e persino pratiche religiose possono essere inferiti dall'uso di luci e apparecchiature.
- **Stato degli Apparecchi:** Le utility possono identificare apparecchi vecchi o inefficienti per targettizzare pubblicità o, in scenari più distopici, le compagnie assicurative potrebbero adeguare i premi basandosi su comportamenti rilevati (es. uso frequente di friggitrici o orari di sonno irregolari).

Negli Stati Uniti, questa invasività ha portato a sentenze storiche. Nel caso *Naperville Smart*

Meter Awareness v. City of Naperville, la Corte d'Appello ha stabilito che i dati granulari degli smart meter sono protetti dal Quarto Emendamento, riconoscendo che tali dati rivelano "dettagli intimi su ciò che accade all'interno di una casa" e che l'accesso governativo a tali dati costituisce una perquisizione che richiede un mandato.

2.2 Vulnerabilità dei Protocolli di Trasmissione: Il Caso Itron e RTLSDR

Una vulnerabilità tecnica critica risiede nei protocolli utilizzati per trasmettere questi dati dai contatori ai concentratori dati o ai veicoli di lettura (drive-by).

2.2.1 Il Protocollo Itron ERT e la Mancanza di Crittografia

In Nord America, e in diverse implementazioni internazionali, il protocollo proprietario ERT (*Encoder Receiver Transmitter*) di Itron è onnipresente. Questi dispositivi operano nella banda ISM a 900 MHz e trasmettono messaggi di consumo standard (SCM) o messaggi di dati intervallati (IDM). La criticità risiede nel fatto che, per milioni di dispositivi legacy ancora in funzione, queste trasmissioni avvengono in chiaro, senza crittografia.
La comunità open source ha sviluppato strumenti potenti per sfruttare questa debolezza. Il tool più noto è rtlamr (RTL-SDR Automated Meter Reading), disponibile su GitHub. Sviluppato in Go, questo software permette a chiunque possieda un dongle RTL-SDR da circa 30 euro di intercettare e decodificare i pacchetti ERT provenienti dai contatori vicini.

Tabella 1: Strumenti e Protocolli per l'Intercettazione Smart Meter

Strumento	Piattaforma	Protocolli Supportati	Funzionalità Principale	Rischio Associato
rtlamr	Linux/Windows/Mac (Go)	Itron ERT (SCM, SCM+, IDM)	Decodifica trasmissioni 900 MHz in chiaro	Wardriving, mappatura consumi quartiere
wmbusmeters	Linux (C++)	Wireless M-Bus (T1, C1, S1)	Decodifica telegrammi wM-Bus (868 MHz)	Lettura contatori gas/acqua/luce europei
rtl_433	Multi-piattaforma	Vari (ISM 433/868/900 MHz)	Analisi protocolli generici e sensori	Intercettazione sensori ambientali e meter
rpitx	Raspberry Pi	Arbitrari (TX via GPIO)	Trasmissione RF senza radio dedicata	Replay attack, jamming, spoofing segnali

L'uso di rtlamr in combinazione con un GPS permette la pratica del "wardriving" dei contatori: un attaccante può guidare attraverso un quartiere, raccogliendo ID dei contatori e letture di consumo, per poi mappare questi dati agli indirizzi fisici. Poiché l'ID del contatore è spesso stampato sul dispositivo stesso ed è visibile dall'esterno, la correlazione è triviale.

2.2.2 Wireless M-Bus e le Sfide Europee

In Europa, lo standard dominante è il Wireless M-Bus (EN 13757-4). Sebbene lo standard preveda modalità crittografate (AES-128 in Mode 5 o 7), l'implementazione pratica varia enormemente. Molte utility, per risparmiare batteria o semplificare la gestione delle chiavi, hanno distribuito contatori che trasmettono in modalità "aperta" o utilizzano chiavi di crittografia statiche derivate dal numero seriale del contatore, rendendo la protezione inefficace contro un attaccante determinato.
Un focus particolare in Italia è sulla frequenza **169 MHz** (Modalità N), utilizzata per la telelettura del gas e dell'acqua grazie alla sua eccellente capacità di penetrazione attraverso muri e terreni (utile per contatori in tombini o seminterrati). Tuttavia, la banda stretta e la bassa velocità di trasmissione rendono questa modalità particolarmente suscettibile al jamming. Un attaccante con un semplice trasmettitore a 169 MHz (come un CC1120 o un dispositivo basato su rpitx) potrebbe oscurare un'intera area, impedendo alla utility di ricevere letture o allarmi critici su fughe di gas.

