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.

The probability that the user actually touches the exposed wire is estimated to be 0,10. Since the user will always experience a shock from the line voltage, the probability of discomfort is P_2 = 0,10. The probability of a burn is lower (0,01) and the probability of death is even lower (0,001).

A *hazardous situation* (HS1) can lead to different kinds of *harm* (H1 to H3), ranging from discomfort, to a burn to death. The probability that the *hazardous situation* leads to *harm* can have different values depending on the kind of *harm*, which values are described as $P_{2(HS1)H1}$ through $P_{2(HS1)H3}$ in Figure 1. The *severity* of *harm* can be affected by the circumstances of the exposure. For example, the consequences of an electric shock can vary from muscle contractions to burns, heart fibrillation or cardiac arrest, depending on voltage, current, duration of the exposure, and location on the human body.

It is emphasized that several scenarios can be relevant, not only those with the highest *severity* of *harm* or with the highest probability of occurrence of *harm*. Other scenarios can also be relevant. The *manufacturer* should consider what the best manner is to document the *hazardous situation*, describing one or more sequences of events that can lead to this *hazardous situation* and the different kinds of *harm* that can occur.

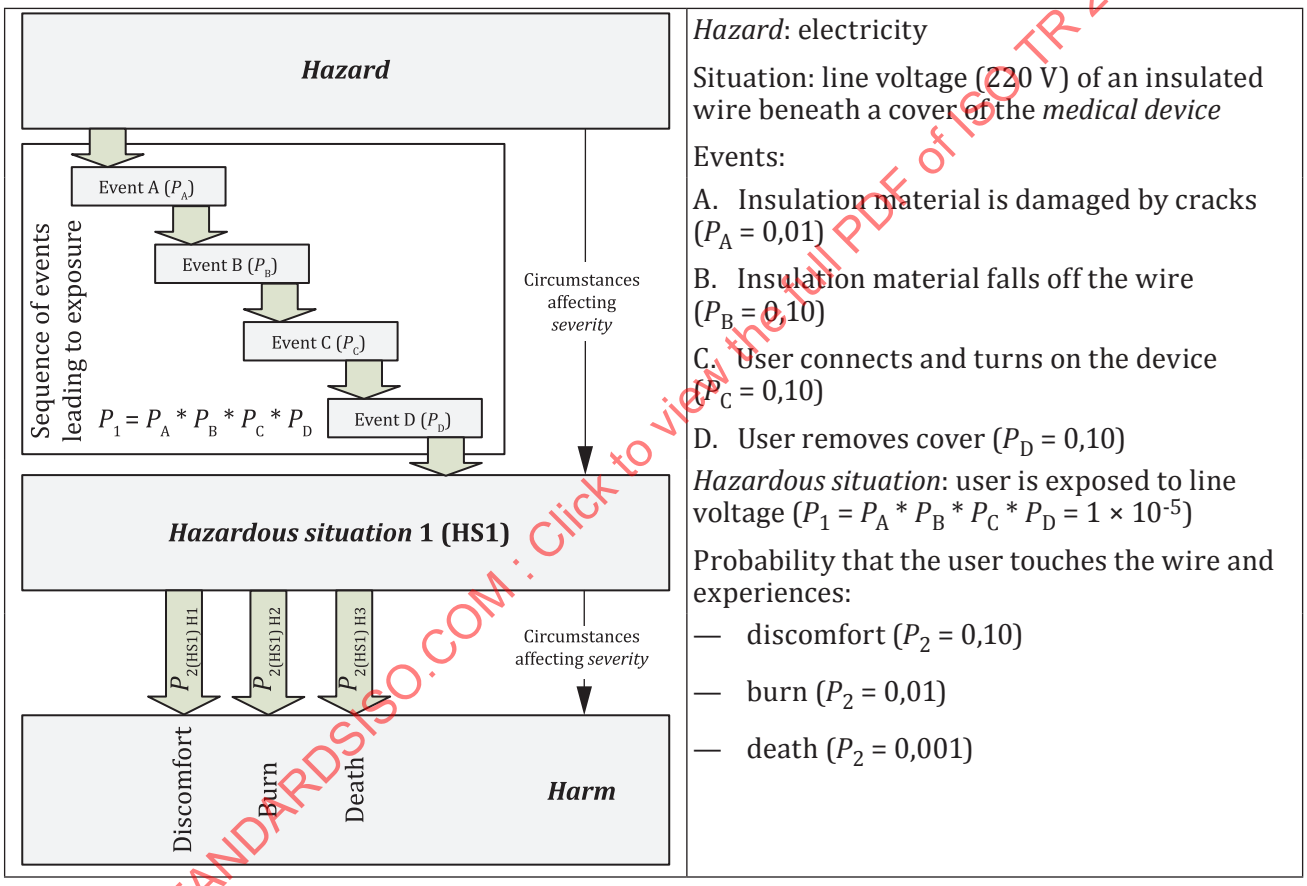


Figure 1 — Pictorial example of a relationship of *hazard*, sequence of events, *hazardous situation* and *harm*

Information about the *medical devices* on the market can be useful in estimating *risk*. Several approaches are commonly employed to estimate probabilities:

— use of historical design and development data;

— prediction of probabilities using analytical or simulation techniques;

— use of experimental data;

— reliability estimates;

— production and *post-production* information;

— use of expert judgment (an expert in this context can be a person competent on the basis of appropriate education, training, skills and experience; see ISO 13485[24]).

Each of these approaches has strengths and weaknesses. Complementary approaches should be used to increase confidence in the results. Expert judgment should be supplemented with one or more of the other approaches wherever possible. When the other approaches cannot be used or are not sufficient, it might be necessary to rely solely on expert judgment.

5.5 *Risk estimation*

5.5.1 General

ISO 14971:2019 requires the *manufacturer* to perform *risk estimation*. Various methods can be used to estimate *risk*. Those methods should examine, for example:

— the circumstances in which a *hazard* is present;

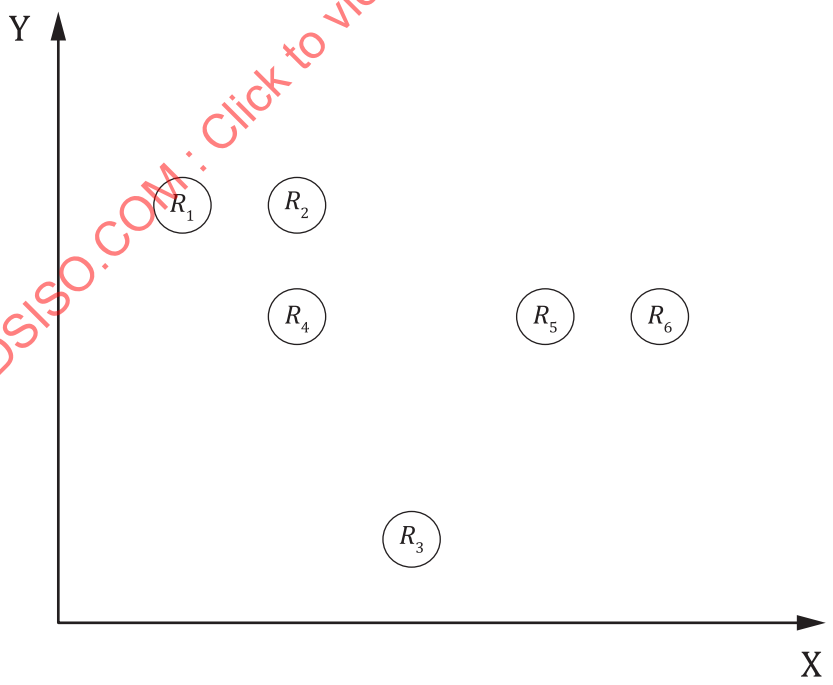
— the sequence of events leading to a *hazardous situation*;

— the probability of a *hazardous situation* occurring;

— the probability of a *hazardous situation* leading to *harm*;

— the nature of the *harm* that could result.

Risk should be expressed in terms that facilitate decision making on *risk* acceptability and the need for *risk control*, for example, using *severity* and probability scales. In order to analyse *risks*, their components, i.e. probability and *severity*, should be analysed separately.



Key

X probability of occurrence of *harm*

Y *severity* of *harm*

Figure 2 — Example of a *risk* chart that illustrates the distribution of estimated *risks*

A *risk* chart such as that shown in Figure 2 shows the distribution of the estimated *risks*, which can be useful for later decision making. The *risks* (R_1, R_2, R_3, ...) would be plotted on the chart as they are estimated. *Risk* matrices developed from this figure will be used in examples throughout this clause. This does not imply that this method has general applicability to all *medical devices*; however, it can be useful in many instances. If a *risk* chart or *risk* matrix is used for ranking *risks*, the particular *risk* chart or *risk* matrix and the interpretation used should be justified for that application.

5.5.2 Probability

When sufficient data are available to estimate the probability of occurrence of *harm* with adequate confidence, a quantitative method should be used. Otherwise, a qualitative method based on expert judgment is preferable to a quantitative estimate with high uncertainty. An example of this situation is a new *medical device* where suitable quantitative data are not available until design validation or later when *post-production* data become available. For a qualitative method, the *manufacturer* can describe a series of probability levels with descriptors appropriate for the *medical device*.

Although probability is a continuous variable, a number of discrete levels can be used in practice to simplify the analysis. The *manufacturer* decides how many probability levels are appropriate, based on the expected confidence in the estimates. A larger number of probability levels can be used when estimates are made with greater confidence. At least three levels should be identified to facilitate decision making. The levels can be descriptive and qualitative (e.g. not expected to occur during the lifetime of the *medical device*, likely to occur a few times, likely to occur frequently, etc.) or quantitative. *Manufacturers* should define the levels explicitly, so that there will be no confusion over what falls within each level. A particularly effective way is to assign ranges of non-overlapping numerical values to the discrete levels. An example of three qualitative probability levels is given in Table 3 and an example of five semi-quantitative probability levels in Table 5.

The definitions of the probability ranges can be the same or different for different product families. For example, a *manufacturer* can choose to use one set of probability ranges for X-ray equipment, but can have a different set of probability ranges for sterile disposable dressings. Scales for probability can include probability of occurrence of *harm* per use, per device, per hour of use, or within a population, etc.

