INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

IEC 81001-5-1
Edition 1.0 2021-12

Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle

INTERPRETATION SHEET 1

This interpretation sheet has been prepared by subcommittee 62A: Common aspects of medical equipment, software, and systems, of IEC technical committee 62: Medical equipment, software, and systems.

The text of this interpretation sheet is based on the following documents:

DISH	Report on voting
62A/1692/DISH	62A/1706/RVDISH

Full information on the voting for the approval of this interpretation sheet can be found in the report on voting indicated in the above table.

_____

This interpretation sheet is intended to clarify the following:

a) Requirements which are needed to provide essential ACCOMPANYING DOCUMENTATION to the operators of the HEALTH SOFTWARE product regarding the transfer of risk related to software items from the MANUFACTURER to the responsible organization or operator.

b) Requirements which are needed to maintain SECURITY of the HEALTH SOFTWARE product

Interpretation of IEC 81001-5-1:2021, Introduction, 0.2

The HEALTH SOFTWARE is part of a connected and complex healthcare ecosystem, which is integrated into a surrounding HEALTH IT SYSTEM and HEALTH IT INFRASTRUCTURE. ISO 81001-1 provides a definition of the sociotechnical ecosystem in which the HEALTH SOFTWARE operates in, and how to reference the security aspect of the HEALTH SOFTWARE within an IT-system inside a broader HEALTHCARE SYSTEM.

IEC 81001-5-1:2021-12/ISH1:2025-11(en)

ICS 11.040.01, 35.240.80

Interpretation of IEC 81001-5-1:2021, 4.1

4.1.7 Disclosing SECURITY-related issues

NOTE 1 This activity is related to 9.3 through 9.5 where additional supporting details are provided.

NOTE 2 On a) "CVSS" and "ranking" address the rating of the severity and characteristics of security vulnerabilities.

4.1.9 ACCOMPANYING DOCUMENTATION review

NOTE For clarification, the documents mentioned with "SECURITY guidelines" are detailed in 5.8.2 and 5.8.7.

Interpretation of IEC 81001-5-1:2021, 4.3

4.3 SOFTWARE ITEM classification relating to risk transfer

NOTE 1 (foundations, intentions):

Table 1 – SOFTWARE ITEM classification mapped to affected clauses

Activity Category	Clause	MAINTAINED	SUPPORTED (includes MAINTAINED)	REQUIRED (includes SUPPORTED)
Quality Management	4.3 Software Item classification related to risk transfer (Note: clarifying roles and responsibilities in support)	X	X	X
Software development	5.2.3 Security Risks for REQUIRED SOFTWARE	X*	X*	X
Software maintenance	6.3.1 SUPPORTED SOFTWARE update documentation	X*	X	
	6.3.2 MAINTAINED SOFTWARE security update delivery	X		
	6.3.3 MAINTAINED SOFTWARE security update INTEGRITY	X		

* Implied inclusion in clause since IEC 81001-5-1:2021, Clause 3 explicitly defines SUPPORTED SOFTWARE "includes MAINTAINED SOFTWARE" and REQUIRED SOFTWARE "includes SUPPORTED SOFTWARE".

SOFTWARE ITEM classification related to risk transfer from 4.3 is clarified as follows:

a) The SOFTWARE ITEM classification categories are nested, but only to ensure clauses that explicitly mention a category are also understood to include the nested categories. Table 1 above notes all clauses that detail requirements specific to a SOFTWARE ITEM classification and notes the implicit inclusion of nested categories. Further requirements of SOFTWARE ITEM classification that are not explicit in an associated clause are not part of this document.

b) The manufacturer shall apply risk transfer activities for all SOFTWARE ITEMS according to their associated category. An organization's policy and procedures may choose different terms for these classifications if clauses citing requirements for these SOFTWARE ITEM classifications are satisfied. Risks for all SOFTWARE ITEMS should be identified and managed (5.2.3), updates for SOFTWARE ITEMS controlled by the manufacturer or PRODUCT user should be communicated (6.3.1) and updates to manufacturer provided SOFTWARE ITEMS should be made available (6.3.2) and have verifiable integrity (6.3.3). For 4.3, any declaration of conformance, or internal policy/procedure, should state the alternative terminology leveraged and how it maps to the specific SOFTWARE ITEM categories when alternative approaches to MAINTAINED, SUPPORTED and REQUIRED SOFTWARE are utilized.

