# Security-by-Design: l'approccio alla cybersecurity secondo lo Standard IEC 81001-5-1

Nel contesto della progettazione di dispositivi medici, il tema della sicurezza cyber è centrale. Nell'ambito di questa rubrica, abbiamo affrontato due aspetti rilevanti: il primo in ambito regolatorio, con la compliance a *Medical Device Regulation* (MDR) 2017/745 [1]; il secondo più tecnico, elencando alcune delle soluzioni hardware e software utili a soddisfare i requisiti di cybersecurity [2]. In questo terzo approfondimento, vedremo come il concetto della *security-by-design* venga esposto nello standard IEC 81001-5-1:2021 [3], e successivamente come applicarlo durante l'intera durata del ciclo di vita del software medicale.

## *Lo Standard IEC 81001-5-1: Definizioni e Scopi*

Partiamo dalla definizione di Software Medicale, o Health Software: *"Software sviluppato per gestire, mantenere o migliorare la salute degli individui, o fornire cura, oppure sviluppato allo scopo di essere incorporato in un dispositivo medico"* [3]. Questa definizione raccoglie una vasta gamma di tipologie di software: da quello presente all'interno dei dispositivi medici attivi, passando per software medicale *standalone*, fino ad arrivare ad infrastrutture IT più vaste.

Lo scopo dello standard IEC 81001-5-1 è quello di stabilire quali siano le attività necessarie a garantire la sicurezza del software medicale durante i processi inerenti al ciclo di vita dello stesso, nonché la sicurezza dei processi stessi.

La Sicurezza, quindi, rappresenta un concetto chiave, un obiettivo da perseguire da parte di chi si occupa di progettazione, verifica e maintenance del Software Medicale: da qui l'approccio Security-by-Design, per cui la Sicurezza è presente fin dall'inizio della progettazione del sistema Software.

Su diversi aspetti, questo standard richiama i concetti relativi al ciclo di sviluppo del Software come Dispositivo Medico espressi nella IEC 62304:2006 "Medical device software - Software life cycle processes" [4]. Ad esempio, se nella IEC 62304 si parla di *Software Requirements*, nella IEC 81001-5-1 si espongono invece i *Security Requirements*: questi ultimi sono requisiti relativi al Software Medicale, ma finalizzati a descrivere gli aspetti di sicurezza dello stesso.

Come riportato in Tabella 1, si possono identificare diversi parallelismi tra i due standard, che descrivono i medesimi concetti ma l'uno con un approccio volto alla *Safety*, l'altro alla *Security*.

| | IEC 62304 | IEC 81001-5-1 |
|---|---|---|
| **Ambito** | Medical device software | Health software and health IT systems safety, effectiveness and security |
| **Focus** | Safety | Security |
| **Requisiti** | Software Requirements | Security Requirements |
| **Design Architetturale** | Software Architectural Design | Defense-in-depth Design |
| **Attività di integrazione e verifica** | Software integration and verification | Security integration and verification |

***Tabella 1***: I parallelismi tra gli standard IEC 62304 e IEC 81001-5-1.

## *Design Architetturale attraverso la Defense-in-Depth*

Nell'ambito del Design Architetturale del Software, la *Defense-in-Depth* è l'approccio proposto: al fine di garantire la sicurezza degli assets, devono essere previsti diversi gradi di protezione del sistema, secondo un'architettura difensiva che si sviluppa su livelli. Questo tipo di struttura garantisce che la probabilità di un attacco sia ridotta, e, qualora invece si verifichi, che l'impatto sia minimo, specialmente sugli assets di maggiore valore. L'analogia che viene spontanea è quella con i sistemi di difesa delle città medievali: il sistema di mura di difesa si sviluppava su livelli concentrici, ognuno progressivamente più sicuro del precedente. La difesa del sistema deve essere variegata, cioè prevedere diversi tipi di protezione su più livelli, e indipendente, ovvero garantire che, nel caso in cui una parte del sistema venga colpita da un cyber-attacco, le altre restino integre e disponibili.

Lo standard inoltre identifica le cosiddette *Secure Design Best Practices*:

- *Documentazione dei Trust Boundaries*: il sistema deve essere segmentato in diverse aree e lo scambio di informazioni tra queste deve avvenire con un certo livello di fiducia. Il Trust Boundary è il confine superato il quale il livello di fiducia aumenta o diminuisce.

- *Principio del privilegio minimo*: ogni attore deve avere accesso alla porzione minima del sistema che gli garantisca di svolgere la sua attività. Ad esempio, l'utente finale di un dispositivo medico non deve poter accedere al database che contiene le password dei diversi dispositivi, oppure al log degli accessi al server ospedaliero.
- *Utilizzo di software sicuri*: è fortemente consigliata l'adozione di software e frameworks sicuri e certificati.
- *Riduzione delle superfici di attacco*: attraverso l'analisi dei rischi, devono essere individuate le vulnerabilità del sistema e di conseguenza le soluzioni da mettere in atto per ridurre i danni in caso di attacco.

## *Analisi e Management dei Rischi legati alla Sicurezza*

Al fine di identificare le possibili vulnerabilità del sistema, il processo di analisi dei rischi associati alla sicurezza deve essere svolto con la massima attenzione. La metodologia proposta nello standard IEC 81001-5-1 è quella del *Threat Modeling*, che prevede l'identificazione delle potenziali minacce e le mitigazioni del rischio associato ad ognuna di esse.

Lo standard non identifica un modello preciso da seguire. Esistono infatti vari framework, tra cui il più diffuso è il metodo STRIDE, acronimo di *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service*, *Elevation of Privilege*. Questo elenco rappresenta diversi tipi di minacce, ognuna delle quali deve essere analizzata per ogni interfaccia del sistema. Se la minaccia rappresenta un rischio concreto per gli assets, devono essere messe in atto mitigazioni del rischio opportune. Il risultato dell'analisi STRIDE è la descrizione dei potenziali attacchi, con la relativa riduzione del rischio messa in atto a proteggere il sistema.

Altri metodi utilizzati per il Threat Modeling sono:

- DREAD: Damage, Reproducibility, Exploitability, Affected users and Discoverability
- CVSS: Common Vulnerability Scoring System
- Attack-defense Tree
- OCTAVE
- VAST: Visual, Agile, Simple Threat modeling.

## *Conclusioni*

In conclusione, lo standard IEC 81001-5-1 propone una metodologia volta a garantire un Software sicuro attraverso l'intero ciclo di vita, proteggendo gli assets di valore da eventuali attacchi malevoli.

## *Fonti:*

1. Cybersecurity nei dispositivi medici: cosa richiede il MDR 2017/745 - Teoresi Group
2. Cybersecurity per dispositivi medici: soluzioni hardware e software per sistemi embedded a prova di regolamento europeo - Teoresi Group
3. 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
4. IEC 62304:2006 - Medical device software — Software life cycle processes

**Keywords: IEC 81001-5-1, IEC 62304, Security-by-Design, Defense-in-Depth, Cybersecurity, Software as Medical Device, Threat Modeling, STRIDE, Security Risk Management, Vulnerability, Trust Boundary, Health Software**

Autore: Gaia Di Federico, Progettista Elettronico R&D