2.3 Vulnerabilità Fisiche e Frodi

Oltre agli attacchi informatici, i sistemi di metering soffrono di vulnerabilità fisiche persistenti. La "truffa del magnete" rimane una minaccia per i contatori del gas e dell'acqua, specialmente quelli con accoppiamento magnetico tra la camera volumetrica e il totalizzatore. L'applicazione di un potente magnete al neodimio può saturare il campo magnetico interno, bloccando il conteggio mentre il fluido continua a scorrere. Sebbene i nuovi contatori elettronici (come gli Open Meter di Enel o i moderni smart meter gas UNI-TS 11291) integrino sensori di Hall per rilevare e segnalare tentativi di frode magnetica, esistono ancora milioni di dispositivi vulnerabili sul campo o tecniche per schermare parzialmente i sensori.
Inoltre, la porta ottica (standard IEC 62056-21) presente su molti contatori per la manutenzione locale rappresenta un vettore di attacco se non adeguatamente protetta. Ricercatori hanno dimostrato che l'uso di password di default o l'assenza di autenticazione robusta su questa interfaccia può permettere a un attaccante con accesso fisico di riprogrammare il contatore, alterare le tariffe o estrarre le chiavi di crittografia utilizzate per la comunicazione remota.

3. Sistemi di Sorveglianza: Il Caso Flock Safety e l'Esposizione Globale

La sorveglianza urbana si è evoluta dalle semplici telecamere a circuito chiuso (CCTV) a sistemi intelligenti di lettura targhe (ALPR - Automated License Plate Recognition) connessi in cloud. Questi sistemi, utilizzati sia dalle forze dell'ordine che da associazioni private (HOA), creano una rete di monitoraggio pervasiva. Tuttavia, la sicurezza di questi dispositivi "edge" è spesso inferiore a quella dei server centrali.

3.1 Le Vulnerabilità Critiche di Flock Safety

Un caso emblematico è quello delle telecamere Flock Safety, ampiamente diffuse negli Stati Uniti. Nel 2025, il ricercatore Ben Jordan, basandosi sul lavoro di Jon Gaines, ha esposto una serie di vulnerabilità devastanti che permettono la compromissione totale del dispositivo.

3.1.1 Il Backdoor Fisico e l'Accesso Root

La vulnerabilità più eclatante risiede in una procedura di debug lasciata attiva nei dispositivi di produzione. I ricercatori hanno scoperto che premendo un pulsante fisico sul retro della telecamera secondo una specifica sequenza temporale, il dispositivo attivava un hotspot Wi-Fi non documentato.
Connettendosi a questo hotspot, un attaccante poteva accedere all'interfaccia ADB (Android Debug Bridge). Poiché le telecamere eseguivano una versione obsoleta di Android (Android 8, non più supportato e privo di patch di sicurezza critiche), l'accesso ADB garantiva privilegi di root (amministratore supremo). Questo livello di accesso è definito "carte blanche": permette l'installazione di malware, la modifica dei file di sistema, l'estrazione di dati e la riconfigurazione completa del dispositivo.

3.1.2 Assenza di Crittografia e Credenziali in Chiaro

Nonostante le dichiarazioni di marketing sulla sicurezza end-to-end, l'analisi forense del filesystem della telecamera ha rivelato che le immagini catturate (targhe e contesti ambientali) erano memorizzate in chiaro sulla memoria locale. Un attaccante che rubasse fisicamente la telecamera o vi accedesse via ADB potrebbe scaricare gigabyte di dati sensibili senza dover affrontare alcuna crittografia.
Inoltre, è emerso che in alcune configurazioni le credenziali di accesso venivano trasmesse in chiaro o erano presenti hardcoded nel firmware, esponendo il sistema ad attacchi Man-in-the-Middle (MitM) se un attaccante riuscisse a interporsi nella connessione di rete, ad esempio utilizzando un IMSI catcher per simulare una torre cellulare a cui la telecamera si connette. Altri dettagli riguardo gli attacchi a cui la rete cellulare è vulnerabile sono stati approfonditi in una pubblicazione dedicata.

