

[Case study] Internet of things e intelligenza artificiale per la prevenzione legionella: il caso Silver

Uno dei campi dove la tecnologia sta producendo sviluppi rapidi e interessantissimi è sicuramente quello dell'Internet of things (in italiano, l'internet delle cose), ovvero tutto quel mondo di oggetti fisici dotati di sensori, software o tecnologie che gli consentono di connettersi e comunicare dati tramite la rete web.

Ovviamente questa possibilità apre le porte anche all'automazione e all'intelligenza artificiale, prospettando scenari di miglioramento e progresso che fino a poco tempo fa erano pura fantascienza. Allo stesso tempo, queste tecnologie spalancano anche nuovi fronti di vulnerabilità e di rischio, che vanno affrontati adeguatamente.

Per avere un esempio concreto di potenzialità (e vulnerabilità) dell'IoT, ho parlato con Flavio Ravazzoni di Silver SNC, azienda che ha da poco presentato un innovativo sistema che integra il filtro Silver Care con la testata IoT Sentinel per contrastare il rischio di legionella negli studi dentistici.

[Oltre a questa chiacchierata, abbiamo tenuto anche un webinar su Youtube: lo trovi [a questo link](#)]

Rischio di contaminazione biologica

da legionella: automatizzare la gestione del rischio

Nel mondo della sicurezza industriale e sanitaria, il tema della legionella e della conformità normativa del trattamento acque rappresenta da anni un punto critico. Il settore odontoiatrico è uno dei campi dove la questione è più sentita: negli studi dentistici, infatti, l'acqua dei riuniti odontoiatrici (le classiche poltrone accessoriate) può ristagnare e diventare veicolo di contaminazioni batteriche e la nebulizzazione dello spray degli strumenti odontoiatrici (turbine e contrangoli) aumenta sensibilmente il rischio.

Le linee guida del Ministero della Salute sulla gestione del rischio da legionella prevedono controlli costanti, flussaggi quotidiani e documentazione puntuale. Si tratta di operazioni che, di solito, sono eseguite manualmente e sono quindi soggette a dimenticanze, oltre ad essere difficili da tracciare con costanza (anche in vista di eventuali ispezioni di controllo).

Silver Italia ha deciso di rispondere a questa necessità con il progetto Sentinel + SilverCare brevettato, che unisce Internet of Things (IoT) e filtrazione avanzata. Questa soluzione non solo monitora i parametri chiave dell'acqua per verificare eventuali contaminazioni, ma integra algoritmi di analisi e funzioni di notifica predittiva per rendere la sicurezza idrica proattiva e documentabile.

→ *Flavio, raccontaci di questo sistema. Come siete arrivati a svilupparlo? Come migliora la gestione della sicurezza idrica?*

Il punto di partenza è stata l'esigenza dei clienti, molti medici si lamentavano della quantità di documenti da compilare e la costante incertezza del dato che poteva essere attribuito a dimenticanze. I filtri antilegionella tradizionali sono 'passivi': hanno una scadenza temporale (12 mesi) o volumetrica. Tuttavia non c'è modo di sapere in tempo reale se sono ancora sicuri. *Con Sentinel passiamo da un dato empirico a un dato reale e verificabile.*

Ogni filtro SilverCare integra infatti un tag NFC (simile a quello delle carte di credito contactless) protetto da password sia in lettura che in scrittura. Questo chip contiene il numero di serie univoco, il lotto di produzione, la data di produzione, la data di installazione e tiene traccia dei litri filtrati in tempo reale. La testa IoT Sentinel legge queste informazioni, le invia al cloud e le mostra su un'app dedicata, che notifica quando il filtro è in scadenza.

Non solo: il sistema monitora costantemente i dati di temperatura, flusso e conducibilità ($\mu\text{S}/\text{cm}$) dell'acqua per prevenire i rischi: se, ad esempio, si registrano a lungo temperature dell'acqua troppo elevate, che favoriscono la proliferazione batterica, il sistema invia una notifica consigliando un flussaggio straordinario. In particolare, quando la temperatura supera i 30°C , Sentinel invia un alert immediato. La legionella infatti diventa dormiente sotto i 20°C , ma tra i 25°C e i 35°C trova le condizioni ideali per

[Case study] Internet of things e intelligenza artificiale per la prevenzione legionella: il caso Silver

proliferare. D'estate, all'interno dei riuniti, quando lo studio è chiuso per ferie, si possono raggiungere anche i 35°C, creando condizioni critiche.

