TECHNICAL REPORT

ISO/TR 24971

Second edition
2020-06

Medical devices — Guidance on the application of ISO 14971

Dispositifs médicaux — Recommandations relatives à l'application de l'ISO 14971

Reference number
ISO/TR 24971:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The *procedures* used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives-and-policies).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see the following URL: www.iso.org/iso/foreword.html.

This document was prepared jointly by Technical Committee ISO/TC 210, *Quality management and corresponding general aspects for medical devices*, and Subcommittee IEC/SC 62A, *Common aspects of electrical equipment used in medical practice*.

This second edition cancels and replaces the first edition, which has been technically revised. The main changes compared to the previous edition are as follows:

— The clauses of ISO/TR 24971:2013 and some informative annexes of ISO 14971:2007 are merged, restructured, technically revised, and supplemented with additional guidance.

— To facilitate the use of this document, the same structure and numbering of clauses and subclauses as in ISO 14971:2019 is employed. The informative annexes contain additional guidance on specific aspects of *risk management*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides guidance to assist *manufacturers* in the development, implementation and maintenance of a *risk management process* for *medical devices* that aims to meet the requirements of ISO 14971:2019, *Medical devices — Application of risk management to medical devices*. It provides guidance on the application of ISO 14971:2019 for a wide variety of *medical devices*. These *medical devices* include active, non-active, implantable, and non-implantable *medical devices*, software as *medical devices* and *in vitro diagnostic medical devices*.

The clauses and subclauses in this document have the same structure and numbering as the clauses and subclauses of ISO 14971:2019, to facilitate the use of this guidance in applying the requirements of the standard. Further division into subclauses is applied where considered useful. The informative annexes contain additional guidance on specific aspects of *risk management*. The guidance consists of the clauses of ISO/TR 24971:2013 and some of the informative annexes of ISO 14971:2007, which are merged, restructured, technically revised, and supplemented with additional guidance.

Annex H was prepared in cooperation with Technical Committee ISO/TC 212, *Clinical laboratory testing and in vitro diagnostic test systems*.

This document describes approaches that *manufacturers* can use to develop, implement and maintain a *risk management process* conforming to ISO 14971:2019. Alternative approaches can also satisfy the requirements of ISO 14971:2019.

When judging the applicability of the guidance in this document, one should consider the nature of the *medical device(s)* to which it will apply, how and by whom these *medical devices* are used, and the applicable regulatory requirements.

Medical devices — Guidance on the application of ISO 14971

1 Scope

This document provides guidance on the development, implementation and maintenance of a *risk management* system for *medical devices* according to ISO 14971:2019.

The *risk management process* can be part of a quality management system, for example one that is based on ISO 13485:2016[24], but this is not required by ISO 14971:2019. Some requirements in ISO 13485:2016 (Clause 7 on product realization and 8.2.1 on feedback during monitoring and measurement) are related to *risk management* and can be fulfilled by applying ISO 14971:2019. See also the ISO Handbook: *ISO 13485:2016 — Medical devices — A practical guide*[25].

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 14971:2019, *Medical devices — Application of risk management to medical devices*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 14971:2019 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

NOTE The defined terms in ISO 14971:2019 are derived as much as possible from ISO/IEC Guide 63:2019[20] which was developed specifically for the *medical device* sector.

4 General requirements for *risk management* system

4.1 *Risk management process*

ISO 14971:2019 requires that the *manufacturer* establishes, implements, documents and maintains an ongoing *risk management process* throughout the *life cycle* of the *medical device*. The required elements in this *process* and the responsibilities of *top management* are given in ISO 14971:2019 and explained in further detail in this document.

4.2 Management responsibilities

4.2.1 *Top management* commitment

Top management has the responsibility to establish and maintain an effective *risk management process*. It is important to note the emphasis on *top management* in ISO 14971:2019 *Top management* has the power to assign authorities and responsibilities, to set priorities and to provide resources within the organization. Commitment at the highest level of the organization is essential for the *risk management process* to be effective.

If the *manufacturer's* organization consists of separate entities, for example business units or divisions, then *top management* can refer to those individuals who direct and control the entity implementing the *risk management process*. Each entity can have its own *risk management process* (and its own quality management system).

