IEC 81001-5-1: The standard for secure health sc

The new cybersecurity standard IEC 81001-5-1 is **just about to be published**. It focuses on how IT security account in the software life cycle.
As a special standard for health software, it supplements IEC 82304-1 and IEC 62304 among others, and can to be closed. The EU is currently planning to harmonize IEC 81001-5-1, with a current target date of May 24th
In this article, you will find out:

- whether IEC 81001-5-1 is relevant for you,
- what the standard requires,
- whether this will result in double work due to overlapping e.g. with IEC 62304, and
- how IEC 81001-5-1 can be rated overall.

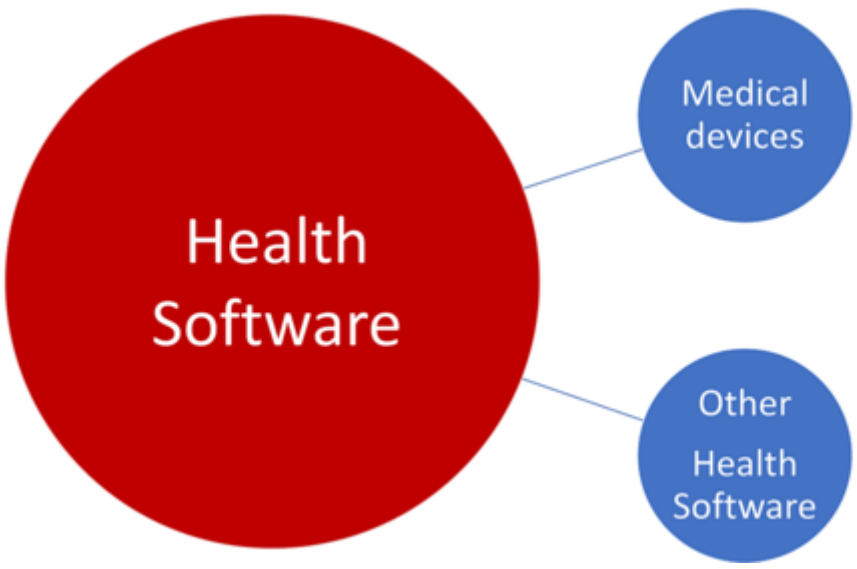
CONTENTS

1. For whom IEC 81001-5-1 is important

IEC 81001-5-1 targets manufacturers of “Health Software”. This does not just include medical devices, it also includes other software used in the health sector.

Examples of health software that is not a medical device:

- Fitness apps for sports purposes
- Yoga apps for wellbeing
- Software for the provision of general nutrition counselling for healthy individuals
- Care planning software for basic care



Health Software includes both medical devices and other health software

The standard therefore does not just target manufacturers of medical devices, but also manufacturers of software for the health sector, or “Health Software”.

Definition of health software according to IEC 81001-5-1

“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"

(Source: IEC 81001-5-1 3.15)

IEC 81001-5-1 also includes stakeholders other than manufacturers: the introduction highlights how important bilateral communication with other organization (such as healthcare delivery organizations) is. This exchange is specifically considered in the standard.

> *"This document applies to the development and maintenance of Health Software by a manufacturer, but recognizes the critical importance of bilateral communication with organizations (e.g. healthcare delivery organizations, HDOS) who have security responsibilities for the Health Software and the systems it is incorporated into, once the software has been developed and released."*

In this respect, IEC 81001-5-1 also deals with the relationship with Healthcare Delivery Organizations (HDOs), which share responsibility for cybersecurity with manufacturers. This aims to ensure, for example, that operators have enough information on the safe operation of the products from manufacturers.

For example, operators must inform manufacturers of problems with IT security promptly so they can work t quickly.