3.1.3 Gestione delle Credenziali e Mancanza di MFA

A livello di piattaforma cloud, è emerso che l'interfaccia utilizzata dalle forze dell'ordine per accedere ai dati Flock inizialmente non imponeva l'autenticazione a più fattori (MFA). Questo ha creato un mercato nero per le credenziali di polizia compromesse (rubate tramite phishing o infostealer), permettendo a criminali di accedere in tempo reale ai movimenti dei veicoli tracciati dal sistema.

3.2 L'Esposizione su Shodan e i Rischi IoT

Il problema non è limitato a un singolo fornitore. Motori di ricerca come **Shodan** scansionano costantemente Internet per indicizzare dispositivi connessi. Una semplice ricerca su Shodan per termini come "webcamxp", "Axis" o "Hikvision" rivela migliaia di telecamere municipali e private esposte pubblicamente, spesso con interfacce di gestione accessibili tramite credenziali di default (admin/admin, root/12345).
Ricercatori hanno dimostrato che è possibile utilizzare Shodan e framework di exploit come Metasploit per identificare e accedere a telecamere vulnerabili su scala globale. Questo non solo viola la privacy dei cittadini ripresi, ma offre agli attaccanti la possibilità di pivotare all'interno della rete municipale, utilizzando la telecamera compromessa come testa di ponte per attaccare altri servizi interni non esposti direttamente su Internet.

4. Controllo del Traffico: Dallo Spoofing IR alle Vulnerabilità Radio

I sistemi di gestione del traffico sono essenziali per la sicurezza stradale, ma la loro architettura si basa spesso su tecnologie datate o protocolli privi di autenticazione. Le vulnerabilità in questo settore spaziano dalla manipolazione dei semafori tramite segnali ottici all'hacking delle reti radio di coordinamento.

4.1 La Vulnerabilità dei Sistemi di Preemption (Opticom)

I sistemi di *Emergency Vehicle Preemption* (EVP) permettono a veicoli di emergenza (polizia, ambulanze, vigili del fuoco) di forzare il verde ai semafori per ridurre i tempi di intervento. Il sistema più diffuso è **Opticom**.

4.1.1 Spoofing Ottico (Infraorosso)

I sistemi Opticom legacy utilizzano un emettitore stroboscopico a infrarossi (IR) montato sul veicolo. Il ricevitore sul semaforo rileva una specifica frequenza di lampeggio: tipicamente 14 Hz per la priorità alta (emergenza) e 10 Hz per la priorità bassa (trasporto pubblico).
La vulnerabilità risiede nella mancanza di autenticazione crittografica: il ricevitore obbedisce a qualsiasi sorgente di luce IR che lampeggi alla frequenza corretta con sufficiente intensità.

- **Il Ruolo del Flipper Zero:** Recentemente, il dispositivo multi-tool **Flipper Zero** è diventato famoso per la sua capacità di emettere segnali IR. Sebbene i video virali mostrino il Flipper Zero che cambia i semafori, la realtà tecnica è più sfumata. I LED IR integrati nel Flipper Zero non hanno la potenza necessaria per attivare i sensori Opticom (che sono montati in alto e progettati per rilevare segnali a centinaia di metri) da un marciapiede o da un'auto in movimento. Tuttavia, il Flipper può generare il segnale corretto (14 Hz).
- **MIRT (Mobile Infrared Transmitter):** Gli hacker hanno da tempo aggirato il limite di potenza costruendo dispositivi MIRT casalinghi (o acquistandoli illegalmente). Questi dispositivi utilizzano array di LED IR ad alta potenza alimentati dalla presa accendisigari dell'auto, replicando perfettamente lo strobo di un'ambulanza e garantendo il verde su richiesta. Questo rappresenta un rischio critico per la sicurezza stradale, potendo causare incidenti in intersezioni trafficate.

