Security-by-Design: cybersecurity approach according to the IEC 81001-5-1 Standard

In the context of medical device design, the topic of cybersecurity is pivotal. Within this series of technical articles, we addressed two relevant aspects: the first in the regulatory field about the compliance with *Medical Device Regulation* (MDR) 2017/745 [1]; the second with a technical approach, listing some of the hardware and software solutions useful to meet cybersecurity requirements [2]. In this third in-depth article, we will see how the concept of *security-by-design* is exposed in the IEC 81001-5-1:2021 standard [3], and subsequently how to apply it throughout the entire medical software life cycle.

IEC 81001-5-1: Definitions and Purposes

Let's start with the definition of Medical Software, or Health Software: *"Software intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device"* [3]. This definition encompasses a wide range of software types: from those present within active medical devices, through standalone medical software, up to larger IT infrastructures.

The purpose of the IEC 81001-5-1 standard is to establish what activities are necessary to ensure the security of medical software in the processes inherent to its life cycles, as well as the security of the processes themselves.

Security, therefore, represents a key concept, a goal to be pursued by those involved in the design, verification and maintenance of Medical Software: hence the Security-by-Design approach, for which Security is present from the early stages of development.

On several aspects, this standard recalls the concepts related to the development cycle of Software as Medical Device expressed in IEC 62304:2006 "Medical device software - Software life cycle processes" [4]. For example, if IEC 62304 speaks of *Software Requirements*, IEC 81001-5-1 instead sets out *Security Requirements*: the latter are requirements relating to Medical Software, but aimed at describing security aspects.

As shown in Table 1, several correspondences can be identified between the two standards: they talk about the same concepts, but the first has an approach aimed at *Safety*, while the other is focused on *Security* aspects.

	IEC 62304	IEC 81001-5-1
Scope	Medical device software	Health software and health IT systems safety, effectiveness and security
Focus	Safety	Security
Requirements	Software Requirements	Security Requirements
Architectural Design	Software Architectural Design	Defense-in-depth Design
Integration and verification activities	Software integration and verification	Security integration and verification

Table 1: The parallels between the IEC 62304 and IEC 81001-5-1 standards.

Architectural Design through Defense-in-Depth

In the context of Software Architectural Design, *Defense-in-Depth* is the proposed approach: to ensure assets security, different degrees of protection of the system must be provided, according to a defensive architecture developed on several levels. This type of structure ensures that the probability of an attack is reduced, and if it does occur, that the impact is minimal, especially on the most valuable assets. The analogy that comes spontaneously is that with the defense systems of medieval cities: the system of defense walls was built on concentric levels, each progressively safer than the previous one. The defense of the system must be variegated, to provide different types of protection on several levels, and independent, to ensure that, if one part of the system is hit by a cyber-attack, the others remain intact and available.

The standard also identifies the so-called *Secure Design Best Practices*:

- *Documentation of Trust Boundaries*: The system must be segmented into different areas and the exchange of information between them must take place with a certain level of trust. The Trust Boundary is the boundary beyond which the level of trust increases or decreases.

- *Principle of least privilege*: each actor must have access to the minimum portion of the system that guarantees them to carry out his activity. For example, the end user of a medical device should not be able to access the database that contains the passwords of the different devices, or the access log to the hospital server.
- *Use of secure software*: the adoption of secure and certified software and frameworks is strongly recommended.
- *Reduction of attack surfaces*: through risk analysis, system vulnerabilities must be identified and consequently threat mitigations shall be implemented to reduce the probability of an attack.

Analysis and Management of Security Risks

In order to identify possible vulnerabilities in the system, the process of analyzing the risks associated with security must be carried out with the greatest attention. The methodology proposed in the IEC 81001-5-1 standard is that of *Threat Modeling*, which involves the identification of potential threats and mitigations of the risk associated with each of them.

The standard does not identify a precise model to follow. In fact, there are various frameworks, among which the most widespread is the STRIDE method, acronym for *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service*, *Elevation of Privilege*. This list represents several types of threats, each of which must be analyzed for each interface of the system. If the threat poses a material risk to assets, appropriate risk mitigations must be put in place. The result of the STRIDE analysis is the description of potential attacks, with the relative reduction of the risk chosen to protect the system.

Other methods used for Threat Modeling are:

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

Conclusion

In conclusion, the IEC 81001-5-1 standard proposes a methodology aimed at ensuring secure software throughout its entire life cycle, protecting valuable assets from malicious attacks.

Sources:

1. Cybersecurity in medical devices: what MDR 2017/745 requires - Teoresi Group
2. Cybersecurity for medical devices: hardware and software solutions for embedded systems that are compliant with European regulations - 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

Author: Gaia Di Federico, R&D Electronic Engineer