It is required to document the chosen probability levels or ranges and their descriptors in the *risk management file* for the particular *medical device* (see ISO 14971:2019, 5.5).

There are several factors that are important for estimating the probability of occurrence of *harm*. These include, but are not limited to, the following.

— How often is a particular *medical device* used?

— What is the lifetime of the *medical device*?

— Who makes up the user and patient populations?

— What is the number of users/patients?

— How long and under what circumstances is the user/patient exposed?

Probability estimation encompasses the circumstances and the sequences of events from the occurrence of the initiating event through to the occurrence of the *harm*. The probability P of occurrence of *harm* can be decomposed into a probability P_1 that a *hazardous situation* occurs (i.e. that persons are exposed to the *hazard*) and a probability P_2 that the *hazardous situation* leads to *harm*. See Figure C.1 in ISO 14971:2019. A decomposition into P_1 and P_2 can be useful to estimate the probability P of occurrence of *harm*, but such decomposition is not mandatory.

When the probability of occurrence of *harm* is decomposed into P_1 and P_2, it could be the case that one of them can be estimated and the other not. In such cases, a conservative approach can be used by setting the unknown probability equal to 1. Such approach can be useful when the estimated probability is either so low that the resulting *risk* becomes clearly insignificant or negligible, or so high that it is clear the resulting *risk* should be reduced.

5.5.3 *Risks* for which probability cannot be estimated

Confidence in a *risk* estimate can be enhanced when a quantitative estimate of the probability of occurrence of *harm* is made on the basis of accurate and reliable data, or when a reasonable qualitative estimate is based on a consensus by qualified experts. However, this is not always achievable. For example, the probabilities of systematic faults, such as those discussed in 5.4.5, are difficult to estimate. When the accuracy of the probability estimate is in doubt, it is often necessary to establish a broad range for the probability or to determine that it is no worse than some particular value.

Examples where probabilities are difficult to estimate include:

— software failure;

— exceptional misuse situations, such as sabotage or tampering with a *medical device*;

— novel *hazards* that are poorly understood, e.g. imprecise knowledge of the infectivity of the causative agent of Bovine Spongiform Encephalopathy (BSE) prevents quantification of the *risk* of transmission;

— certain toxicological *hazards*, such as genotoxic carcinogens and sensitizing agents, where it might not be possible to determine a threshold of exposure below which toxic effects do not occur.

When the probability of occurrence of *harm* cannot be estimated, it is necessary to evaluate the *risk* on the basis of the *severity* of *harm* alone. The *risk control* measures should focus on preventing the *hazardous situation* entirely or on preventing that the *hazardous situation* leads to *harm*. If this is not possible, the *risk control* measures should focus on reducing the *severity* of the *harm*.

An inverse relationship can be presumed between the rigors of the *processes* used in design, development, manufacturing and maintenance and the probability of some systematic faults being introduced or remaining undetected. The required rigor of these *processes* can be determined by taking account of the *severity* of the consequences of systematic faults and the effectiveness of *risk control* measures external to the *medical device*. The more severe the consequences are and the less effective the external *risk control* measures, the more rigorous these *processes* should be.

5.5.4 *Severity*

To categorize the *severity* of the potential *harm*, the *manufacturer* should use descriptors appropriate for the *medical device*. *Severity* is, in reality, a continuum; however, in practice, the use of a discrete number of *severity* levels simplifies the analysis. In such cases, the *manufacturer* decides how many categories are appropriate and how they are to be defined. The levels should be descriptive and should not include any element of probability. See the examples in Table 2 and Table 4.

Severity levels are chosen and justified by the *manufacturer* based on the *harms* that could result for a particular *medical device*. The *severity* levels should be defined with sufficient specificity, so that the correct level of *severity* can be assigned to each *harm* identified in the *risk analysis*.

It is required to document the chosen *severity* levels or ranges and their descriptors in the *risk management file* for the particular *medical device* (see ISO 14971:2019, 5.5).

NOTE Terminology used by regulators can be useful in describing the levels of *severity* of *harm*.

5.5.5 Examples

Several approaches can be used for qualitative analysis. A typical approach is to use an N-by-M matrix to describe the *severities* and probabilities of occurrence of *harm* associated with each *hazardous situation*. One carefully defines N levels of probability and M levels of *severity*. Each cell of the matrix represents a subset of the full set of possible *risks*.

A simple example is a 3 × 3 *risk* matrix constructed by using the three *severity* levels of Table 2 as columns and the three qualitative probability levels of Table 3 as rows. The estimated *risks* (R_1, R_2, R_3,

...) are entered into the appropriate cells and the result is shown in Figure 3. *Manufacturers* should make these definitions as device-specific and explicit as needed to ensure their reproducible use.

Table 2 — Example of three qualitative *severity* levels

Common terms	Possible description
Significant	Death or loss of function or structure
Moderate	Reversible or minor injury
Negligible	No injury or slight injury

Table 3 — Example of three qualitative probability levels

Common terms	Possible description
High	Likely to happen, often, frequently, always Likely to happen several times during the lifetime of the *medical device*
Medium	Can happen, but not frequently Likely to occur a few times during the lifetime of the *medical device*
Low	Unlikely to happen, rare, remote Not likely to occur during the lifetime of the *medical device*

		Qualitative *severity* levels		
		Negligible	**Moderate**	**Significant**
Qualitative probability levels	**High**	R_1	R_2	
	Medium		R_4	R_5, R_6
	Low		R_3	

NOTE The estimated *risks* in Figure 3 are not the same as those depicted in Figure 2.

Figure 3 — Example of a qualitative 3 × 3 *risk* matrix

A more elaborate example is a 5 × 5 *risk* matrix constructed by using the five *severity* levels of Table 4 as columns and the five semi-quantitative probability levels of Table 5 as rows. The estimated *risks* (R_1, R_2, R_3, …) are entered into the appropriate cells and the result is shown in Figure 4.

Table 4 — Example of five qualitative *severity* levels

Common terms	Possible description
Catastrophic / Fatal	Results in death
Critical	Results in permanent impairment or irreversible injury
Serious / Major	Results in injury or impairment requiring medical or surgical intervention
Minor	Results in temporary injury or impairment not requiring medical or surgical intervention
Negligible	Results in inconvenience or temporary discomfort

Table 5 — Example of five semi-quantitative probability levels

Common terms	Examples of probability range
Frequent	$\geq 10^{-3}$
Probable	$<10^{-3}$ and $\geq 10^{-4}$
Occasional	$<10^{-4}$ and $\geq 10^{-5}$
Remote	$<10^{-5}$ and $\geq 10^{-6}$
Improbable	$<10^{-6}$

		Qualitative *severity* levels				
		Negligible	**Minor**	**Serious / Major**	**Critical**	**Catastrophic / Fatal**
Semi-quantitative probability levels	**Frequent**					
	Probable	R_1	R_2			
	Occasional		R_4		R_5	R_6
	Remote					
	Improbable			R_3		

Figure 4 — Example of a semi-quantitative 5 × 5 *risk* matrix

Other sizes than 3 × 3 or 5 × 5 matrices can be employed. However, matrices with more than five levels can require significantly more data to be able to distinguish between the various levels and to avoid overlap of the levels. Rationales for the selection of matrices and their outcome scores should be documented. Note that matrices with three levels might not always be sufficiently accurate for adequate decision making. While the above examples were 3 × 3 and 5 × 5, there is no need that these matrices be balanced. For example, a 4 × 5 matrix could be appropriate for a given application.

6 *Risk evaluation*

ISO 14971:2019 describes the *process* for *risk evaluation*. The standard, however, does not specify levels of acceptable *risk*. The criteria for *risk* acceptability are based on the *manufacturer's* policy for determining acceptable *risk* and are documented in the *risk management* plan.

During *risk evaluation* the *manufacturer* compares the estimated *risks* with the criteria for *risk* acceptability and determines if these criteria are met or not. See Annex C for further guidance and examples of applying the criteria for *risk* acceptability in *risk evaluation*.

7 *Risk control*

7.1 *Risk control* option analysis

7.1.1 *Risk control* for *medical device* design

Several options exist to reduce *risks* associated with a *medical device*. These can be used alone or in combination. The *manufacturer* can explore different options to reduce the *risks* to acceptable levels in a reasonably practicable way. The order of priority is important, as emphasised in ISO 14971:2019. This is explained below and clarified with some examples.

a) Making the *medical device* design and the manufacturing *process* inherently safe by:

— eliminating a particular *hazard*;

EXAMPLE 1 Eliminating the *hazard* of sharp edges that can cause injury by designing the surfaces with rounded edges. Eliminating the *hazard* of electric shock by using a manually operated pump instead of an electrical pump.

— reducing the probability of occurrence of the *harm*;

EXAMPLE 2 Reducing the probability of fibrillation *harm* due to an electric shock by having no accessible live parts. Reducing the probability of unauthorised access to data by identity management. Reducing the probability of biological reactions due to microbial contamination by using cleanroom technologies or sterilization.

— reducing the *severity* of the *harm*.

EXAMPLE 3 Reducing the *severity* of *harm* from being squeezed by a moving part by using a low-power motor and low speed. Reducing the *severity* of *harm* from an electric shock by using low electric voltage (below 42 V).

b) Taking protective measures by:

— preventing the occurrence of a *hazardous situation*;

EXAMPLE 4 Using automatic cut-off or over-pressure valves. Protective covers of electrical wires and power units (covered plugs, sockets and connectors). Guards for moving parts or to prevent patients falling off a table or out of bed. Inspection testing in manufacturing to detect non-conforming products.

— preventing a *hazardous situation* from leading to *harm*.

EXAMPLE 5 Using visual or acoustic alarms to alert the user to a *hazardous situation*.

c) Providing information for *safety* by:

— placing warnings on the *medical device*;

EXAMPLE 6 Warning: Do not use after [expiry date].

— including contra-indications in the *accompanying documentation*;

EXAMPLE 7 Do not use with neonates.