4.2.2 Policy for establishing criteria for *risk* acceptability

ISO 14971:2019 requires *top management* to define and document the policy for establishing criteria for *risk* acceptability. Annex C provides detailed guidance on how to define such a policy and which elements should be included, such as applicable regulations, relevant international standards, the generally acknowledged *state of the art* and known stakeholder concerns. Annex C also explains the relation between the policy and the criteria for *risk* acceptability and how these criteria are used in *risk control* and *risk evaluation*.

The policy can allow specific criteria for each type of *medical device* (or *medical device* family). This can depend on the characteristics of the *medical device* and its *intended use* (including the intended patient population). ISO 14971:2019 requires that the policy provides guidelines on how to establish the criteria for acceptability of the overall *residual risk*.

4.2.3 Suitability of the *risk management process*

ISO 14971:2019 requires *top management* to review the suitability of the *risk management process* at planned intervals. The review of the suitability is a high-level review of the *risk management process* and can include reviewing the following aspects, for example:

— the effectiveness of the implemented *risk management procedures*;

— the adequacy of the criteria for *risk* acceptability, which can imply the need for an adaptation of the criteria for *risk* acceptability for specific *medical devices*; and

— the effectiveness of the feedback loop of the production and *post-production* information (see 10.4).

4.3 Competence of personnel

Ensuring the assignment of competent personnel is a responsibility of *top management*. Examples of the personnel that can be involved in specific *risk management* tasks and the relevant knowledge and experience supporting effective completion of the associated tasks are given in Table 1.

Some *risk management* activities can be performed by external consultants or specialists. The required competence should be documented as well as the *objective evidence* of the fulfilment of these requirements.

Table 1 — Examples of competent personnel and relevant knowledge and experience

Personnel or function	Knowledge and experience
Risk management owner	*Medical device risk management process*
Engineer or scientist	*Medical device* technologies, design and operating principles
Operations	Manufacturing *processes*
Supply-chain management	Sources of material and services, including outsourced *processes*
Medical or clinical expert	Clinical evaluation methodologies and requirements Use in medical practice, including *benefits*, *hazardous situations* and possible *harm*

Table 1 *(continued)*

Personnel or function	Knowledge and experience
Regulatory affairs	Regulatory requirements pertaining to *safety* and *risk management* in countries/regions where the *medical device* is intended to be marketed
Quality assurance	Quality management systems and quality practices
Packaging, storage, handling and distribution	*Hazards* and *risk control* measures in relation to packaging, storage, handling and distribution
Service engineer, biomedical engineer or medical physicist	*Hazards* and *risk control* measures in relation to installation, maintenance, repair, calibration, service and support *processes* and practices
Post-production	Customer complaints and adverse event reporting, post-market surveillance
Information services	Data mining *processes*, methodologies for literature search
All individuals involved in the review and approval of the *records*	Expertise in the functional area for which they are reviewing and approving

Consider the need to include the following topics in the education of *risk management* experts:

— management of a *risk management* program for *medical devices*;

— ethics, *safety*, security and liability;

— concepts of *risk, risk* acceptability and *benefit-risk* analysis;

— probability and statistics for *risk management* and reliability;

— *risk management* and reliability in design and development;

— relevant standards and regulations;

— *risk estimation* including methods to determine the *severity* and probability of occurrence of *harm*;

— *risk assessment* methodology;

— methods for *risk control*;

— methods for verifying the effectiveness of *risk control* measures;

— methods for analysing production and *post-production* information.

4.4 *Risk management* plan

4.4.1 General

The *risk management* plan describes the scope of the *risk management* activities, the responsibilities and authorities of those involved, the criteria for *risk* acceptability, the production and *post-production* information to be collected and reviewed for the *medical device*, and all *risk management* activities that are carried out during the entire product *life cycle*. The *risk management* plan can be a separate document, or it can be integrated with other documentation, e.g. quality management system documentation. It

can be self-contained or it can reference other documents, such as planning of clinical, biological or usability evaluations or planning of *post-production* activities.

The *risk management* plan is a "living document" that will be reviewed and updated throughout the *life cycle* of the *medical device* as new information becomes available. The information should be collected on a continuous basis, even after the last *medical device* is sold and placed on the market. ISO 14971:2019 requires that changes to the *risk management* plan be recorded in the *risk management file*.

