Il nuovo modello integrato del software medicale: IEC 62304 & IEC 81001-5-1

Un software medicale può essere perfettamente conforme alla IEC 62304 e funzionare correttamente, fino a quando non viene compromesso da una vulnerabilità sfruttata in un contesto reale. Questo è il punto di rottura del modello tradizionale: la compliance alla safety non è più sufficiente a garantire la sicurezza del paziente in un ecosistema connesso.

Perché un sistema conforme alla IEC 62304 può comunque non essere sicuro nel contesto reale di oggi?

Nel software medicale moderno non esiste più una separazione reale tra safety e cybersecurity: il software medicale non fallisce solo per bug software, ma anche quando viene attaccato, con conseguenze dirette sulla sicurezza del paziente.

Dispositivi connessi, ecosistemi digitali sanitari e software distribuiti hanno cambiato radicalmente il modo in cui il rischio deve essere gestito: non basta più garantire esclusivamente che il software funzioni correttamente, ma che sia protetto da attacchi esterni.

È in questo contesto che la relazione tra IEC 62304 e IEC 81001-5-1 diventa centrale: non si tratta di due standard alternativi, ma di prospettive complementari dello stesso problema: costruire un software medicale affidabile, sicuro e resiliente attraverso il suo intero ciclo di vita.

IEC 62304: il fondamento del software medicale

La IEC 62304 rappresenta ancora oggi la base normativa per lo sviluppo del software medicale e continua, a vent'anni dalla sua pubblicazione, a essere un riferimento consolidato a livello internazionale per la gestione del ciclo di vita del software nei dispositivi medici.

Il suo obiettivo è definire un framework strutturato per il ciclo di vita del software, con un focus chiaro: garantire che il comportamento del software non introduca rischi inaccettabili per il paziente.

I concetti principali su cui la IEC 62304 pone maggiore attenzione sono:

- il ciclo di vita del software: dallo sviluppo alla manutenzione;
- la classificazione del rischio software: Classe A, B, C;
- la tracciabilità tra requisiti, implementazione e test;
- la gestione dei rischi;

- la gestione delle anomalie e delle modifiche.

In altre parole, IEC 62304 risponde a una domanda precisa:

“Il software funziona correttamente e in modo sicuro rispetto al suo design?”

È un modello fortemente orientato alla **safety**, cioè alla “libertà da rischi inaccettabili” [1], al fine di prevenire i danni derivanti da errori, difetti o malfunzionamenti interni.

IEC 81001-5-1: la cybersecurity nel ciclo di vita del software medicale

La IEC 81001-5-1 estende il modello tradizionale introducendo la dimensione della **cybersecurity nel ciclo di vita del software medicale**.

Non si limita a definire controlli tecnici, ma integra la sicurezza informatica nei processi di sviluppo e manutenzione. Un aspetto rilevante è che tale standard nasce dall'esperienza maturata nel mondo dell'automazione industriale e dei sistemi di controllo, recependo e adattando al contesto del software medicale i principi della IEC 62443-4-1, riferimento internazionale per il Secure Development Lifecycle nei sistemi industriali [2].

Gli aspetti principali riportati dalla IEC 81001-5-1 sono:

- Secure Development Lifecycle (SDL)
- Threat Modeling
- Requisiti di Security
- Gestione continua delle vulnerability
- Software Bill of Materials (SBOM)
- Patch & Update governance

Questi elementi non rappresentano soltanto buone pratiche di sviluppo sicuro, ma stanno assumendo un ruolo sempre più rilevante anche dal punto di vista regolatorio. L’applicazione della IEC 81001-5-1 è oggi sempre più utilizzata come riferimento per dimostrare la conformità ai requisiti generali di sicurezza dei regolamenti europei MDR e IVDR, essendo considerata una delle principali espressioni dello stato dell’arte per la gestione della cybersecurity nel software medicale. Questo approccio è inoltre coerente con le più recenti linee guida FDA sulla cybersecurity nei dispositivi medici.