— providing instructions to support correct use and to avoid *use error*;

EXAMPLE 8 Apply epinephrine injector to the middle of your outer thigh (upper leg), through clothing if necessary. Do not inject into your veins, buttocks, fingers, toes, hands or feet. Hold the leg of young children firmly in place before and during injection to prevent injuries.

— providing instructions to use personal protective equipment;

EXAMPLE 9 Use gloves and eyeglasses when handling toxic or hazardous materials.

— providing instructions about measures to reduce the *severity* of *harm*;

EXAMPLE 10 Rinse immediately with water after contamination with hazardous substances.

— providing training to users on how to use the *medical device* correctly;

EXAMPLE 11 Training program for operators of radiotherapy equipment or for home-use dialysis machines.

— providing instructions relating to installation and maintenance during the lifetime of the *medical device*.

EXAMPLE 12 Maintenance intervals, maximum expected lifetime, how to dispose of the *medical device* properly.

Options a) to c) are listed in descending order of priority with regard to their generally recognised effectiveness in reducing *risk*. The *manufacturer* should take this order into account before deciding on the most appropriate (combination of) *risk control* measures.

Examples of specific *risk control* measures for different types of *medical devices* are given in Table 6. Further guidance on providing information for *safety* is given in Annex D.

Table 6 — Examples of *risk control* measures

Medical device	***Hazard***	***Hazardous situation***	**Inherently safe design**	**Protective measure**	**Information for *safety***
Syringe (for single use)	Biological contamination	Reuse after previous use on another patient	Self-destruction after use	Clear indication of first use	Warning against reuse
Implantable pacemaker	Loss of functionality	Pacemaker stops functioning due to early battery depletion	Reliable long-life batteries	Alarm before battery depletion	Information on typical battery lifetime
Mechanical patient ventilator	Air pressure	Software failure causes excessive pressure in patient airway	Blower incapable of delivering high pressure	Over-pressure valve in ventilator or in breathing hose	Instruction to use only breathing hose delivered by *manufacturer*
IVD blood analyser	Systematic error or bias	Incorrect result reported to clinician	Self-calibration	Metrologically traceable calibrators provided	Instruction to verify calibration with trueness controls
X-ray equipment	Ionising radiation	Staff exposed to stray radiation	Not feasible (stray radiation always occurs)	Lead shields and lead aprons	Information on radiation level in occupancy zones

In this step possible solutions for inherently safe design and protective measures can be investigated for their strengths and weaknesses. The choice of design solutions should be based on these investigations. Much knowledge of the possible design solutions and related *risks* can be created in this *process*. The *manufacturer* should consider how to retain this knowledge for future use.

7.1.2 *Risk control* for manufacturing *processes*

Deviations or errors in manufacturing *processes* can compromise the *safety* of *medical devices*, for example, by:

— introducing hazardous residues or particulates;

— affecting critical physical or chemical properties such as surface coating, tensile strength, resistance to ageing, homogeneity, etc.;

— exceeding critical tolerances;

— insufficient *process* control, leading to mix up of gas lines during the assembly of a respirator; or

— impairing the integrity of welding, gluing, or bonding of components.

Inherently safe manufacture eliminates the particular *hazard* from the manufacturing *process* and ensures that the *hazard* is not present in the *medical device*. Protective measures in the manufacturing *process*, such as inspection and/or testing, can detect non-conformities and can prevent the distribution of affected *medical devices*.

Techniques such as Failure Mode and Effects Analysis (FMEA, see Annex B.5) and Hazard Analysis and Critical Control Points (HACCP, see Annex B.7) can be useful for analysing critical steps in the manufacturing and distribution *processes*. It is important to also consider the need for *risk control* in:

— outsourced *processes*, such as purchased products, components and services; and

— other phases of the *medical device life cycle*, such as storage, distribution, installation, servicing, decommissioning and disposal.

7.1.3 Standards and *risk control*

Generally, international standards can be considered to represent the generally acknowledged *state of the art*. By applying a standard, the *manufacturer* can simplify the task of analysing *residual risks*, but it is emphasised that the standard might not address all *risks* associated with a *medical device*.

Many standards address inherent *safety*, protective measures, and information for *safety* for *medical devices*. When relevant standards exist, they can address some or all *risks* associated with a particular *medical device*. The *manufacturer* can presume that, in the absence of *objective evidence* to the contrary, meeting the requirements of the relevant standards results in particular *risks* being reduced to an acceptable level. See Annex E for further guidance on the use of international standards.

7.2 Implementation of *risk control* measures

ISO 14971:2019 requires implementation of *risk control* measures, *verification* of implementation and *verification* of the effectiveness of those *risk control* measures. The *risk management* plan specifies how the two distinct *verification* activities will be carried out.

Verification of implementation of *risk control* measures in the *medical device* can be obtained from design documentation. *Verification* of the effectiveness of the *risk control* measures in the *medical device* can require testing of individual *risk control* measures or testing the *medical device*. The *verification* requirements apply to all *risk control* measures, including information for *safety*. Testing with users can provide useful information supporting the *verification* of effectiveness, for example usability testing (see IEC 62366-1[16]), clinical investigation (see ISO 14155[26]) or clinical performance studies of *in vitro diagnostic medical devices* (see ISO 20916[37]). More guidance on the use of international standards in *risk management* is provided in Annex E.

Verification of implementation of *risk control* measures in the manufacturing *process* can be done by checking the *process* specifications. *Verification* of the effectiveness of *risk control* measures in the manufacturing *process* can be done by qualification of the manufacturing *process*, such as *process* validation, inspection method qualification or other appropriate means.

The *risk management* plan can detail the *verification* activities explicitly or by reference to the plan for other *verification* activities.

7.3 *Residual risk* evaluation

Residual risks are evaluated by the same method and with the same criteria for *risk* acceptability as the initial *risks*. The *residual risk* is either acceptable or unacceptable. When unacceptable, further *risk control* options should be investigated. If further *risk control* is not practicable, a *benefit-risk* analysis may be performed. *Residual risk* evaluation can be repeated through the *life cycle* of the *medical device*, when production and *post-production* information indicate that either the *risk* or its acceptability could have changed.

7.4 *Benefit-risk* analysis

7.4.1 General

ISO 14971:2019 allows the *manufacturer* to perform a *benefit-risk* analysis for those *risks* that are not judged acceptable using the criteria established in the *risk management* plan and for which further *risk*

control is not practicable. The *benefit-risk* analysis is used to determine if the *residual risk* is outweighed by the expected *benefits* of the *intended use* of the *medical device*.

Benefit-risk analyses cannot be used to weigh *residual risks* against business advantages or economic advantages (i.e. for business decision making). See also ISO 14971:2019, A.2.7.4.

The practicability of further *risk* reduction should be taken into account before considering the *benefits* (see Annex C). The decision as to whether *risks* are outweighed by *benefits* is essentially a matter of judgment by experienced and knowledgeable individuals, usually a multidisciplinary team comprising medical, clinical or application experts. An important consideration is whether an anticipated *benefit* can be achieved through the use of alternative solutions without that *risk* or with smaller *risk*. This involves comparing the *residual risk* for the *manufacturer's medical device* with the *residual risk* for similar *medical devices*.

7.4.2 *Benefit* estimation

The *benefit* arising from a *medical device* is related to the likelihood and extent of improvement of health expected from its use. *Benefits* can be described in terms of positive impact on clinical outcome, the patient's quality of life, outcomes related to diagnosis, positive impact from diagnostic devices on clinical outcomes, or a positive impact on public health. The nature and degree of *benefits* can depend on the patient population.

Sometimes *benefits* can be described in terms of magnitude of the positive effects, for example the proportion of patients that will experience the *benefit* and the duration of *benefit*.

Benefit can be estimated from knowledge of several factors such as:

— the performance expected during clinical use;

— the clinical outcome expected from that performance;

— *benefits* resulting from the use of similar *medical devices*;

— factors relevant to the *risks* and *benefits* of other diagnosis or treatment options.

Confidence in the *benefit* estimate is strongly dependent on the reliability of the information addressing these factors. This includes recognition that there is likely to be a range of possible outcomes. For example:

— It can be difficult to compare different outcomes, e.g. which is worse, pain or loss of mobility? Different outcomes can result from the side-effects being very different from the initial problem.

— It is difficult to take account of non-stable outcomes. These can arise both from the recovery time and long-term effects.

Due to the difficulties in applying a rigorous approach, it is generally necessary to make simplifying assumptions. Therefore, it will usually prove expedient to focus on the most likely outcomes for each option and those that are the most favourable or unfavourable.

The following aspects should be taken into account:

— the type of expected *benefits* for the patient or other people (e.g. the *medical device* is life-saving or essential in a given medical scenario);

— the magnitude of the expected *benefits* (e.g. the degree to which the patient will experience the therapeutic or diagnostic *benefit*);

— the probability that the patient will experience the expected *benefits* (i.e. the likelihood that the *medical device* is effective in treating or diagnosing the patient's disease or condition); and

— the duration of the expected effects (i.e. how long the *benefit* is expected to last for the patient).

An estimate of *benefit* can vary markedly across different phases of the design *process*. If reliable clinical data demonstrating the consistent performance and effectiveness of the *medical device* are available, the *benefit* can be estimated confidently. In cases where clinical data are limited in quantity or quality, *benefit* is estimated with greater uncertainty from whatever relevant information is available. For example, it is sometimes necessary early in the *process* to estimate the *benefit* from the expected degree of health improvement and the likelihood of achieving the intended performance.

Where significant *risks* are present and the *benefit* estimate has a high degree of uncertainty, it will be necessary to verify the anticipated performance or effectiveness through a simulation study or a clinical investigation. This is essential to confirm that the *benefit-risk* balance is as expected and to prevent unwarranted exposure of patients to a large *residual risk*. ISO 14155[26] specifies *procedures* for clinical investigations of *medical devices* and ISO 20916[37] for clinical performance studies of *in vitro diagnostic medical devices*.