The extent of planned activities and the level of detail of the *risk management* plan should be commensurate with the level of *risk* associated with the *medical device*. The requirements in ISO 14971:2019 are the minimum requirements for a *risk management* plan. *Manufacturers* can include other items such as time-schedule, *risk analysis* tools, or a rationale for the choice of specific *risk* acceptability criteria.

4.4.2 Scope of the *risk management* plan

The scope identifies and describes the *medical device* and the *life cycle* phases for which each element of the plan is applicable.

Some of the elements of the *risk management* plan can apply to the product realization *process* (design, development and production of the *medical device*). Other elements can apply to the production and *post-production* phase (such as installation, use, maintenance, decommissioning and disposal of the *medical device*).

4.4.3 Assignment of responsibilities and authorities

The *risk management* plan identifies the personnel or functions with responsibility for the execution of specific activities related to *risk management* (see Table 1). In addition, the *risk management* plan identifies the individuals with appropriate authority to review and approve *risk management* decisions and actions. This can entail assignment of personnel familiar with the unique characteristics of the *medical device* (or *medical device* family) and their possible relevance to *safety*. This assignment can be included in a resource allocation matrix defined for the specific *life cycle* phase and the activities covered in the scope of the plan.

4.4.4 Requirements for review of *risk management* activities

The *risk management* plan details how and when the *risk management* activities will be reviewed for a specific *medical device* (or *medical device* family). This should include the review method, the responsible individuals or functions, who is required to participate in the review, and how the review results are managed. The results of the review of planned *risk management* activities will be consolidated in the *risk management* report (see Clause 9). The requirements for the review of *risk management* activities can be part of other quality system review requirements, such as design and development review (see ISO 13485[24]).

4.4.5 Criteria for *risk* acceptability

Criteria for *risk* acceptability are established according to the *manufacturer's* policy for determining acceptable *risk*. This includes criteria for situations where the probability of occurrence of *harm* cannot be estimated, in which case the criteria for *risk* acceptability can be based on the *severity* of *harm* alone. The criteria can be common for categories of similar *medical devices* (or *medical device* families).

It is important to establish the criteria for *risk* acceptability before starting the *risk assessment*. Otherwise, the results of the *risk assessment* could influence the decision when establishing the criteria.

See Annex C for further guidance and examples of criteria that are derived from the policy and applied in *risk evaluation*.

4.4.6 Method to evaluate overall *residual risk* and criteria for acceptability

The method to evaluate the overall *residual risk* and the criteria for its acceptability are derived from the *manufacturer's* policy for establishing criteria for *risk* acceptability. ISO 14971:2019 requires that the method and the criteria be stated in the *risk management* plan for the particular *medical device* under development. Some inputs for and considerations on the evaluation of overall *residual risk* are listed in Clause 8.

4.4.7 *Verification* activities

The *risk management* plan specifies how the two *verification* activities required per 7.2 of ISO 14971:2019 are carried out. The *risk management* plan can detail the *verification* activities explicitly or by reference to other plans.

Verification of implementation of *risk control* measures can be part of design review, approval of specifications, design and development *verification* in a quality management system, or other *verification* activities in a quality management system.

Verification of the effectiveness of *risk control* measures can be part of design and development *verification* in a quality management system. It can require the collection of clinical data, usability studies, etc., as part of design and development validation in a quality management system.

4.4.8 Activities related to collection and review of production and *post-production* information

ISO 14971:2019 requires the *manufacturer* to establish a system to actively collect and review information about the *medical device* in the production and *post-production* phases and to review this information for relevance to *safety*. Thus, it is important that the *risk management* plan includes the activities necessary to establish this system. *Manufacturers* should understand that the information to be collected can be voluminous and comes from many disparate sources. Consequently, robust *processes* should be used to analyse the information and to identify trends that could otherwise go undiscovered, so that appropriate conclusions and actions can be taken. Statistical techniques should be considered to assist in the processing of the collected data.

The system to actively collect and review information includes monitoring and receiving feedback such as complaints and adverse event reports. In addition, the system should include active solicitation of feedback from users and collection of other relevant information. The *manufacturer* should consider the extent of these activities and determine which activities are appropriate for the particular *medical device*.

For example, limited monitoring might be sufficient for *medical devices* with a long history of use and well understood *risks*. For *medical devices* involving novel treatments (for example new *intended uses*) or innovative technologies and possibly with less understood *risks*, more elaborate monitoring including post-market clinical follow-up (PMCF) studies could be warranted to understand the issues that can arise in the actual use of the *medical device*. Further guidance is provided in Clause 10.