Definition of HDO

> *"facility or enterprise such as a clinic or hospital that provides healthcare services"*
>
> (Source: ICE 81001-5-1, 3.16; identica

2. Measures to ensure secure software in IEC 81001-5-1

IEC 81001-5-1, entitled "Health software and health IT systems safety, effectiveness and security — Part 5-1: S product life cycle" covers the entire life cycle of health software: from development through to post-marketin the general information and specifications for the life cycle processes such as software development and soft standard's annexes also provide tips on best practice.
Many of the requirements in IEC 81001-5-1, though, are not new for manufacturers of medical devices and in redundant: the standard takes content from numerous existing specifications such as the framework of the N Standards and Technology (NIST), guidance documents from the FDA and IEC 62443 ("Industrial communication networks - IT security for networks and systems"). Manufacturers who have taken into account the latest developments to date and co surprised
The requirements of IEC 81001-5-1, however, are noteworthy because, unlike comparable standards (such as specifically tailored to the field of health software.
We have put together more information on the general requirements for IT security in the health care sector

a) Overview: What IEC 81001-5-1 regulates

General requirements

The general specifications of IEC 81001-5-1 for software relate to:

- Quality management system
  (e.g. responsible persons and their qualifications, procurement processes for software components, review of the accompanying documents)
- Risk management for IT security
- Note about the degree to which the risk lies with the operator in the case of software components

Processes

IEC 81001-5-1 contains specifications for the following processes:

- Software development process
- Software maintenance process
- Process to manage security risks
- Software configuration management process
- Software problem resolution process

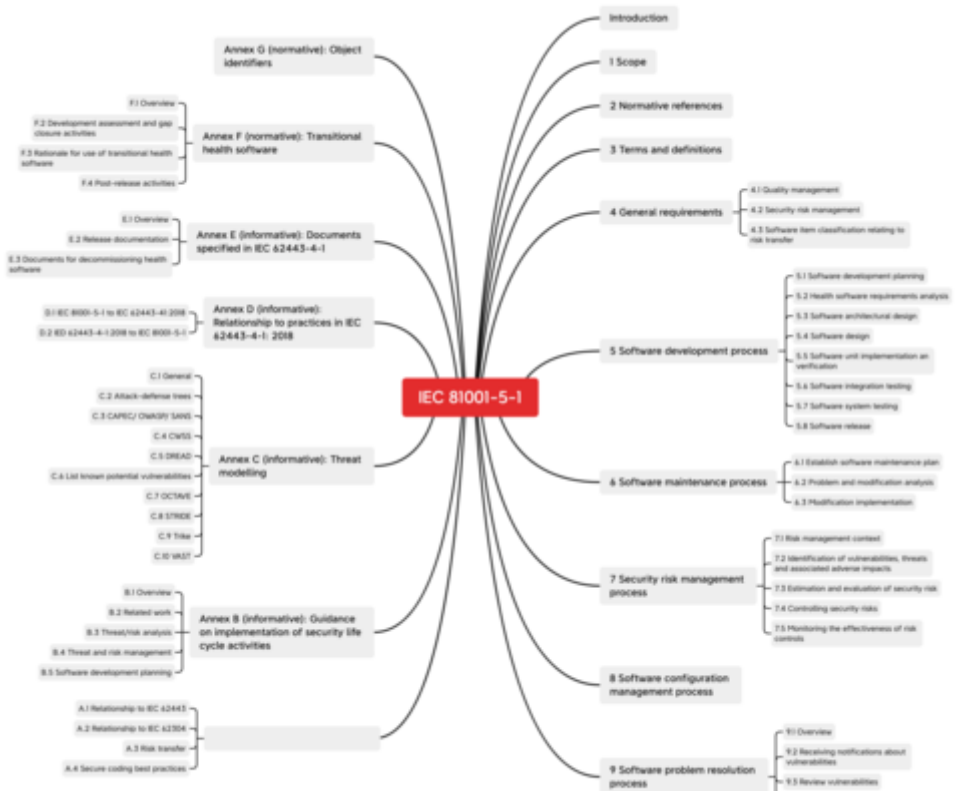
These processes overlap with the processes in IEC 62304, but are specifically tailored to health software. More information on the relationship with IEC 62304 can be found below.