7.4.3 Criteria for *benefit-risk* analysis

Those involved in making *benefit-risk* judgments have a responsibility to understand and take into account the technical, regulatory, economic and sociological context of their *risk management* decisions. This can involve an interpretation of fundamental requirements set out in applicable regulations or standards, as they apply to the *medical device* under consideration under the anticipated conditions of use. Since this type of analysis is highly product-specific, further guidance of a general nature is not possible. Instead, the *safety* requirements specified by standards addressing specific products or *risks* can be presumed to be consistent with an acceptable level of *risk*, especially where the use of those standards is sanctioned by the prevailing regulatory system. Note that a clinical investigation might be required to verify that the balance between *benefit* and *residual risk* is acceptable.

7.4.4 *Benefit-risk* comparison

A direct comparison of *benefit* and *risk* is complicated and should take the following into account:

— characterization of the disease or condition of the intended patients;

— the uncertainty of data. Initially a literature search for the *hazards* and the *medical device* being considered can provide insight into the balance between *benefit* and *risk*;

— production and *post-production* information for similar *medical devices* that are already available on the market;

— the generally acknowledged *state of the art*;

— a comparison of the *benefits* of the *medical device* under development with the *benefits* of similar *medical devices* available on the market;

— a comparison of the *residual risks* of the *medical device* under development with the *residual risks* of similar *medical devices* available on the market.

ISO 14971:2019 requires the *manufacturer* to record the results of a *benefit-risk* analysis in the *risk management file*. It is recommended to include the rationale how the conclusion was reached.

7.4.5 Examples of *benefit-risk* analyses

The following examples illustrate the conclusions of *benefit-risk* analyses.

EXAMPLE 1 Burns can occur where the return electrode of a high-frequency surgery device is improperly attached to the patient. Although conformance to the relevant product standard minimizes the probability of such burns, they can still occur. Nevertheless, the *benefit* of using a high-frequency surgery device outweighs the *residual risk* of burns.

EXAMPLE 2 Although X-rays are known to be potentially harmful, the clinical effectiveness of conventional diagnostic imaging almost always justifies its use. However, the unwanted effects of radiation on the patient are not ignored. Standards exist to minimize radiation exposure to patients. When a new application of ionizing radiation is developed and existing standards are not applicable, the *manufacturer* verifies that the results of the *benefit-risk* analysis are at least as favourable as that of alternative *medical devices* and treatments.

EXAMPLE 3 Once implanted, some cochlear implant components, such as the implant receiver stimulator with electrode array, cannot easily be replaced. They are intended to remain implanted for life and are required to perform reliably for years and even decades. (This is an especially important consideration in the case of a young adult or child.) Accelerated reliability testing of these components can be conducted for specific failure mechanisms. However, validating the reliability of components that are to last for decades is not practical. Therefore, the *residual risk* of *medical device* failure is weighed against the *benefit* of potential hearing improvement. The *residual risk* depends on the estimated reliability of the components and the confidence in the reliability estimates for those components that cannot be validated. In some cases, the *residual risk* outweighs the *benefit*; in other cases the *benefit* outweighs the *risk*.

7.5 *Risks* arising from *risk control* measures

Implementing a *risk control* measure to reduce one *risk* can introduce new *risks* or increase other *risks*, including those previously evaluated to be acceptable. For example, elimination of a use-related *risk* in the user interface can restrict the user's flexibility in using the *medical device* and restrict his ability to intervene in *hazardous situations*. A second example is a software change to control one particular *risk*, which unintentionally undermines another *risk control* measure embedded in the software architecture. The *manufacturer* reviews these effects to ensure that those *risks* are still acceptable.

One way to perform this review is to update the *risk analysis* of the *medical device*, including all *risk control* measures, and to identify if new *risks* are introduced or existing *risks* are increased. For *risk control* measures in the manufacturing *process*, the *manufacturer* can perform the review as part of *process risk analysis* or *process* validation.

7.6 Completeness of *risk control*

ISO 14971:2019 requires that the *risks* from all identified *hazardous situations* are considered and that all *risk control* activities are completed. This can be achieved by maintaining a list of all *hazards* and *hazardous situations* and the associated *risks*. The list can be checked to ensure that the *risks* from all identified *hazardous situations* have been considered and that no *risks* are overlooked. The results of this activity are documented in the *risk management file*.

8 Evaluation of overall *residual risk*

8.1 General considerations

ISO 14971:2019 requires that the overall *residual risk* be evaluated in relation to the *benefits* of the *intended use* of the *medical device*, and that both the criteria for acceptability of the overall *residual risk* and the method of evaluation of overall *residual risk* be included in the *risk management* plan.

The evaluation of overall *residual risk* is the point where *residual risk* is viewed from a broad perspective. All identified *hazardous situations* have been evaluated and all *risks* have been reduced to an acceptable level or have been accepted based upon a *benefit-risk* analysis. Now, the *manufacturer* considers if the overall *residual risk* associated with the *medical device* as a whole satisfies the criteria for acceptability of overall *residual risk*. This consideration takes into account the contributions of all *residual risks* together in relation to the *benefits* of the *intended use* of the *medical device*. This step is particularly important for complex *medical devices* and for *medical devices* with a large number of individual *risks*. The evaluation can lead to the conclusion that the *medical device* is safe.

The evaluation of overall *residual risk* is a challenging task that cannot be achieved by adding all individual *risks* numerically. The difficulty arises for the following reasons:

— Each probability of occurrence of *harm* is related to a different *harm* with different *severity* and can be related to different *hazardous situations*.

— Probabilities are often known with different degree of uncertainty. Some probabilities could be known precisely from either historical data or testing. Other probabilities might be known imprecisely such as estimates by expert judgment, or cannot be estimated such as the probability of a software failure.

— It is not possible to combine the *severities* of individual *harms* within the broad categories usually employed in *risk analysis*.

Furthermore, the criteria for acceptability of the overall *residual risk* can be different from the criteria for acceptability of individual *risks*. The criteria used to evaluate individual *risks* usually include limits for the probability of occurrence of *harm* with a particular *severity*. The criteria used to evaluate the overall *residual risk* are often based on additional elements, such as the *benefits* of the *intended use* of the *medical device*.

There is no preferred way for evaluating the overall *residual risk*. The *manufacturer* is responsible for determining an appropriate method. In the following subclauses some examples of approaches are presented that can be used in defining the evaluation method. This guidance is intended to assist *manufacturers* in establishing methods and criteria.

ISO 14971:2019 requires that the overall *residual risk* be evaluated by persons with the knowledge, experience and authority to perform such tasks. It is recommended to involve application specialists with knowledge of and experience with the *medical device*. Ultimately, the evaluation should be based on expert judgment with essential roles for application knowledge and clinical expertise.

The results of the evaluation of overall *residual risk* form part of the *risk management file*. It is recommended to document the rationale for the acceptance of the overall *residual risk*.

ISO 14971:2019 requires the *manufacturer* to inform users of significant *residual risks* and to provide the necessary information in the *accompanying documentation* to disclose those *residual risks*. See Annex D for guidance on the disclosure of *residual risk*.

8.2 Inputs and other considerations

The evaluation of overall *residual risk* can take several inputs and considerations into account. Some examples of inputs and their use are presented below.

a) Different sequences of events can lead to different *hazardous situations* and *risks*, each contributing to the overall *residual risk*. For example, the reuse of a single-use device can be associated with infection, leaching of toxic substances, mechanical failure due to ageing and bio-incompatible disinfectant residues. Event Tree Analysis (ETA, see Annex B.4) can be a suitable method for analysing these *risks*, to differentiate between sequences of events with considerable versus negligible probability of occurrence or *severity* of *harm*. The combined contribution of these *risks* is considered in the evaluation of the overall *residual risk*.

b) A particular *harm* can originate from different *hazardous situations*. In such cases, the probability of occurrence of the *harm* can be used to determine the overall *residual risk* based on a combination of the individual probabilities. Fault Tree Analysis (FTA, see Annex B.3) can be a suitable method for estimating the combined probability of occurrence of a particular *harm*.

c) *Risk control* measures that are appropriate for independent individual *risks* could result in conflicting requirements, which can increase the overall *residual risk*. For example, an instruction to address the *risk* of an unconscious patient falling off a patient table could be “never leave an unconscious patient unattended”. This could conflict with the instruction “stand behind protective screen when making X-ray images” intended to protect medical staff from being exposed to X-rays.

d) A warning considered on its own could provide adequate reduction of an individual *risk*. However, too many warnings can confuse the user of the *medical device* and can thus reduce the effect of the individual warnings. An analysis might be needed to determine if there is an over-reliance on warnings and whether such over-reliance could have an impact on the *risk* reduction and the overall *residual risk*.

e) A comprehensive review of all operating instructions for the *medical device* might reveal that the instructions are inconsistent or too difficult to follow. This can also have an impact on the overall *residual risk*.

f) The results of the design validation, usability studies, clinical evaluations and clinical investigations can provide useful information about the overall *residual risk*. Appropriate input from stakeholders can provide useful information.

g) All *benefit-risk* analyses for individual *risks* should be taken into account.

h) When there have been trade-offs between *risks* in the *risk analysis*, the impact on the overall *residual risk* should be analysed with extra care. These are instances where one *risk* might have been allowed to increase somewhat in order that another *risk* could be reduced. For example, the *risk* to one person (the user) is allowed to increase so that the *risk* to another (the patient) can be reduced. The evaluation can take the form of going through related major *risks*, describing why the trade-off balance is justified, and why the combined level of the *risks* in the trade-off decision is acceptable.