The following clarifying statements help illustrate how the implicit software category nesting affects the clauses that explicitly mention one of the SOFTWARE ITEM classifications:

1) 5.2.3 applies for all 3 categories of software. SECURITY Risks from REQUIRED, SUPPORTED and MAINTAINED software should be identified and managed.

2) 6.3.1 applies to MAINTAINED software in addition to SUPPORTED software. PRODUCT users also should be notified about updates to MAINTAINED software and SUPPORTED SOFTWARE.

3) 6.3.2 & 6.3.3 applies only to MAINTAINED software.

NOTE 2 (explain practical consequences)

It is generally understood that along with purchasing, installing, and using HEALTH SOFTWARE, the risk related to its use over time (often constrained by legal provisions) transitions to the operator. For the purposes of information security, MANUFACTURERS depend on information from suppliers of SOFTWARE ITEMS (being a logical part of the HEALTH SOFTWARE) for certain post-market activities, such as 9.3, to maintain a secure state.

Similarly, operators depend on information from MANUFACTURERS regarding which SOFTWARE ITEMS are intended to be used with HEALTH SOFTWARE product, which kind of support the MANUFACTURER declares for these SOFTWARE ITEMS and which are not supported. Therefore, aspects of risk transfer of the HEALTH SOFTWARE from the MANUFACTURER to the operator is addressed by the categories introduced in 4.3 and the associated clauses citing the SOFTWARE ITEM classifications.

For technical or organizational reasons, it is possible that operators wish to be in control of when or whether a new security update is being installed on related systems where the MANUFACTURER does not provide the security updates. As an example, updates to a database shared among several devices and services require good planning such that both selection and timing of updates cannot be left in the hands of a single MANUFACTURER. This is a reason for introducing the category of SUPPORTED SOFTWARE.

For technical or organizational reasons, MANUFACTURERS in some cases are not in a position to obtain security notifications or security updates for certain SOFTWARE ITEMS. This is a reason for introducing the category of REQUIRED SOFTWARE. When vulnerabilities for such (“end-of-support” or otherwise unsupported) software become known, MANUFACTURERS can still select other means of maintaining the overall security of the HEALTH SOFTWARE product.

Over the HEALTH SOFTWARE LIFE CYCLE, the MANUFACTURER can update the SOFTWARE ITEM categorization, which is typically done by downgrading SOFTWARE ITEMS from MAINTAINED to SUPPORTED, from MAINTAINED to REQUIRED or SUPPORTED to REQUIRED. When this happens, the requirements from associated clauses shall be evaluated to ensure appropriate risk transfer from MANUFACTURERS to operators.

NOTE 3 (distinguish from transitional software)

For clarification, *Transitional* (Annex F) is an attribute applied to the whole HEALTH SOFTWARE product – independent of the above categories for SOFTWARE ITEMS. The term “transitional“ does not specify a fourth category for SOFTWARE ITEMS – rather it is a circumstance in which the MANUFACTURER developed the HEALTH SOFTWARE product before IEC 81001-5-1 existed. Therefore, *Transitional HEALTH SOFTWARE* (Annex F) is an alternative approach for evaluating HEALTH SOFTWARE that was “developed without following all of the ACTIVITIES defined in of IEC 81001-5-1:2021, Clause 4 to Clause 9.

Interpretation of IEC 81001-5-1:2021, 6.1

6.2.1 Monitoring public incident reports

NOTE For clarification, this activity specifies “review of the information” rather than review of the source.