The method for collecting production and *post-production* information can be part of established quality management system *processes* (see for example 8.2 of ISO 13485:2016[24]). While a reference to an existing *procedure* can be sufficient in some cases, any requirements specific to the *medical device* under consideration should be documented in the *risk management* plan. Details of the monitoring activities and any planned PMCF studies should also be specified in the *risk management* plan.

The frequency of review of the collected information should be commensurate with the *risk* and can also depend on the number of *medical devices* on the market, the number of incidents reported and the *severity* of *harm* reported. The collection and review should continue during the expected lifetime of the *medical device*.

4.5 *Risk management file*

ISO 14971:2019 requires the *manufacturer* to establish and maintain a *risk management file*, which contains *records* and other documents created during *risk management* activities for the *medical device*

throughout its *life cycle* from initial conception until final decommissioning and disposal. The individual clauses in ISO 14971:2019 specify what *records* and related documents are to be maintained as part of the *risk management file*. The *risk management file* should provide the information necessary for the review of the *risk management process* at any phase in the *medical device's life cycle*.

The *risk management file* can be structured and organized for one type of *medical device* or for a *medical device* family. It is important that the *risk management records* can be assembled in a timely fashion throughout the *life cycle* of the *medical device*, as the information could be used during the *life cycle* to support other activities and decision making, for example during review of production and *post-production* information, evaluation of the effect of a change to the *medical device*, or during audits.

The *risk management file* is a logical construct. It is not necessary that the *risk management file* physically contains all the required *records* and related documents. The *records* and related documents can be part of files required by other systems such as the *manufacturer's* quality management system. The *records* and related documents can exist in any format or media (hard copy, electronic *records*, etc.).

ISO 14971:2019 requires traceability for each identified *hazard* to the *risk analysis*, *risk evaluation*, implementation and *verification* of *risk control* measures, and the evaluation of *residual risk*. Traceability is a requirement to prove that all identified *hazards* have been completely addressed in the *risk management process*. A traceability tool can be used to provide an index to each document in the *risk management file* providing information on the identified *hazard*. Such an index can be useful in the management of *risk* knowledge concerning the identified *hazards*. This index could be used in later activities such as the evaluation of overall *residual risk* and the review of production and *post-production* information. Traceability should be updated as new information becomes available and when the *medical device* is changed.

See Annex G for guidance on building a *risk management file* for *medical devices* that were designed without using ISO 14971:2019.

5 *Risk analysis*

5.1 *Risk analysis process*

The *risk analysis process* consists of the following steps, which are explained in further detail in the next subclauses:

— description of the *intended use* of the *medical device* and *reasonably foreseeable misuse*;

— identification of the characteristics of the *medical device* that are related to *safety*;

— identification of *hazards* and *hazardous situations* associated with the *medical device*;

— estimation of *risks* for each *hazardous situation*.

5.2 *Intended use* and *reasonably foreseeable misuse*

The *intended use* should take into account information such as:

— the intended medical indication, e.g. treatment or diagnosis of type 2 diabetes mellitus, cardiovascular disease, bone fracture, infertility;

— patient population, e.g. age groups (adults, children, adolescent, elderly), gender (male, female), or disease state;

— part of the body or type of tissue interacted with, e.g. leg or arm;

— user profile, e.g. patient, lay person, health care provider;

— use environment, e.g. home, hospital, intensive care unit; and

— operating principle, e.g. mechanical piston driven syringe, X-ray imaging, MR imaging, subcutaneous drug delivery.

Reasonably foreseeable misuse is defined as use of the *medical device* in a way not intended by the *manufacturer*, but which can result from readily predictable human behaviour. This can relate to *use error* (slip, lapse or mistake), intentional acts of misuse, and intentional use of the *medical device* for other (medical) applications than intended by the *manufacturer*. Cases of *reasonably foreseeable misuse* can be identified during design and development by an analysis of simulated use, for example by applying a usability engineering *process*, or during the *post-production* phase by an analysis of actual use. *Reasonably foreseeable misuse* can be identified throughout the *life cycle* of a *medical device*, including iterations of design activities, during which the *manufacturer's* ability to anticipate potential misuse progressively increases.