La domanda che introduce è profondamente diversa rispetto alla IEC 62304:

“Il software rimane sicuro anche in un ambiente ostile, imprevedibile e in continua evoluzione?”

Qui il focus non è più sull'errore, ma sull'**attacco intenzionale** e sulla capacità del sistema di resistere, rilevare e reagire [3].

Dal software lifecycle al secure software lifecycle

Quando il modello si sposta da "errore interno" a "minaccia esterna", cambia anche la natura del rischio.

Un malfunzionamento non è più l'unica fonte di pericolo: ad esempio, un software di controllo infusionale può rispettare pienamente i requisiti della IEC 62304 e funzionare correttamente, ma diventare rischioso se un attaccante altera la logica di dosaggio sfruttando una vulnerabilità non gestita.

La correttezza funzionale non è più una garanzia sufficiente: un sistema può essere pienamente conforme e, al tempo stesso, vulnerabile a compromissioni esterne. È in questo spazio che entra in gioco la IEC 81001-5-1, che estende la prospettiva del ciclo di vita introducendo la dimensione della cybersecurity come parte integrante della gestione del rischio.

Nel software medicale moderno, integrare IEC 62304 e IEC 81001-5-1 non significa eseguire due processi separati.

La cybersecurity non introduce un lifecycle parallelo, ma una nuova dimensione del rischio all'interno delle stesse attività già previste dal ciclo di sviluppo software.

Ed è proprio qui che emerge la complementarità tra le due norme:

- IEC 62304 definisce la struttura del software lifecycle. Garantisce la correttezza del comportamento del software.
- IEC 81001-5-1 estende quel lifecycle introducendo requisiti di resilienza e cybersecurity. Garantisce la resilienza del software nel mondo reale.

La seguente tabella mostra come le attività del ciclo di vita IEC 62304 non vengano sostituite, ma estese dalla prospettiva della IEC 81001-5-1.

Fase del ciclo di vita del software	Approccio IEC 62304	Estensione IEC 81001-5-1
Requisiti	Requisiti funzionali e di safety	Requisiti di security e Access Control
Architettura	Architettura software e segregazione componenti	Defense-in-depth Design e Threat Modeling
Implementazione	Coding guidelines e controllo anomalie	Secure Coding Practices
Verifica	Functional testing e Risk Control Verification	Security testing, Vulnerability Assessment e Penetration testing
Manutenzione	Bug fixing e Change Management	Vulnerability Management e Patch Management
Attività post-market	Problem Resolution	Monitoraggio continuo delle vulnerabilità e gestione delle problematiche di sicurezza

Table 1: *Come IEC 81001-5-1 estende il ciclo di vita IEC 62304*

Impatto pratico: cosa cambia per chi sviluppa software medicale?

L'integrazione tra IEC 62304 e IEC 81001-5-1 non rappresenta solo un'evoluzione teorica del framework normativo. Cambia concretamente il modo in cui il software medicale viene progettato, verificato e mantenuto nel tempo.

Nel modello tradizionale, i **requisiti** software sono principalmente funzionali: descrivono cosa il sistema deve fare, come deve comportarsi e come verificarne la correttezza rispetto agli obiettivi di safety. Nel modello integrato, questo non è più sufficiente: ogni requisito deve essere valutato anche in termini di esposizione alle minacce, possibilità di abuso e accesso non autorizzato.

Lo stesso cambiamento si riflette nell'**architettura** software. Tradizionalmente, l'architettura viene costruita per garantire modularità, manutenibilità e segregazione delle funzioni safety-critical. Con l'introduzione della cybersecurity-by-design, entrano però nuovi concetti: riduzione della superficie di attacco, isolamento dei componenti critici e gestione dei trust boundaries diventano parte integrante delle decisioni architetturali.

Anche la fase di **verifica** evolve profondamente. La validazione non si limita più al functional testing o alla verifica dei controlli di rischio previsti dalla IEC 62304. Security testing, vulnerability assessment e penetration testing diventano attività sempre più rilevanti per dimostrare non solo che il software funzioni correttamente, ma anche che non sia facilmente sfruttabile.