8.3 Possible approaches

The method to evaluate the overall *residual risk* can include the following approaches or other approaches deemed appropriate by the *manufacturer*.

a) The *benefits* related to the *intended use* of the *medical device* are weighed against the overall *residual risk*. *Benefits* can be described by their magnitude or extent, the probability of experiencing the *benefit* within the intended patient population, and the duration and frequency of the *benefit*. The evaluation should take into account knowledge of the intended medical indication, the generally acknowledged *state of the art* in technology and medicine, and the availability of alternative *medical devices* or treatments.

b) Visual representations of the *residual risks* can be useful. Each individual *residual risk* can be shown in a *risk* chart or *risk* matrix, such as those in Figure 3 and Figure 4, giving a graphic view of the distribution of the *risks*. If many of the *risks* are in the higher *severity* regions or in the higher probability regions of the *risk* matrix, or clusters of *risks* are borderline, then the distribution of the *risks* can indicate that the overall *residual risk* might not be acceptable, even if each individual *risk* has been judged acceptable.

c) The *manufacturer* can compare the *medical device* under consideration to similar *medical devices* available on the market. The key question is whether the *medical device* under consideration has an acceptable overall *residual risk* in relation to the medical *benefits*, in comparison to similar *medical devices*. *Residual risks* posed by the *medical device* can be compared individually to corresponding *risks* for the similar *medical device*, taking account of differences in *intended use*. Up-to-date information on *intended use* and adverse events of similar *medical devices* should be carefully reviewed, as well as information from scientific literature, including information about clinical experience.

d) The *manufacturer* can use experts to support the evaluation of the overall *residual risk* in relation to the *benefits* expected from using the *medical device* under consideration. These experts can come from a variety of disciplines and should include those with clinical or application experience and those with knowledge of similar *medical devices*. The experts should have an appropriate level of independence from those who designed and developed the *medical device*. They can assist the *manufacturer* in taking into account stakeholder concerns. Attention is drawn to the requirements in ISO 14971:2019 for training and experience.

e) Even though all individual *risks* should have been identified, controlled and judged acceptable at this point, it could be appropriate that some *risks* are investigated further as a result of the overall *residual risk* evaluation. For example, there could be many *risks* close to being not acceptable. Hence, the overall *residual risk* could not be deemed acceptable and a further investigation would be appropriate.

f) Further investigation can also be appropriate when some *risks* are interdependent with respect to either their causes or the *risk control* measures applied. *Risk control* measures should be verified for effectiveness, not only individually but also in combination with other *risk control* measures. This can also apply to *risk control* measures designed to control multiple *risks* simultaneously. Fault Tree Analysis (FTA) or Event Tree Analysis (ETA) can be useful tools to discover such relationships between *risks* and *risk control* measures.

9 *Risk management* review

ISO 14971:2019 requires that the final results of the *risk management process* be reviewed to ensure that the *risk management* plan has been appropriately executed, that the overall *residual risk* is acceptable, and that appropriate methods are in place to collect and review relevant production and *post-production* information. The *risk management* review is performed after implementation and *verification* of all *risk control* measures but prior to commercial release of the *medical device*. The *risk management* report provides the summary of this review and is included in the *risk management file*.

There can be a need to revise or update the *risk management* report if new information becomes available, for example during the production and *post-production* phases. The *manufacturer* determines when subsequent reviews of the execution of the *risk management* plan and updates of the *risk management* report are performed, for example, after a major change in the design of the *medical device*.

The review of the execution of the *risk management* plan is not to be confused with the review of the suitability of the *risk management process* at planned intervals by *top management* (see 4.2.3). The *risk management* plan is related to the *life cycle* of one type of *medical device* (or *medical device* family). The review of the suitability of the *risk management process* is related to the effectiveness of the *process* and how this *process* is implemented.

10 Production and *post-production* activities

10.1 General

Monitoring of production and *post-production* information is the critical step that enables *medical device manufacturers* to close the feedback loop and to make *risk management* a continuous *life cycle process*. During this phase, information is collected from many different sources, reviewed for relevance to *safety*, and where appropriate, fed back into earlier phases of the *risk management process* to maintain the *safety* of the *medical device*.

ISO 14971:2019 requires the *manufacturer* to establish a system to actively collect and review information about the *medical device* that could be related to *safety*. The activities necessary to establish this system are recorded in the *risk management* plan (see 4.4.8).

The production and *post-production* activities can be part of a post-market surveillance system. See ISO/TR 20416[35] for more guidance on post-market surveillance.

NOTE This phase is aligned with the relevant parts of Clauses 7 and 8 of ISO 13485:2016[24]. More guidance is provided in the ISO Handbook: *ISO 13485:2016 – Medical devices – A practical guide*[25].

10.2 Information collection

Information relevant to the *safety* of the *medical device* can come from a variety of sources. The more experience a *manufacturer* has in developing and marketing similar *medical devices*, the more likely the

manufacturer will have a good understanding of the *medical device* performance, the patient population, the *reasonably foreseeable misuse* that could occur, and the *risks* associated with the *medical device*.

Production and *post-production* activities can include receiving information about the *medical device safety* and performance. Sources typically include general feedback from users, distributors, service personnel and training personnel. The information can be related to *harm* that has occurred or to *hazardous situations* that occurred without *harm*. The activities can also include soliciting information about the *medical device* performance and related *risks*. These activities involve reaching out to stakeholders to obtain specific information and insight, using methods such as customer surveys, expert user groups (focus groups) and *manufacturer*-sponsored *medical device* tracking/implant registries. It also includes publicly available information such as clinical literature, incident reports and adverse event databases.

The activities can further include post-market clinical follow-up (PMCF) studies carried out following market approval, which are intended to enhance the clinical evidence for the *safety* and performance of a *medical device* after it is placed on the market. PMCF studies typically address specific questions related to the *safety* or performance (i.e. the *residual risks*) when a *medical device* is used in accordance with its *intended use*. See ISO 14155[26] for requirements on clinical investigations and GHTF/SG5/N4:2010[3] for further guidance on PMCF studies.

The information collected does not necessarily have to be directly related to the *manufacturer's medical device*. Other *medical devices* with similar *intended use*, similar principle of operation or similar *hazards* can yield useful information about the *risks* associated with the *manufacturer's medical device*. This also applies to other products without a medical purpose but with similar use or similar operating principle.

Table 7 presents a list of data sources containing production and *post-production* information that should be considered for analysis and possible relevance to *safety*. This table is based on GHTF/SG3/N18:2010[2].

If the collection and review of information is performed by different departments, effective communication and coordination between those departments is essential.

Table 7 — Data sources related to production and *post-production* information

Data sources	Information
Production	— Data from monitoring supplier performance/controls — *Process* monitoring — In-*process* inspection/testing — Internal/external audits
Complaint handling	— Quantity — By *medical device* family — By customer (physician, healthcare facility, patient, etc.) — Reason for complaint — Complaint codes — *Severity* of any *harm* — Component involved

Table 7 *(continued)*

Data sources	Information
Service reports	— Installation — First use of *medical device* — Frequency of maintenance visits — Types of repairs — Frequency of repairs — Usage frequency — Parts replaced — Service personnel
Risk management	— Published adverse event reports for similar *medical devices* — Stakeholder concerns and generally acknowledged *state of the art*
Clinical activities	— Post-Market Clinical Follow-up (PMCF) studies
Market/patient surveys	— Service response time — Solicited information on new or modified *medical devices*
Scientific literature	— Research publications
Media sources	— Online newsletters — Medical information websites — Articles in trade journals, scientific journals and other literature
Security data sources	— Independent security researchers — In-house testing — Suppliers of software or hardware technology — Health care facilities — Published events for devices sharing similar technologies as the *medical device* — Information Sharing and Analysis Center (ISAC)

10.3 Information review

The collected information is reviewed to determine if the information is relevant to *safety*. The following questions can help in this review:

— Is the *intended use* still valid?

— Are the anticipated *benefits* achieved?

— Is there evidence of *hazards* or *hazardous situations* not previously identified? For example, did any unforeseen *harm* occur?

— Are there occurrences of misuse which were previously not foreseen?

— Is there an increasing trend of use for applications other than the *intended use*?

— Does the frequency of occurrence of a particular *hazardous situation* or *harm* suggest that the probability of occurrence of *harm* was underestimated?

— Does the reported *harm* indicate that the *severity* of *harm* was underestimated?

— Is there evidence that the *risk control* measures are not effective?

— Does the evaluation of the overall *residual risk* accurately represent the actual market experience?

— Are there changes in the generally acknowledged *state of the art*?

— Are there indications that the criteria for *risk* acceptability should be adjusted?

The information review can lead to several possible outcomes, for example:

— The *hazard* and *hazardous situation* were correctly identified. The *risk* was adequately assessed and remains acceptable.

— The *hazard* and *hazardous situation* were correctly identified, but the *risk* has increased and is no longer acceptable. Further action is required.

— The *hazard* or *hazardous situation* was not identified. Further action is required.

— The generally acknowledged *state of the art* or the *benefits* for the *medical device* have changed. Further action is required.

Concerning changes in the generally acknowledged *state of the art*, consideration should also be given to the availability of alternatives to treat or diagnose the medical condition of the intended patients, including the *safety* and effectiveness and the associated *risks* of those alternatives. The *risks* and *benefits* to patients in situations where no treatment or diagnosis is available should also be considered.

The *manufacturer* should also assess whether the anticipated *benefits* of the *intended use* are achieved or have changed. If the *benefits* change while the *risks* remain the same, the balance between *benefit* and overall *residual risk* can also change. See 7.4.2 for a discussion of *benefit* estimation.

Statistical techniques should be considered to assist in the processing of data, such as trend analysis, predictive reliability engineering techniques (e.g. Weibull analysis), and reliability evaluation (e.g. testing *medical devices* or components to failure, testing failed components returned to the *manufacturer*, or testing *medical devices* from the same lot or previous/succeeding lots). See ISO/DIS 10017[21][1)] for further guidance on the selection and use of statistical techniques.

10.4 Actions

If the collected information is reviewed and determined to be relevant to *safety*, several actions are required by ISO 14971:2019. Some of these actions are related to the particular *medical device*, while other actions are related to the *risk management process*.

If a *hazard* or *hazardous situation* is present that was not previously recognised, the associated *risks* are assessed and controlled where appropriate, following the steps of ISO 14971:2019 Clauses 5 to 7. The results of the *risk assessment* and the implemented *risk control* measures are recorded in the *risk management file*.

If a *risk* has become no longer acceptable, an update of the assessment of the specific *risk* is necessary. The impact of the collected information on previously implemented *risk control* measures is evaluated to see if these measures are still effective and sufficient to reduce the *risk*. The results of this evaluation should be considered as an input for modification of the *medical device*. If appropriate, the steps of ISO 14971:2019 Clauses 5 to 7 are repeated and new/additional *risk control* measures are implemented. The updated *risk assessment* and the implemented *risk control* measures are recorded in the *risk management file*.