4.2 Attacchi alle Reti Radio 900 MHz

Oltre ai sistemi ottici, molti semafori moderni sono collegati in rete via radio per sincronizzare i tempi. Uno studio fondamentale condotto dall'Università del Michigan ha rivelato che molti di questi sistemi utilizzano radio nella banda ISM a 900 MHz senza crittografia.
Gli attaccanti, utilizzando un semplice laptop e una scheda radio compatibile, potevano:

1. **Sniffare il traffico:** Leggere i dati di telemetria e configurazione in chiaro.
2. Iniettare comandi: Inviare pacchetti per modificare i tempi di fase o forzare tutti i semafori al rosso (o al verde, sebbene i meccanismi hardware MMU - Malfunction Management Unit - impediscano solitamente il "verde su tutti i lati" per evitare collisioni dirette). L'accesso alla rete permetteva il controllo su centinaia di intersezioni da un unico punto, creando potenzialmente un blocco totale del traffico cittadino.

4.3 Il Protocollo VDV R09.16 e il Trasporto Pubblico

In Europa, e specificamente in Germania e paesi limitrofi, la priorità semaforica per autobus e tram è gestita tramite il protocollo radio **VDV R09.16**. I veicoli trasmettono "telegrammi" radio contenenti il numero di linea, la destinazione e la richiesta di priorità.
La ricerca ha dimostrato che questi telegrammi non sono né crittografati né autenticati.

- **Strumenti di Analisi:** Repository su GitHub come r09-receiver o script per GNU Radio permettono di decodificare questi messaggi utilizzando semplici ricevitori SDR.
- **Attacco di Spoofing:** Un attaccante con un dispositivo di trasmissione (come un HackRF o un Flipper Zero con modulo CC1101 esterno) può registrare e riprodurre (Replay Attack) o generare ex-novo telegrammi validi. Simulando l'arrivo di un autobus "fantasma" in ritardo, è possibile manipolare il ciclo semaforico per ottenere il verde per il proprio veicolo privato, a discapito del flusso di traffico legittimo. Questo tipo di attacco è particolarmente insidioso perché difficile da rilevare senza un monitoraggio attivo dello spettro radio.

5. Protocolli IoT Urbani: LoRaWAN e wM-Bus

Le Smart City si affidano a reti LPWAN (*Low Power Wide Area Network*) per connettere migliaia di sensori (parcheggi, rifiuti, qualità dell'aria). Due protocolli dominano questo spazio: LoRaWAN e Wireless M-Bus.

5.1 Vulnerabilità nelle Implementazioni LoRaWAN

LoRaWAN è progettato con la sicurezza in mente (crittografia AES-128), ma le implementazioni reali soffrono spesso di errori di configurazione.

- **ABP vs. OTAA:** Esistono due modi per connettere un dispositivo: *Over-The-Air Activation* (OTAA), che negozia chiavi di sessione sicure, e *Activation By Personalization* (ABP), dove le chiavi sono hardcoded. Molti deployment municipali usano ABP per semplicità. Tuttavia, ABP rende i dispositivi vulnerabili ai **Replay Attacks**: il contatore di frame si resetta al riavvio del dispositivo, permettendo a un attaccante di registrare un pacchetto valido e ritrasmetterlo in seguito, facendo credere alla rete che il sensore stia inviando nuovi dati.
- **Gestione delle Chiavi:** La sicurezza di LoRaWAN dipende interamente dalla segretezza della AppKey. Se queste chiavi vengono generate in modo predicibile (es. basate sul seriale) o trapelano da database insicuri, l'intera rete è compromessa.
- **Bit-Flipping:** Ricercatori hanno dimostrato che in certe condizioni è possibile manipolare i bit del payload cifrato senza invalidare il controllo di integrità (CRC), alterando i dati ricevuti dal server centrale (es. cambiare lo stato di un sensore di parcheggio da "occupato" a "libero").

5.2 Wireless M-Bus e la Banda 169 MHz in Italia

Come anticipato nella sezione AMI, il Wireless M-Bus è lo standard per i contatori in Europa. La specifica **UNI-TS 11291** in Italia regola l'uso della banda 169 MHz per il gas.

- **Jamming Selettivo:** La banda 169 MHz è una banda "stretta". Questo offre grande portata ma rende il segnale facile da disturbare. Un jammer di bassa potenza può oscurare le comunicazioni di un intero quartiere.
- **Replay Attack sui Comandi:** Se il contatore (o la valvola del gas smart) non implementa correttamente i contatori anti-replay o le finestre temporali, un attaccante potrebbe registrare un comando di "chiusura valvola" inviato dalla utility e ritrasmetterlo a piacimento, causando un'interruzione di servizio (DoS) fisica al cliente.