È proprio a livello progettuale che emerge uno degli aspetti più delicati dell'integrazione tra i due standard. Un tema centrale nella progettazione di sistemi medicali critici è il possibile trade-off tra safety e security. In alcuni casi, requisiti di sicurezza informatica e requisiti di sicurezza clinica possono entrare in conflitto.

Un esempio tipico è l'implementazione di un blocco dell'accesso al dispositivo dopo un numero limitato di tentativi di autenticazione falliti: una misura efficace dal punto di vista della security (IEC 81001-5-1), ma potenzialmente problematica in scenari clinici di emergenza, dove il ritardo nell'accesso può introdurre un rischio non accettabile per il paziente (IEC 62304).

Nella pratica progettuale, questo tipo di conflitto viene spesso gestito attraverso soluzioni architetturali e procedurali che bilanciano i due requisiti, ad esempio prevedendo modalità di accesso alternative in contesti critici, con livelli diversi di autenticazione e controllo.

L'integrazione tra IEC 62304 e IEC 81001-5-1 è proprio ciò che consente di rendere espliciti e analizzabili questi delicati trade-off di design, supportando una valutazione strutturata del rischio che tenga conto simultaneamente di safety e cybersecurity lungo tutto il ciclo di vita del sistema.

Una trasformazione significativa emerge anche nelle attività di **manutenzione** e **post-market**. Nel modello tradizionale, la manutenzione riguarda principalmente correzione dei bug, gestione delle modifiche ed evoluzione controllata del software. Nel modello integrato, questa visione si estende alla gestione continua delle vulnerabilità, all'analisi dell'esposizione a nuove minacce e al rilascio di patch di sicurezza con priorità variabile.

Nel **post-market** non si tratta più soltanto di monitorare anomalie software o problemi funzionali, ma di mantenere una sorveglianza continua sulle vulnerabilità e sui rischi di sicurezza emergenti. Il monitoraggio continuo delle vulnerabilità, la gestione delle problematiche di sicurezza e un processo strutturato di aggiornamento e correzione diventano parte integrante del ciclo di vita del software.

Conclusioni

La relazione tra IEC 62304 e IEC 81001-5-1 non rappresenta semplicemente l'evoluzione di due normative parallele, ma un cambiamento molto più profondo nel modo in cui il software medicale viene progettato, mantenuto e gestito nel tempo.

Per anni il modello dominante è stato costruito attorno alla safety: garantire che il software funzionasse correttamente e non introducesse rischi clinici derivanti da errori o malfunzionamenti.

La vera evoluzione introdotta dall'integrazione tra IEC 62304 e IEC 81001-5-1 non è l'aggiunta di nuovi controlli tecnici, ma è il passaggio da un modello di software safety a un modello di software trust, in cui il software lungo tutto il suo ciclo di vita deve essere:

- corretto,
- resiliente,
- monitorabile,
- aggiornabile,
- sicuro

Per questo motivo, il futuro del software medicale non sarà definito dalla capacità di applicare singolarmente standard diversi, ma dalla loro integrazione in un unico framework operativo di gestione del rischio digitale.

IEC 62304 definisce come costruire software medicale affidabile. IEC 81001-5-1 definisce come mantenerlo sicuro in un ambiente reale e dinamico. Insieme, definiscono il nuovo modello integrato del software medicale.

Fonti:

1. IEC 62304:2006 - Medical device software — Software life cycle processes
2. IEC 81001-5-1:2021 - Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle
3. Security-by-Design in Medical Software (IEC 81001-5-1)

Keywords: IEC 81001-5-1, IEC 62304, IEC 62443-4-1, Cybersecurity, Software Lifecycle, Software as Medical Device, Secure Development Lifecycle, Software Security, Software Safety

Autore: Maria Santoro, R&D Product Specialist - Medical Devices