The usability engineering *process* can help to determine whether a particular misuse is reasonably foreseeable or not, for example by observation during usability testing. The usability test might reveal that users could routinely use the *medical device* in a manner that is not according to the *manufacturer's* instructions. This misuse can occur due to poor working culture, inadequate *risk* perception, limited knowledge of the consequences, or because operating *procedures* are not clear.

The following example illustrates a case of *reasonably foreseeable misuse* that was identified and analysed by application of a usability engineering *process*. More information on usability engineering can be found in IEC 62366-1[16] and IEC TR 62366-2[17].

EXAMPLE A single-use *medical device* is designed to be used only once, but it is reasonably foreseeable that some users might attempt to reuse the *medical device*. Therefore, warnings against reuse and indications of the possible *harm* resulting from reuse were included in the *accompanying documentation*. Application of usability engineering according to IEC 62366-1[16] demonstrated that this information for *safety* would be effective, i.e. users would know the correct use and understand the *risk* of reusing the *medical device*. However, the usability evaluation also showed that some users are likely to disregard this information and intentionally reuse the *medical device*. Intentional reuse can be considered abnormal use, which is beyond the scope of the usability engineering *process*, because the associated *risks* cannot be controlled in the user interface (see 3.1 and 3.26 of IEC 62366-1:2015[16]). Since this behaviour can be considered *reasonably foreseeable misuse*, the *risks* from such reuse are analysed in the *risk management process* and evaluated against the criteria for *risk* acceptability according to ISO 14971:2019. It could be necessary to implement *risk control* measures outside the user interface.

5.3 Identification of characteristics related to *safety*

It is important to identify the characteristics of the *medical device* that could affect *safety*. These characteristics can be qualitative or quantitative and can be bound by certain limits. The questions in Annex A cover many aspects of *medical devices* and can assist in identifying the characteristics related to *safety*. For every question, it is indicated which factors should be considered in further detail, with the ultimate goal of identifying all *hazards* and *hazardous situations* associated with the *medical device*. The list of questions in Annex A should not be used as a check list. It can also be helpful to review available information and literature, including adverse event reports, for similar *medical devices*.

A *manufacturer* can identify the performance or the functions of the *medical device* that are necessary to achieve its *intended use* or that could affect *safety*, and consider whether any *hazardous situations* could occur, if any of these functions did not perform properly.

5.4 Identification of *hazards* and *hazardous situations*

5.4.1 *Hazards*

A *hazard* is a potential source of a *harm*. Depending on the specific situation, *hazards* can have different origins/natures. Examples of *hazards* are electricity, moving parts, infectious bacteria, chemicals, gases, sharp edges, high currents, temperature, and ionising radiation.

Hazards associated with the *medical device* can be deduced from the *intended use* and *reasonably foreseeable misuse* as determined in 5.2 and the characteristics related to *safety* as determined in 5.3. Annex C of ISO 14971:2019 provides guidance that can help in identifying *hazards* and sequences of

events that can lead to *hazardous situations*. Annex H provides similar guidance for *IVD medical devices*, where incorrect diagnostic information can lead to indirect *risks* to patients.

5.4.2 *Hazardous situations* in general

Medical devices only cause *harm* if a sequence of events occurs that results in a *hazardous situation*, which then causes or leads to *harm*. Sequences of events can include a chronological series of causes and effects, as well as combinations of concurrent events. A *hazardous situation* occurs when people, property or the environment are exposed to one or more *hazards*.

Hazardous situations can arise even when there are no faults, i.e. in the normal condition for the *medical device* when it is performing as intended. *Hazardous situations* can be intrinsic aspects of certain therapies. For example, an automated external defibrillator (AED) delivers an electric shock to the patient as part of its normal operation. Similarly, wound cauterization involves the application of high energy to a wound site, and a scalpel has a sharp blade intended to make incisions.

Annex A provides guidance in the form of questions on the characteristics of the *medical device* that could affect *safety*. Those characteristics can help in identifying *hazards* and *hazardous situations*. Annex B provides guidance on several techniques that can support a *risk analysis*. Annex H provides specific guidance on identifying *hazards* and *hazardous situations* for *in vitro diagnostic medical devices*.