Infine, con questi dati il sistema genera un report mensile che va a integrare il documento di valutazione dei rischi (DVRL) ed è fondamentale in caso di controlli da parte dell'ASL.

Un'altra funzionalità che i clienti apprezzano molto è il reminder delle procedure che garantiscono la conformità. La testata IoT del filtro rileva automaticamente se vengono eseguite le attività previste dalle linee guida (es. il flussaggio) e, in caso contrario, invia un promemoria all'operatore.

Sentinel consente inoltre di ricostruire con precisione millimetrica l'esposizione al rischio di ogni singolo paziente: il sistema registra infatti ogni evento con timestamp preciso al secondo, e permette di sapere quanti litri sono stati erogati, a che temperatura, con quale livello di conducibilità.

In caso di necessità – ad esempio se un paziente dovesse manifestare sintomi sospetti – il dentista può risalire esattamente alle condizioni dell'acqua utilizzata durante quella specifica visita. Questo livello di tracciabilità rappresenta non solo una garanzia di sicurezza, ma anche una protezione legale documentale per il professionista.

→ In questo momento state lavorando per

integrare nel sistema alcune funzioni dell'intelligenza artificiale. Vuoi spiegarci quali sono gli obiettivi e, anche, quali difficoltà state riscontrando?

Attualmente Sentinel utilizza algoritmi per analizzare i parametri idrici e segnalare anomalie rispetto al rischio da Legionella, ma stiamo progettando di introdurre l'IA per stimare il rischio di contaminazioni biologiche anche da altri patogeni come lo *Pseudomonas* o l'*Escherichia coli*.

Il pericolo più rilevante è quello dei falsi positivi, che potrebbero creare inutili allarmismi, oltre a costare tempo e denaro ai dentisti per approfondire le analisi e verificare il tutto. Questo è il motivo per cui stiamo procedendo con molta cautela, testando gli algoritmi a 360 gradi.

La prospettiva, comunque, è che la raccolta massiva di dati da migliaia di installazioni consenta di addestrare modelli predittivi sempre più accurati: analizzando correlazioni tra temperatura, conducibilità, pattern di utilizzo e risultati delle analisi periodiche, l'IA potrebbe identificare situazioni di rischio che sfuggirebbero all'occhio umano.

In ogni caso, l'approccio all'IA che stiamo adottando prevede che l'ultima parola resti sempre all'operatore umano: il sistema non prende decisioni in autonomia, si limita a segnalare eventuali situazioni di rischio e suggerire soluzioni. Inoltre, per garantire la trasparenza, andiamo a memorizzare tutti "i ragionamenti" dell'intelligenza artificiale che portano a sviluppare analisi

[Case study] Internet of things e intelligenza artificiale per la prevenzione legionella: il caso Silver

e ipotizzare le azioni di contrasto.



→Avete valutato scenari di guasto, perdita di connessione o la possibilità cyber-attacchi? Come li gestite a livello di sicurezza informatica e continuità operativa?

Sì, sono stati analizzati in modo approfondito sia gli scenari di guasto e perdita di connettività, sia le potenziali minacce di natura informatica, con l'obiettivo di garantire la sicurezza del sistema e la continuità operativa, in piena coerenza con i principi stabiliti dalla Direttiva Europea NIS 2 in materia di cybersicurezza.

[Case study] Internet of things e intelligenza artificiale per la prevenzione legionella: il caso Silver

La comunicazione con la piattaforma centrale avviene esclusivamente attraverso canali cifrati e autenticati. Dopo la prima autenticazione, basata su credenziali univoche integrate nel dispositivo, viene generato un token di sessione che consente le connessioni successive in modo sicuro e tracciato.