It could be necessary to evaluate the overall *residual risk* again in relation to the *benefits* of the *intended use* of the *medical device*. It could also be necessary to repeat the *risk management* review and to prepare a new *risk management* report. See Clauses 8 and 9 of ISO 14971:2019.

1) Under preparation. Stage at the time of publication: ISO/DIS 10017:2020.

The *manufacturer* should also consider if actions are needed to address those *medical devices* that are:

— already distributed (i.e. beyond the control of the *manufacturer*), because correction of these *medical devices* or removal from the market could be necessary;

— already manufactured but not distributed (i.e. still under the control of the *manufacturer*), because containment and correction of these *medical devices* could be necessary; or

— to be manufactured in the future, because modification of the *medical device* design and related manufacturing or servicing *processes* could be necessary.

For *medical devices* on the market, the *manufacturer* should consider whether any urgent information should be communicated to users, patients and other stakeholders as an interim measure (for example as an advisory notice as described in 8.3 of ISO 13485:2016[24]), before further *risk control* measures are developed. The degree of urgency in this communication should be commensurate with the degree of *risk*, because the speed of these actions contributes to their effectiveness. The time period can be subject to regulatory requirements. The decisions and actions taken are recorded in the *risk management file*.

The results of the information review can indicate that the *risk management process* is insufficient or inadequate. Therefore, ISO 14971:2019 requires the *manufacturer* to evaluate the impact of the collected information on the previously implemented *risk management* activities, to see which activities should be improved. The results of this evaluation are communicated to *top management*, who will take these results as input into the planned reviews of the suitability of the *risk management process* (see 4.2.3). *Top management* then decides which parts or aspects of the *risk management process* require improvement to ensure its continuing effectiveness.

Annex A
(informative)

Identification of *hazards* and characteristics related to *safety*

A.1 General

ISO 14971:2019 requires that the *manufacturer* identify those characteristics of the *medical device* that could affect *safety*. Consideration of these characteristics is an essential step in identifying the *hazards* associated with the *medical device*. One way of doing this is to ask a series of questions concerning the manufacture, intended users, *intended use*, *reasonably foreseeable misuse*, and ultimate disposal of the *medical device*. If one asks these questions from the point of view of all the individuals involved (e.g. users, maintenance staff, patients, etc.), a more complete picture can emerge of the *hazards* that might exist.

The questions in A.2 can assist the reader in identifying all the characteristics of the *medical device* that could affect *safety*. Annex H contains additional points to consider in estimating *risks* from *IVD medical devices*. These lists are neither exhaustive nor representative of all *medical devices*, and the *manufacturer* is advised to add questions that can have applicability to the particular *medical device* and to skip questions that are not relevant. The *manufacturer* is also advised to consider each question not only on its own but also in relation to others.

The *manufacturer* may further consult relevant clinical literature, applicable regulations, or the essential principles of *safety* and performance for *medical devices* in ISO 16142-1[29] or for *in vitro diagnostic medical devices* in ISO 16142-2[30]. An additional source for *medical devices* where security is a concern is AAMI TIR 57[1].

A.2 Questions

A.2.1 What is the *intended use* and how is the *medical device* to be used?

Factors that should be considered include:

— what is the *medical device*'s role relative to:
  — diagnosis, prevention, monitoring, treatment or alleviation of disease,
  — diagnosis, monitoring, treatment or alleviation of or compensation for an injury,
  — investigation, replacement, modification or support of anatomy or a physiological process, or
  — control of conception?
— what are the indications for use (e.g. patient population, user profile, use environment)?
— what are the contra-indications?
— does the *medical device* sustain or support life?
— is special intervention necessary in the case of failure of the *medical device*?
— can the performance of the *medical device* be impacted in the event of a security breach (performance degradation or loss of availability)?
— can unauthorized access, unauthorized activities, or loss of data affect the *medical device safety*?

A.2.2 Is the *medical device* intended to be implanted?

Factors that should be considered include the location of implantation, the characteristics of the patient population, age, weight, physical activity, the effect of ageing on implant performance, the expected lifetime of the implant, the reversibility of the implantation, whether the implant can be modified or configured while implanted and the access connection to perform this modification or configuration (e.g. physical access point or wireless connection to the implanted *medical device*).

A.2.3 Is the *medical device* intended to be in contact with the patient or other persons?

Factors that should be considered include the nature of the intended contact, i.e. surface contact, invasive contact, or implantation and, for each, the period and frequency of contact.

A.2.4 What materials or components are utilized in the *medical device* or are used with, or are in contact with, the *medical device*?

Factors that should be considered include:

— compatibility with relevant substances;

— compatibility with tissues or body fluids;

— whether characteristics relevant to *safety* are known;

— is the *medical device* manufactured utilizing materials of animal origin?

NOTE See Annex B of ISO 10993-1:2018[22] and also the ISO 22442 series of standards[39].

A.2.5 Is energy delivered to or extracted from the patient?

Factors that should be considered include:

— the type of energy transferred;

— its control, quality, quantity, intensity and duration;

— whether energy levels are higher than those currently used for similar *medical devices*.

A.2.6 Are substances delivered to or extracted from the patient?

Factors that should be considered include:

— whether the substance is delivered or extracted;

— whether it is a single substance or range of substances;

— the maximum and minimum transfer rates and control thereof.

A.2.7 Are biological materials processed by the *medical device* for subsequent reuse, transfusion or transplantation?

Factors that should be considered include the type of *process* and substance(s) processed (e.g. auto-transfusion, dialysis, blood component or cell therapy processing).

A.2.8 Is the *medical device* supplied sterile or intended to be sterilized by the user, or are other microbiological controls applicable?

Factors that should be considered include:

— whether the *medical device* is intended for single use or reuse packaging;

— shelf-life issues;

— limitation on the number of reuse cycles;

— method of product sterilization;

— the impact of other sterilization methods not intended by the *manufacturer*.

A.2.9 Is the *medical device* intended to be routinely cleaned and disinfected by the user?

Factors that should be considered include the types of cleaning or disinfecting agents to be used and any limitations on the number of cleaning cycles. The design of the *medical device* can influence the effectiveness of routine cleaning and disinfection. In addition, consideration should be given to the effect of cleaning and disinfecting agents on the *safety* or performance of the *medical device*.

A.2.10 Does the *medical device* modify the patient environment?

Factors that should be considered include:

— temperature;

— humidity;

— atmospheric gas composition;

— pressure;

— light.

A.2.11 Are measurements taken?

Factors that should be considered include the variables measured and the accuracy and the precision of the measurement results, as well as whether the measurement apparatus or data can be compromised. In addition, the need for calibration and maintenance should be considered (see also A.2.18).

A.2.12 Is the *medical device* interpretative?

Factors that should be considered include whether conclusions are presented by the *medical device* from input or acquired data, the algorithms used, and confidence limits. Special attention should be given to unintended applications of the data or algorithm, as well as unauthorized manipulation or changes to algorithms and data.

A.2.13 Is the *medical device* intended for use in conjunction with other *medical devices*, medicines or other medical technologies?

Factors that should be considered include:

— identifying any other *medical devices*, medicines or other medical technologies that can be involved;

— the potential problems associated with interactions (such as the *medical device* impacting the performance of other *medical devices*); and

— whether the patient follows the instructions for the therapy.

A.2.14 Are there unwanted outputs of energy or substances?

Energy-related factors that should be considered include noise and vibration, heat, radiation (including ionizing, non-ionizing, and ultraviolet/visible/infrared radiation), contact temperatures, leakage currents, and electric or magnetic fields.

Substance-related factors that should be considered include substances used in manufacturing, cleaning or testing having unwanted physiological effects if they remain in the product.

Other substance-related factors that should be considered include discharge of chemicals, waste products, and body fluids.

A.2.15 Is the *medical device* susceptible to environmental influences?

Factors that should be considered include the operational, transport and storage environments. These include light, temperature, humidity, vibrations, spillage, susceptibility to variations in power and cooling supplies, and electromagnetic interference.

A.2.16 Does the *medical device* influence the environment?

Factors that should be considered include:

— the effects on power and cooling supplies;

— emission of toxic materials;

— the generation of electromagnetic disturbance.

A.2.17 Does the *medical device* require consumables or accessories?

Factors that should be considered include specifications for such consumables or accessories and any restrictions placed upon users in their selection of these.

A.2.18 Is maintenance or calibration necessary?

Factors that should be considered include:

— whether maintenance or calibration are to be carried out by the user or by a specialist;

— whether special substances or equipment are needed for proper maintenance or calibration;

— traceability of the calibrator values to a higher order reference;

— how to determine when maintenance or recalibration is needed;

— how to verify that calibration is (still) acceptable.

A.2.19 Does the *medical device* contain software?

Factors that should be considered include whether software is intended to be installed, verified, modified or exchanged by the user or by a specialist, and the authenticity of a software update.

A.2.20 Does the *medical device* allow access to information?

Factors that should be considered include accessible Ethernet ports, USB ports, serial ports, and removable hard drives.

A.2.21 Does the *medical device* store data critical to patient care?

Factors that should be considered include the possibility of the data being modified or corrupted, unauthorized access to the data, and the consequences for the patients.

A.2.22 Does the *medical device* have a restricted shelf life?

Factors that should be considered include whether the *medical device* can deteriorate over time, the impact of storage conditions and primary packaging, the communication of the expiry date (by labelling or an indicator), possibility of use after the expiry date, and the disposal of expired *medical devices*.

A.2.23 Are there any delayed or long-term use effects?

Factors that should be considered include ergonomic and cumulative effects. Examples could include pumps for saline that corrode over time, mechanical fatigue, loosening of straps and attachments, vibration effects, labels that wear or fall off, long-term material degradation.

A.2.24 To what mechanical forces will the *medical device* be subjected?

Factors that should be considered include whether the forces to which the *medical device* will be subjected are under the control of the user or controlled by interaction with other persons.

A.2.25 What determines the lifetime of the *medical device*?

Factors that should be considered include battery depletion, deterioration of materials and failure of components due to ageing, wear, fatigue or repeated use. The availability of spare parts should be considered as well.

A.2.26 Is the *medical device* intended for single use?