6. Strumenti di Analisi e Sfruttamento su GitHub e Reddit

La disponibilità di strumenti open source ha abbassato drasticamente la barriera d'ingresso per l'analisi di questi sistemi.

6.1 L'Ecosistema RTL-SDR e GNU Radio

La combinazione di hardware SDR economico e software open source è il fulcro della ricerca sulla sicurezza RF.

- **GNU Radio:** Una suite software che permette di costruire elaboratori di segnali complessi. Esistono moduli specifici (gr-inspector, gr-rds, ecc.) per analizzare segnali sconosciuti, demodularli e decodificarli. È lo strumento base per il reverse engineering di protocolli proprietari come quelli dei semafori o dei sensori parcheggio.
- **Universal Radio Hacker (URH):** Spesso citato su Reddit come alternativa più semplice a GNU Radio per analizzare protocolli replay e strutturare pacchetti bit a bit.

6.2 Repository GitHub Specifiche

- **rtlamr (bemasher):** Lo standard de facto per la lettura dei contatori Itron ERT. La sua semplicità d'uso (riga di comando, output JSON) lo rende ideale per l'integrazione in sistemi di sorveglianza domestica (Home Assistant) o per attività di wardriving.
- **wmbusmeters (weetmuts):** Decodificatore avanzato per wM-Bus. Supporta dongle RTL-SDR e hardware dedicato (IM871A). Le discussioni sulle "issue" di questo repository sono una miniera d'oro per comprendere le implementazioni reali (e difettose) dei vari produttori di contatori europei.
- **rpitx (F5OEO):** Un software rivoluzionario che permette di trasformare un pin GPIO del Raspberry Pi in un trasmettitore FM/SSB/AM senza hardware radio dedicato. Sebbene il segnale sia "sporco" (pieno di armoniche), è sufficiente per eseguire attacchi di replay o jamming su frequenze come 433 MHz o 868 MHz con un hardware da 35 dollari.

6.3 Il Ruolo di Reddit

Subreddit come r/RTLSDR, r/flipperzero e r/netsec fungono da centri di condivisione della conoscenza. Qui gli utenti condividono file di acquisizione (IQ files) di segnali sconosciuti, collaborano al reverse engineering di protocolli locali (es. telecomandi di cancelli, sensori meteo, contatori) e discutono le limitazioni reali degli strumenti (es. sfatando i miti sul Flipper Zero e i semafori).

7. Analisi Strategica e Conclusioni

L'indagine sulle tecnologie utilizzate dalle amministrazioni pubbliche dipinge un quadro di "città vulnerabile". L'adozione accelerata di tecnologie Smart City ha spesso preceduto la maturazione degli standard di sicurezza necessari a proteggerle.

Le criticità sistemiche identificate sono:

1. **Debito Tecnico nei Protocolli:** L'uso massiccio di protocolli legacy (Itron ERT, Opticom IR, Modbus su radio 900 MHz) che mancano nativamente di crittografia e autenticazione.
2. **Gestione Chiavi Deficitaria:** Anche quando i protocolli sono sicuri (LoRaWAN, wM-Bus), l'implementazione soffre di gestione delle chiavi statica, condivisa o derivabile, vanificando la protezione crittografica.
3. **Sicurezza Fisica Trascurata:** Dispositivi critici come le telecamere ALPR e i contatori sono esposti a manipolazione diretta, con porte di debug aperte e protezioni anti-tamper aggirabili.

Implicazioni Future:
Mentre le città si muovono verso l'automazione guidata dall'IA, il rischio di "data poisoning" diventa critico. Se un attaccante può spoofare i sensori di traffico o i contatori energetici su larga scala, può indurre gli algoritmi di gestione urbana a prendere decisioni errate, causando ingorghi artificiali, blackout mirati o errori nella pianificazione delle risorse.