La comunicazione locale con l'app mobile è ulteriormente protetta da un livello di crittografia applicativa proprietaria, che assicura la riservatezza dei dati trasmessi anche in caso di intercettazione del traffico BLE.

Il dispositivo accetta solo firmware firmati digitalmente, grazie a un meccanismo di avvio sicuro (secure boot) che impedisce l'esecuzione di software non autorizzato. Inoltre, non espone servizi in ascolto verso l'esterno, riducendo drasticamente la superficie d'attacco.

In caso di perdita di connessione, il sistema esegue tentativi automatici di riconnessione con intervalli progressivi. In modalità offline, il dispositivo continua a operare autonomamente, memorizzando i dati su memoria flash interna da 64 Mbit. Tali dati sono protetti da controlli di integrità (CRC), che ne verificano la validità prima della successiva trasmissione.

Sono stati valutati e mitigati possibili scenari di attacco, tra cui intercettazioni, accessi non autorizzati e interruzioni del servizio. La protezione è assicurata da una combinazione di canali cifrati, autenticazione forte, gestione sicura delle chiavi e verifica dell'integrità del software, garantendo un elevato livello di resilienza e conformità ai requisiti della Direttiva NIS 2.

→ *Oltre all'integrazione dell'intelligenza artificiale, quali sono le prospettive per il futuro di questo progetto?*

In prima battuta, come dicevamo, vogliamo allargare la funzione predittiva del filtro grazie alle possibilità offerte dall'IA: l'idea è creare un sistema in grado di aiutare a prevenire un ampio spettro di rischi biologici sull'acqua.

L'altra direzione su cui vogliamo puntare in futuro è quella dell'allargamento del mercato. Noi lavoriamo da sempre nel settore odontoiatrico, ma questo tipo di prodotto è sicuramente interessante anche in ambito HO.RE.CA (Hotel, Ristoranti e Caffetterie) o, perché no, anche per installazioni domestiche...

Tre lezioni dal caso Silver su conformità, IA e sicurezza informatica

Dall'intervista con Flavio Ravazzoni sono emersi alcuni punti chiave che vanno oltre il singolo prodotto e offrono spunti utili per chiunque stia valutando l'integrazione di IoT e Intelligenza Artificiale in ambito industriale e sanitario. Proviamo a elencarli:

1. Dal dato empirico al dato oggettivo: la tecnologia come garante della conformità

Passare da controlli manuali e potenzialmente incompleti a un sistema che registra e notifica in tempo reale riduce l'errore umano e semplifica la conformità normativa. L'uso di sensori IoT, di uno storico digitale e di notifiche proattive offre un vantaggio enorme per la sicurezza, specialmente in contesti con obblighi documentali stringenti.

2. Intelligenza artificiale come supporto (ma con criterio)

Silver Italia ha scelto un approccio prudente, in cui l'IA verrebbe usata per analizzare parametri multipli e stimare il rischio, dove però la decisione finale resta in carico all'operatore umano. Questo è particolarmente interessante in un campo dove, come ci ha spiegato Flavio Ravazzoni, i falsi positivi possono paralizzare l'attività e avere ricadute importanti anche a livello di costi per le analisi.

3. Sicurezza informatica come prerequisito e non come optional

Un sistema IoT introduce rischi legati a cybersecurity, perdita dati e interruzioni di servizio. Silver li ha affrontati con attenzione alla sicurezza dati, al salvataggio in memoria dei dati anche offline e integrando

[Case study] Internet of things e intelligenza artificiale per la prevenzione legionella: il caso Silver

validazioni contro manomissione e corruzione dei dati. Si tratta di un buon esempio di come i sistemi di sicurezza digitale possano agire da vera protezione quando sono parte integrante della progettazione, non un'aggiunta successiva.

[Case study] Internet of things e intelligenza artificiale
per la prevenzione legionella: il caso Silver



Intelligenza artificiale, pericoli e valutazione rischi

Se vuoi saperne di più, dai un'occhiata al mio libro!

[Case study] Internet of things e intelligenza artificiale per la prevenzione legionella: il caso Silver

Lo trovi in vendita su Amazon, [qui](#).