Factors that should be considered include:

— whether the *medical device* self-destructs after use;

— whether it is obvious to the user that the *medical device* has been used.

A.2.27 Is safe decommissioning or disposal of the *medical device* necessary?

Factors that should be considered include the waste products that are generated during the disposal of the *medical device* itself, and the proper sanitization (removal) of all sensitive data on the *medical device*. For example, does it contain hazardous material (e.g. toxic chemical or biological agent), or is the material recyclable? If the *medical device* stores data, proper handling and security of the stored data should be considered, including data removal and retention.

A.2.28 Does installation or use of the *medical device* require special training or special skills?

Factors that should be considered include the complexity and novelty of the *medical device* and the knowledge, skills and ability of the persons installing, maintaining or using the *medical device*. This can include training, education, competence assessment, certification or qualification.

A.2.29 How will information for *safety* be provided?

Factors that should be considered include:

— whether information will be provided directly to the end user by the *manufacturer* or will it involve the participation of third parties such as installers, care providers, health care professionals, laboratory directors or pharmacists and whether this will have implications for training;

— commissioning and transferring to the end user and whether it is likely/possible that installation can be carried out by people without the necessary skills;

— based on the type and expected lifetime of the *medical device*, whether re-training or re-certification of users or service personnel would be indicated.

A.2.30 Are new manufacturing *processes* established or introduced?

Factors that should be considered include the application of new or innovative technology and changes in the scale of production. This can also involve changes in contract manufacturing, suppliers and vendors.

A.2.31 Is successful application of the *medical device* dependent on the usability of the user interface?

A.2.31.1 Can the user interface design features contribute to *use error*?

Factors that should be considered include: control and indicators, symbols used, ergonomic features, physical design and layout, hierarchy of operation, menus for software-driven *medical devices*, visibility of warnings, audibility of alarms, standardisation of colour coding. See IEC 62366-1[16] for additional information on usability and IEC 60601-1-8[7] for alarms.

A.2.31.2 Is the *medical device* used in an environment where distractions can cause *use error*?

Factors that should be considered include:

— the consequence of *use error*;

— whether the distractions are commonplace;

— whether the user can be disturbed by an infrequent distraction;

— whether repetitive stress can reduce the user's awareness or attention.

A.2.31.3 Does the *medical device* have connecting parts or accessories?

Factors that should be considered include the possibility of wrong connections, similarity to other products' connections, connection force, feedback on connection integrity, and over- and under-tightening.

A.2.31.4 Does the *medical device* have a control interface?

Factors that should be considered include spacing, coding, grouping, mapping, modes of feedback, blunders, slips, control differentiation, visibility, direction of activation or change, whether the controls are continuous or discrete, and the reversibility of settings or actions.

A.2.31.5 Does the *medical device* display information?

Factors that should be considered include visibility in various environments, orientation, the visual capabilities of the user, populations and perspectives, clarity of the presented information, units, colour coding, and the accessibility of critical information.

A.2.31.6 Is the *medical device* controlled by a menu?

Factors that should be considered include complexity and number of layers, awareness of state, location of settings, navigation method, number of steps per action, sequence clarity and memorization problems, and importance of control function relative to its accessibility and the impact of deviating from specified operating *procedures*.

A.2.31.7 Is the successful use of the *medical device* dependent on a user's knowledge, skills and abilities?

Factors that should be considered include:

— the (intended) users, their mental and physical abilities, skill and training;

— the use environment, ergonomic aspects, installation requirements;

— the capability of intended users to control or influence the use of the *medical device*; and

— the personal characteristics of intended users that can affect their ability to successfully interact with the *medical device*. See IEC TR 62366-2[17].

A.2.31.8 Will the *medical device* be used by persons with specific needs?

Factors that should be considered include:

— users with special characteristics, such as disabled persons, the elderly and children, who might need assistance by another person to enable the use of a *medical device*;

— users having wide-ranging skill levels and differing cultural backgrounds and expectations that could lead to differences in what is considered appropriate application of the *medical device*.

A.2.31.9 Can the user interface be used to initiate unauthorised actions?

Factors that should be considered include whether the user interface allows the user to enter an operation mode with restricted access (e.g. for maintenance or special use), which increases the possibility of *use error* and thereby the associated *risks*, and whether the user becomes aware of having entered such operation mode.

A.2.32 Does the *medical device* include an alarm system?

Factors that should be considered are the *risk* of false alarms, missing alarms, disconnected alarm systems, unreliable remote alarm systems, and the user's ability of understanding how the alarm system works. Guidance for alarm systems is given in IEC 60601-1-8[7].

A.2.33 In what ways might the *medical device* be misused (deliberately or not)?

Factors that should be considered are incorrect use of connectors, disabling *safety* features or alarms, neglect of *manufacturer's* recommended maintenance, unauthorized access to the *medical device* or to *medical device* functions.

A.2.34 Is the *medical device* intended to be mobile or portable?

Factors that should be considered are the need for grips, handles, wheels or brakes, and the need for mechanical stability and durability.

A.2.35 Does the use of the *medical device* depend on essential performance?

Factors that should be considered are, for example, the characteristics of the output of life supporting *medical devices* or the operation of an alarm. See IEC 60601-1[5] for a discussion of essential performance of medical electrical equipment and medical electrical systems.

A.2.36 Does the *medical device* have a degree of autonomy?

Factors that should be considered include:

— awareness of the user when the *medical device* with a degree of autonomy generates an error, alarm or failure;

— awareness of the user when intervention in an autonomously performed action is required;

— the ability of the user to intervene in or to abort an action that is performed autonomously; and

— the ability of the user to select and perform proper corrective actions.

See IEC TR 60601-4-1[9] for further guidance on *medical devices* with a degree of autonomy.

A.2.37 Does the *medical device* produce an output that is used as an input in determining clinical action?

Factors that should be considered include whether incorrect or delayed outputs can result in direct or indirect *risks* to patients, e.g. an incorrect diagnosis resulting in delayed or omitted therapy for a patient. See Annex H for guidance on *in vitro diagnostic medical devices*.

Annex B
(informative)

Techniques that support *risk analysis*

B.1 General

This annex provides guidance on several techniques that can be used to support a *risk analysis*. Some techniques start with the possible *harm* and analyse the variety of events that can cause that *harm*. Other techniques start with an initiating event and analyse the subsequent sequence or combinations of events that could lead to *harm*. The basic principle is that the sequence of events is analysed.

It is emphasized that *risk analysis* is only one step of the *risk management process* described in ISO 14971:2019. Further, the techniques described in this annex do not address all elements of a *risk analysis*, and only provide supporting information. For example, the identification of *hazardous situations* is not included in all of these techniques. These techniques are complementary, and it can be necessary to use more than one of them in order to support a thorough and complete *risk analysis*.

The following analysis techniques are discussed in more detail:

— Preliminary Hazard Analysis (PHA) is a technique that can be used early in the development *process* to identify the *hazards*, *hazardous situations*, and events that can cause *harm* when few of the details of the *medical device* design are known.

— Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are especially useful in *safety* engineering, early in the development *process*, for the identification and prioritization of *hazards* and *hazardous situations* and possible *risk control* measures as well as for analysing the consequences of adverse events.

— Failure Mode and Effects Analysis (FMEA) is a technique by which effects or consequences of individual components are systematically identified and is more appropriate as the design matures and the failure modes are better understood.

— Hazard and Operability Study (HAZOP) is typically used in the early stages of the development *process* to study deviations from the intended performance.

— Hazard Analysis and Critical Control Point (HACCP) is typically used in the later stages of the development *process* to verify and then optimize design concepts or changes.

B.2 Preliminary Hazard Analysis (PHA)

PHA is an inductive method of analysis with the objective of identifying the *hazards*, *hazardous situations* and events that can cause *harm* for a given activity, facility or system. It is most commonly carried out early in the development of a project when there is little information on design details or operating *procedures* and can often be a precursor to further studies. It can be useful when analysing existing systems or prioritizing *hazards* where circumstances prevent a more extensive technique from being used.

In a PHA, a list of *hazards* and *hazardous situations* is formulated by considering characteristics such as:

— materials used or produced and their reactivity;

— equipment used;

— use environment;

— layout;

— interfaces among system components.

The method is completed with:

a) the identification of the probabilities that a *hazardous situation* occurs and the probabilities that a *hazardous situation* leads to *harm*;

b) the qualitative evaluation of the extent of possible *harm*; and

c) the identification of possible *risk control* measures.

The results obtained can be presented in different ways such as tables and trees.

B.3 Fault Tree Analysis (FTA)

FTA is primarily a means of analysing *hazards* identified by other techniques and starts from a postulated undesired consequence, i.e. a possible *harm* or *hazardous situation*, also called a "top event." In a deductive manner, starting with the top event and asking "Why?", the possible causes or fault modes of the next lower functional system level causing the undesired consequence are identified. Following stepwise identification of undesirable system operation to successively lower system levels will lead to the desired system level, which is usually either the component fault mode or the lowest level at which *risk control* measures can be applied. This will reveal the combinations most likely to lead to the postulated consequence. The results are represented pictorially in the form of a tree of fault modes. At each level in the tree, combinations of fault modes are described with logical operators (AND, OR, etc.). The fault modes identified in the tree can be events that are associated with hardware faults, human errors, or any other pertinent event, which leads to the undesired event. They are not limited to the single-fault condition.

FTA allows a systematic approach that is sufficiently flexible to allow analysis of a variety of factors, including human interactions. FTA is used in *risk analysis* as a tool to provide an estimate of fault probabilities and to identify single faults and common cause faults that result in *hazardous situations*. The pictorial representation leads to an easy understanding of the system behaviour and the factors included, but, as the trees become large, processing of fault trees can require computer systems.

See IEC 61025[12] for more information on the *procedures* for FTA.

B.4 Event Tree Analysis (ETA)

ETA is a causal analytical technique that is based on an analysis of a sequence of actions and events that can lead to a negative outcome. ETA uses the same logical and mathematical techniques as Fault Tree Analysis (FTA). However, whereas FTA analyses how an undesirable top event can occur, ETA considers the impact of the failure of a particular component or item in the system, and works out the effect such a failure can have on the overall system and on the users and patients. ETA uses an inductive approach, whereas FTA is deductive.