Raccomandazioni:
È imperativo che le amministrazioni adottino un approccio "Secure by Design". Ciò include la sostituzione progressiva dei dispositivi legacy che trasmettono in chiaro, l'implementazione rigorosa di autenticazione a livello di messaggio per i comandi critici (es. semafori, valvole gas) e la segmentazione delle reti IoT dalle reti amministrative interne. Solo attraverso una revisione profonda dell'architettura di sicurezza sarà possibile realizzare la promessa della Smart City senza comprometterne la resilienza.

Glossario degli Acronimi:

- **AMI:** Advanced Metering Infrastructure (Infrastruttura di Misurazione Avanzata)
- **ALPR:** Automated License Plate Recognition (Riconoscimento Automatico Targhe)
- **ERT:** Encoder Receiver Transmitter (Protocollo Itron)
- **NILM:** Non-Intrusive Load Monitoring (Monitoraggio Non Intrusivo del Carico)
- **wM-Bus:** Wireless M-Bus (Standard europeo di metering)
- **LoRaWAN:** Long Range Wide Area Network
- **SDR:** Software Defined Radio
- **ADB:** Android Debug Bridge
- **EVP:** Emergency Vehicle Preemption (Prelazione Veicoli Emergenza)
- **UNI-TS:** Ente Nazionale Italiano di Unificazione - Specifica Tecnica

Stefano Rossi
IU2UEI

Bibliografia

1. Ben Jordan Exposes Severe Security Vulnerabilities in Flock ... https://www.privacyguides.org/news/2025/11/17/ben-jordan-exposes-severe-security-vulnerabilities-in-flock-surveillance-cameras/
2. Get your smart electric, water and gas meter scm readings into home assistant with a RTL-SDR https://community.home-assistant.io/t/get-your-smart-electric-water-and-gas-meter-scm-readings-into-home-assistant-with-a-rtl-sdr/93707
3. Tutorial: Replay Attacks with an RTL-SDR, Raspberry Pi and RPiTX https://www.rtl-sdr.com/tutorial-replay-attacks-with-an-rtl-sdr-raspberry-pi-and-rpitx/
4. Smart meter technology is privacy intrusive, researchers claim - Pinsent Masons https://www.pinsentmasons.com/out-law/news/smart-meter-technology-is-privacy-intrusive-researchers-claim
5. Privacy Preservation in Smart Meters: Current Status, Challenges and Future Directions https://pmc.ncbi.nlm.nih.gov/articles/PMC10098615/
6. Living in a Glass House: Privacy Implications of Smart Meter Data - Bass Connections https://bassconnections.duke.edu/news/living-glass-house-privacy-implications-smart-meter-data/
7. Why Is Smart Meter Data Privacy Important https://energy.sustainability-directory.com/question/why-is-smart-meter-data-privacy-important/
8. Privacy win! US court says Fourth Amendment protects smart meter data https://privacyinternational.org/news-analysis/2234/privacy-win-us-court-says-fourth-amendment-protects-smart-meter-data
9. Itron ERT - Digi International https://docs.digi.com/resources/documentation/digidocs/90001931/appendices/ert_technologies/ert_itron.html
10. bemasher/rtlamr: An rtl-sdr receiver for Itron ERT compatible smart meters operating in the 900MHz ISM band. - GitHub https://github.com/bemasher/rtlamr
11. wmbus · GitHub Topics https://github.com/topics/wmbus
12. rtl_433/README.md at master - GitHub https://github.com/merbanan/rtl_433/blob/master/README.md?plain=1
13. Flipper Zero Kills Smart Meter?? - Reverse Engineering News - June 13th 2023 - YouTube https://www.youtube.com/watch?v=QmNAA2bVo4Q
14. Using RF to read ITRON utility meters | DIY Solar Power Forum https://diysolarforum.com/threads/using-rf-to-read-itron-utility-meters.4038/
15. Wireless M-Bus 101: Demystifying Modes and Regional Application Profiles - Texas Instruments https://www.ti.com/document-viewer/lit/html/SSZT149
16. AN043: Wireless M-Bus Security - Radiocrafts https://radiocrafts.com/uploads/AN043_Wireless_M-Bus_security.pdf
17. Smart Grid wM-Bus RF Subsystem at 169 MHz - Texas Instruments https://www.ti.com/lit/pdf/tidu512
18. Truffa Contatori: ecco i 2 metodi (illegali!) per ridurre la Bolletta Luce e Gas https://luce-gas.it/attualita/truffa-contatori-2-metodi-illegali
19. Cos'è la truffa del magnete contatore gas? - Energit https://energit.it/cose-la-truffa-del-magnete-contatore-gas/
20. fornitura di gruppi di misura “smart meter” calibro g4 - | AMGA Legnano S.p.A.