Support for implementation in the annexes

The annexes also offer a guide for how best to handle many relevant topics.
These include:

- Best practice for secure coding (e.g. not using software components that are known to cause a security risk)
- Security life cycle (e.g. threat analysis)

- Threat and risk management
- Planning the development of health software
  (among other things a guide to the analysis of the special requirements of health software)



CONTENTS

b) Particularly noteworthy manufacturer requirements

Cybersecurity process in the quality management system

According to IEC 81001-5-1, manufacturers must implement a cybersecurity process into their quality manag

With regard to this, the standard states:

> *"The manufacturer" shall perform security activities in the product life cycle on the basis of an establish management system."*

IEC 81001-5-1 therefore leaves the question of whether cybersecurity is implemented as a separately described process or the corresponding activities are integrated into existing quality management system processes open.

Suppliers and "upstream cybersecurity"

"Upstream cybersecurity" (in other words IT security relating to collaboration with third parties) has proven to be very relevant in practice:

Suppliers can represent a security risk for health software. It is often small companies with limited knowledge of the field of software security that take insufficient security measures at a company level or during the development process.

Hackers are aware of this weakness. They focus on these gateways. Manufacturers should therefore carry out a critical evaluation of their suppliers as a matter of urgency.

Continuous improvement

Health software must be continuously improved. If manufacturers identify a cybersecurity problem on the market, they must provide a security update or patch if necessary,

but this is generally not sufficient. Manufacturers need to ask themselves the question of whether the cybersecurity problem occurred as a result of a cause in the quality management system as part of the continuous improvement process. Corresponding corrective actions must be implemented in their processes if necessary.

For example, network connection ports that were accidentally left open may have enabled an attack to be carried out. In this case, the manufacturer must ensure that the product is delivered with closed ports and they must provide for port scans in their product verification process.

External tests

The title of 5.7.5 of IEC 81001-5-1 is *Managing conflicts of interest between testers and developers*. It is about achieving objectivity when evaluating test results. The standard feels that the greatest possible objectivity is achieved through having testers and developers that are separate from one another. This can be achieved by having an internal testing team that is separate to the development team or by using

external testing providers.

3. IEC 81001-5-1 within the set of standards

a) Gaps that IEC 81001-5-1 could close

Although IEC 81001-5-1 does not bring with it any groundbreaking innovations, it does specify the regulations of other standards more precisely for health software.

Health software may differ from other medical devices or software in terms of

- the role of the operator (healthcare delivery organization),

- the link to risk management according to ISO 14971 in the field of safety, and

- the reference to other standards from the health environment.

IEC 82304-1 and ISO 82304-2

To date, only **IEC 82304**-1 and **ISO 82304-2** were specifically for health software. IEC 82304-1, though, only s of the software life cycle (IEC 82304-1: “General requirements for product safety”. It primarily focuses on dang the product itself (such as danger to humans caused by defective software).

In contrast to this, IEC 81001-5-1 requires a development process according to ISO 62304 and ISO 82304 and activities are necessary in the respective phases of the development process to ensure cybersecurity. In this r as a supplement to IEC 82304-1 and IEC 62304.

ISO 82304-2 differs in terms of the scope and the objective, as ISO 82304-2 relates specifically to quality label

MDR

IEC 81001-5-1 also closes the gaps in specific standards for medical device manufacturers who provide softwa MDR. While all other topics from Annex I MDR area already broadly covered by standards that are harmonize this is missing for the field of IT security (Annex I point 17.2 MDR).

In addition to the MDR, to date there was only the Guideline MDCG 2019-16 (Guidance on Cybersecurity for n summarizes the requirements of the MDR in terms of cybersecurity and provides reflections and backgrounc contains specific and compact requirements for manufacturers.