5.4.3 *Hazardous situations* resulting from faults

In cases where a *hazardous situation* only occurs due to a fault, the probability of a fault occurring is not the same as the probability of the occurrence of *harm*. A fault can initiate a sequence of events but does not necessarily result in a *hazardous situation*. A *hazardous situation* does not always result in *harm*.

It is important to understand that there are generally two types of fault that can lead to a *hazardous situation*: random and systematic faults.

5.4.4 *Hazardous situations* resulting from random faults

Random faults are typically due to physical or chemical causes such as corrosion, contamination, thermal stress, and wear-out. For many random faults, a numerical value can be given for the probability that the fault will occur. Some examples of random faults are:

— the failure of a part such as an integrated circuit in an electronic assembly;

— the contamination of an IVD reagent leading to incorrect results;

— the presence of an infectious or toxic substance in or on a *medical device*.

NOTE A quantitative estimate can only be applied to biological *risks* if sufficient information is known about the *hazard* and the circumstances affecting the probability of the *hazardous situation* occurring, for example in the use of sterility assurance levels.

5.4.5 *Hazardous situations* resulting from systematic faults

A systematic fault can be caused by an error in any activity. It will systematically give rise to a failure when some particular combination of inputs or environmental conditions arises, but will otherwise remain latent.

Errors leading to systematic faults can occur in any part of the *medical device* such as hardware and software in electro-mechanical *medical devices*. Systematic faults in labelling can lead to *use errors* for any *medical device*. These systematic faults can be introduced at any time during a *medical device*'s development, manufacture or maintenance. Some examples of systematic faults are:

— an incorrectly rated fuse fails to prevent a *hazardous situation*: the fuse rating could have been incorrectly specified during design;

— a software database does not provide for the condition of full database: if the database is full, it is not clear what the software will do, with possible consequence that the system will simply replace existing data with new data;

— a fluid, used during the production of a *medical device*, has a boiling point lower than body temperature: residues of the fluid can, in certain circumstances, be introduced into the blood, possibly leading to an embolism;

— the antibody in a hepatitis assay does not detect some variants of the virus;

— inadequately designed environmental control leads to contamination with a toxic substance or an infectious agent;

— the user's manual is written so that if a maintenance routine is performed according to the instructions, the user could be injured (e.g. by a sharp probe).

The accurate estimation of the probability of occurrence of systematic faults is difficult. This is primarily for the following reasons.

— The frequency of systematic faults is laborious to measure. Achieving a reasonable level of confidence in the result will not be possible without extensive data on systematic faults or parameters relevant to *risk control*.

— Consensus does not exist for a method to quantitatively estimate the probability of occurrence of systematic faults.

Because *risk estimation* is difficult in these circumstances, the *manufacturer* should not focus on estimating the *risk* of systematic faults but rather on implementing robust systems to prevent systematic faults which could lead to *hazardous situations* or *harm*.

5.4.6 *Hazardous situations* arising from security vulnerabilities

Security in this document includes cybersecurity and data and systems security. Security vulnerabilities can lead to loss of data, disclosure of personal health information, unauthorized access to patient *records*, etc. Such situations can initiate sequences of events, which can ultimately lead to *harm* (patient injury or damage to property). For example:

— loss of confidentiality can lead to the disclosure of personal health information;

— loss of integrity can lead to incorrectly represented lab results or malfunction of the *medical device*;

— loss of availability can prevent the use of critical functionality of a *medical device* or can stop the use of a *medical device* altogether.

See Annex F for further guidance on security.

5.4.7 Sequences or combinations of events

The *hazardous situation* can be the result of a sequence or combinations of independent events. This is illustrated in Figure 1. The probability P_1 of the *hazardous situation* occurring is then given by the product of the probabilities of occurrence of the independent events. A sequence of events can have branches leading to different *hazardous situations* and different events can lead to the same *hazardous situation*. These complexities are not shown in Figure 1.

The example in Figure 1 is for an electricity *hazard* and is related to an insulated wire inside a medical electrical device. There is a small probability that the insulation material is degraded and becomes damaged by cracks, and that the cracks lead to an exposed wire. The next possible events are that the user connects and turns on the *medical device*, and that (depending on choices in the user interface) the exposed wire now has line voltage. When the user subsequently opens the protective cover, the *hazardous situation* occurs, namely that the user is exposed to the line voltage of 220 V. The combined probability of this sequence of events is P_1.