https://www.amga.it/sites/default/files/Allegato%201%20-%20Specifiche%20Tecniche%20misuratori%20G4.pdf
21. Open Meter - Risposte ai quesiti pervenuti relativi al Piano di messa in servizio del sistema di smart metering 2G - Arera https://www.arera.it/fileadmin/allegati/operatori/smartmetering/e-distrRispostaquesiti_PMS2.pdf
22. FTC sought to probe Flock Safety's cybersecurity protections | SC Media https://www.scworld.com/brief/ftc-sought-to-probe-flock-safetys-cybersecurity-protections
23. Discover vulnerable cameras with Shodan | by Vasileiadis A. (Cyberkid) - Medium https://medium.com/@redfanatic7/discover-vulnerable-cameras-with-shodan-5aa49937348a
24. An Investigation of Vulnerabilities in Smart Connected Cameras - IEEE Xplore http://ieeexplore.ieee.org/document/8480184/
25. Your IP Camera Can Be Abused for Payments: A Study of IoT Exploitation for Financial Services Leveraging Shodan and Criminal Infrastructures https://cea.howard.edu/sites/cea.howard.edu/files/2025-06/Your_IP_Camera_Can_Be_Abused_for_Payments_A_Study_of_IoT_Exploitation_for_Financial_Services_Leveraging_Shodan_and_Criminal_Infrastructures%20%282%29.pdf
26. A Device to Turn Traffic Lights Green - Schneier on Security https://www.schneier.com/blog/archives/2023/02/a-device-to-turn-traffic-lights-green.html
27. Hacker Uncovers How to Turn Traffic Lights Green With Flipper Zero - The Drive https://www.thedrive.com/news/hacker-uncovers-how-to-turn-traffic-lights-green-with-flipper-zero
28. Safeguarding Smart Traffic Lights: A Top Priority for Smart Cities - Asimily https://asimily.com/blog/safeguarding-smart-traffic-lights-smart-cities/
29. Researchers demo hack to seize control of municipal traffic signal systems https://cse.engin.umich.edu/stories/researchers-demo-hack-to-seize-control-of-municipal-traffic-signal-systems
30. Green Lights Forever: Analyzing the Security of Traffic Infrastructure - USENIX https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf
31. tlm-solutions/r09-receiver: radio configuration running on the traffic stop boxes - GitHub https://github.com/tlm-solutions/r09-receiver
32. Low Powered and High Risk: Possible Attacks on LoRaWAN Devices | Trend Micro (US) https://www.trendmicro.com/en_us/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html
33. Security in LoRaWAN| Tektelic Blog https://tektelic.com/expertise/lorawan-security/
34. Le norme Tecniche per le verifiche metrologiche dei contatori gas https://smg-anie.it/wp-content/uploads/2019/10/2019-10-Fiameni_CIG.pdf
35. gnuradio/gnuradio: GNU Radio – the Free and Open Software Radio Ecosystem - GitHub https://github.com/gnuradio/gnuradio
36. gnuradio/gr-inspector: Signal Analysis Toolbox for GNU Radio - GitHub https://github.com/gnuradio/gr-inspector

37. CRC issues reported by wmbusmeters with HASS, nanoCUL and a F90 heat meter #1429 https://github.com/orgs/wmbusmeters/discussions/1429
38. F5OEO/rpitx: RF transmitter for Raspberry Pi - GitHub https://github.com/F5OEO/rpitx
39. Hacker Uncovers How to Turn Traffic Lights Green With Flipper Zero : r/cars - Reddit https://www.reddit.com/r/cars/comments/114r89e/hacker_uncovers_how_to_turn_traffic_lights_green/
40. AskNetsec - Reddit https://www.reddit.com/r/AskNetsec/
41. The flipper zero CANNOT control traffic lights. : r/flipperzero - Reddit https://www.reddit.com/r/flipperzero/comments/1f6ov16/the_flipper_zero_cannot_control_traffic_lights/