Otherwise, to date manufacturers have had to rely on guides such as **that of the Johner Institute** or the standard IEC 62443-4-1, which is from outside the industry. IEC 62443-4-1, for example, does not just take into account the special features of medical devices.

Relationship with IEC 62443 and IEC 62304

The overlaps with the related (but not specific to medical devices) standards IEC 62443-4-1 and IEC 62304 were taken into account in the draft of IEC 81001-5-1. The relationship with both standards is explicitly explained in Annex A of IEC 81001-5-1.

- **IEC 62443-4-1**
  - IEC 62443 relates to “industrial communication networks – IT security for networks and systems”.
  - IEC 81001-5-1 is based on the requirements of IEC 62443-4-1, but the corresponding regulations have been tailored more specifically to health software (concepts, reference to corresponding standards such as ISO 14971).
  - Which adjustments these are and which needs to be taken into account, including to achieve compliance with IEC 62443-4-1, is listed in Annex A.
- **IEC 62304**
  - **IEC 62304** addresses the software life cycle but does not say anything about the specific requirements in terms of IT security
  - This standard was also taken into account when developing IEC 81001-5-1. This new standard assumes that the life cycle is already defined according to IEC 62304 and supplements the measures needed for IT security at the relevant points in the cycle.

b) EU plans for harmonization

Since IEC 81001-5-1 covers important points under EU law about which there has as yet not been a standard, it is already on the **EU’s application list for harmonization (heading “Attachment”, pos. 27)** before it is even published. The implementation is planned for May 24th, 2024.

CONTENTS

4. What IEC 81001-5-1 has done well, and what it has done less well

What is good

- **Compact, but comprehensive**
  At around 60 pages, IEC 81001-5-1 is relatively compact. Nevertheless, the standard provides a very nice and extensive overview of all necessary activities, precautions, requirements and documentation.
- **Clearly delineated requirements**
  The levels of liability are clear (e.g. “manufacturer can”, “… should”, “…. shall”). The document also lists clear requirements that mean the document can be used for an implementation strategy.
- **Focus on what is most important**
  The standard successfully balances providing an overview and providing more detail. Where it does not reference to other guidelines. This makes it more “digestible” than an extensive framework such as mos National Institute of Standards and Technology (NIST).

Where there is room for improvement

IEC 81001-5-1 addresses numerous point that have already been discussed in other documents, e.g. in the gu Institute on cybersecurity (**IT Security Guideline**), but the new IEC standard remains abstract in many place

One example of this is the “Intended product security context”. Here, the standard merely states that this mu be more helpful to describe the practical implementation in detail, which could look something like this:

> *“- the manufacturer has identified all neighboring systems (e.g. medical devices, IT systems, cloud servic to the product.*"
>
> *"- the manufacturer has created a list of roles (people, neighboring systems) that may interact with the product.*
>
> (Source: IT Secur

In this respect, IEC 81001-5-1 is helping to implement the procedural landscape. More specific details in some manufacturers to meet the requirements. Other documents such as the **IT Security Guideline** should there checklists.

5. Conclusion

All in all, IEC 81001-5-1 is a very important standard that was long overdue. Uniform standards for cybersecurity in the field of medical devices have been needed for a long time. That was why the Johner Institute provided an **IT Security Guideline** some time ago. This is now confirmed by the newly published draft standard.

The fact that the standard is intended for harmonization with EU regulations even before it is published also shows how much a standard of this type is needed.

IEC 81001-5-1 will also help the notified bodies. They will be able to use the standard as the basis for audits of the quality management system and the technical documentation in the future.

Manufacturers of medical devices should implement IEC 81001-5-1 as soon as it is published. It will already be significant as the “state of the art” even before the official harmonization.

You can use the **IT Security Guideline** by the Johner Institute as a guide when looking at the security of your health software. You can contact us at any time if you have any questions about the topic. You can use this **form** or simply send an **email**.

CONTENTS