The initiating event in an event tree will usually fall into one of the following four categories:

a) failures or unsafe conditions in the *medical device*;

b) *use error*;

c) utility failures (such as loss of power or internet connectivity); and

d) environmental conditions (such as temperature, humidity, altitude, weather).

The goal of ETA is to determine the probability of possible negative outcomes that can result from the selected initiating event and that can eventually lead to *harm*. It is necessary to use detailed information about a system to understand the sequence of events to construct the event tree diagram. The event

tree begins with the initiating event where consequences of this event follow in a binary (success/failure) manner. Each event creates a path in which a series of successes or failures will occur where the overall probability of occurrence for that path can be estimated.

See IEC 62502[18] for more information on the *procedures* for ETA.

B.5 Failure Mode and Effects Analysis (FMEA)

FMEA is a technique by which the consequences of an individual fault mode are systematically identified and evaluated. It is an inductive technique using the question "What happens if ... ?". Components are analysed one at a time, thus generally looking at a single-fault condition. This is done in a "bottom-up" mode, i.e. following the *procedure* to the next higher functional system level.

The FMEA is not restricted to a failure of a component's design but can also include failures in the manufacturing and assembling of components (*Process* FMEA) and the use or misuse of the product by the end user (Use FMEA). FMEA can be extended to incorporate an investigation of the individual component fault modes, their probability of occurrence and detectability (only to the degree that detection will enable preventive measures in the context of ISO 14971:2019) and also the degree of *severity* of the consequences. In order to perform an FMEA, the construction of the *medical device* should be known in some detail.

Disadvantages of this technique can arise from difficulties in dealing with redundancies and the incorporation of repair or preventive maintenance actions, as well as its restriction to single-fault conditions.

See IEC 60812[10] for more information on the *procedures* for FMEA.

B.6 Hazard and Operability Study (HAZOP)

HAZOP is based on a theory that assumes that *hazardous situations* and *harm* are caused by design deviations or operational variations. HAZOP can be performed early in the development *process* when only the design and development inputs are defined. It is a systematic technique for identifying *hazards* and operability problems. It was originally developed for use in the chemical industry focusing on deviations from design intent, but there are alternative applications for *medical device* developers. HAZOP can be applied to the operation/function of the *medical device* (e.g. to the existing methods/*processes* used for the diagnosis, treatment or alleviation of disease as the "design intent"), or to a *process* used in the manufacture or maintenance/service of the *medical device* (e.g. sterilization) that can have significant impact on the function of the *medical device*.

Two particular features of a HAZOP are:

— it uses a team of people with expertise covering the design of the *medical device* and its application;

— guide words are used to help identify deviations from normal use (ALL, NONE, NO/NOT, MORE/LESS THAN, AS WELL AS, PART OF, etc.).

The objectives of the technique are:

— to produce a full description of the *medical device* and how it is intended to be used;

— to review systematically every part of the *intended use* in order to discover how deviations from the normal operating conditions and the *medical device* design can occur;

— to identify the consequences of such deviations and to decide whether these consequences can lead to *hazardous situations* or operability problems.

When applied to the *processes* used to manufacture a *medical device*, the last objective is particularly useful in those cases where the *medical device* characteristics depend upon the manufacturing *process*.

See IEC 61882[14] for more information on the *procedures* for HAZOP.

B.7 Hazard Analysis and Critical Control Point (HACCP)

HACCP is a systematic approach to identify *hazards* and *hazardous situations* and to control and monitor the associated *risks* by focusing on the critical control points in a manufacturing *process*. In the description below, *risk management* terminology is supplemented to conventional HACCP terminology where appropriate.

HACCP is based on the following seven core principles:

1. Conduct a hazard analysis (*risk analysis*) to identify *hazards* and *hazardous situations*;
2. Determine the critical control points;
3. Establish appropriate limits;
4. Monitor each critical control point;
5. Establish corrective and preventive actions (identify and implement *risk control* measures);
6. Establish *procedures* for *verification*;
7. Establish *procedures* for documentation and *record* keeping.

Each *medical device* has its own *hazards* and *hazardous situations* that can be related to its *intended use*, *reasonably foreseeable misuse* or its characteristics related to *safety*. *Hazardous situations* can be initiated by events during different phases in the *life cycle*, such as design, development, manufacturing, service, use, disposal, etc.

The heart of an effective HACCP system focuses on the continuing control and monitoring of the identified *hazards* and *hazardous situations*. The *manufacturer* demonstrates the effectiveness of the implemented *risk control* measures by establishing and documenting the *process* flow diagram, the hazard analysis worksheet and the critical control plan.

The HACCP system uses the following tools as documented evidence:

a) *Process* flow diagram

The purpose of the diagram is to provide a clear and simple description of the steps involved in the *process*. The diagram is necessary to the HACCP team in its subsequent work. The diagram can also serve as a future guide for others to understand the *process* for their *verification* activities. The scope of the *process* flow diagram should cover all the processing steps that are under the direct control of the *manufacturer*.

b) Hazard analysis worksheet

The worksheet contains the *records* of the hazard analysis (*risk analysis*):

— the identification and listing of steps in the *process* where *hazards* of significance are present;

— the listing of all identified *hazards* (and *hazardous situations*) associated with each step and their significance;

— the listing of all *risk control* measures for each *hazard* (and *hazardous situation*);

— the identification of all critical control points and their monitoring and controls.

c) Critical control plan

The plan is based on the seven principles of HACCP and delineates the *procedures* to be followed to assure the control of a specific design, product, *process* or *procedure*. The plan includes:

— identifying critical control points and appropriate limits;

— monitoring and continuing control activities;

— implementing and monitoring *risk control* measures;

— activities for *verification* and *record* keeping.

Annex C
(informative)

Relation between the policy, criteria for *risk* acceptability, *risk control* and *risk evaluation*

C.1 General

This annex describes the relation between the *manufacturer's* policy for determining acceptable *risk* as defined by *top management* and the criteria for *risk* acceptability established based on that policy. This description includes elements that can be part of the policy. It explains how the criteria for *risk* acceptability can be used in *risk control* and *risk evaluation*. Examples of the relation between the policy, the criteria and the *risk evaluation* are given for several policy elements.

C.2 Policy for establishing criteria for *risk* acceptability

The policy provides a framework for establishing the criteria for *risk* acceptability. This framework directs and guides the establishing of the criteria. This concerns both the criteria for acceptability of individual *residual risks* and the criteria for acceptability of the overall *residual risk*.

ISO 14971:2019 requires that the policy for establishing the criteria for *risk* acceptability be documented, for example as part of the *manufacturer's* quality management system documentation. However, it is not necessary that the policy is part of the *risk management file*.

A policy for establishing the criteria for *risk* acceptability can typically address the following elements:

— purpose;

— scope;

— factors and considerations for determining acceptable *risk*;

— approaches to *risk control*;

— requirements for approval and review.

The policy and its elements should be tailored to fit the specific needs of the *manufacturer's* organization. Each of the elements is discussed in more detail below.

— The purpose describes the goals of the policy for establishing criteria for *risk* acceptability.

  EXAMPLE 1 The purpose of the policy is to provide guidance for establishing the criteria for *risk* acceptability. These criteria are used in the evaluation of *residual risks* associated with the *medical devices* manufactured by [*manufacturer's* name]. The criteria will ensure that the *medical devices* have a high level of *safety* consistent with stakeholder expectations.

— The scope specifies to whom, where and when the policy applies.

  EXAMPLE 2 This policy applies to all persons involved in establishing, reviewing, updating, and approving the criteria for *risk* acceptability in *risk management* plans for *medical devices* designed, developed and/or manufactured by [*manufacturer's* name] for commercial distribution.

— The following factors and considerations should be taken into account when establishing the criteria for *risk* acceptability:

  — Applicable regulatory requirements in the regions where the *medical device* is to be marketed;

  - Relevant international standards for the particular type of *medical device*, including standards for testing of specific properties with approval/rejection limits (see also Annex E);
  - The generally acknowledged *state of the art*, which can be determined from a review of international standards, best practices in technology, results of accepted scientific research, publications from authorities, and other information for similar *medical devices* and similar other products.
  - Validated concerns from stakeholders, for example obtained through direct communication from users, clinicians, patients or regulatory bodies, or through indirect communication via news reports, social media or patient forums. It is important to consider that the perception and understanding of *risk* acceptability can vary between different groups of stakeholders and can be influenced by their background and the nature of their interest.

— Approaches to *risk control* can be defined according to ISO 14971:2019, 4.2, Note 1. The approach can include considerations of practicability, such as reducing *risk* as low as reasonably practicable, reducing *risk* as low as reasonably achievable, or reducing *risk* as far as possible without adversely affecting the *benefit-risk* ratio. Another possible approach to *risk control* can be related to the magnitude of the *risk*, for example that *risk control* can be omitted for small *risks* below a certain limit. This is elaborated further in C.4.

  EXAMPLE 3 *Risks* are reduced as far as possible without adversely affecting the *benefit-risk* ratio. Consideration is given to whether technically practicable measures would reduce the *risk* without impacting the *intended use* or the *benefit* of the *medical device*.

  EXAMPLE 4 *Risks* related to radiation exposure are reduced to a level as low as reasonably achievable (ALARA), taking account of the technical practicability of the *risk control* measures.

— Requirements for approval and review can be specified in the policy. This can include who approves and, if needed, how often the policy is reviewed.

  EXAMPLE 5 The policy for establishing the criteria for *risk* acceptability is approved by [title/function of *top management*] and is reviewed at least every [X] years by [name of reviewing body].

C.3 Criteria for *risk* acceptability

The criteria for *risk* acceptability are established based on the *manufacturer's* policy for determining acceptable *risk*. This also applies to criteria for accepting *risks* when the probability of occurrence of *harm* cannot be estimated, in which case the criteria can be based on the *severity* of *harm* alone. The criteria for *risk* acceptability are recorded in the *risk management* plan.

Specific criteria can be established for each type of *medical device* (or *medical device* family), dependent on its characteristics and *intended use*, or the same criteria can be applied to all *medical devices*. The criteria for *risk* acceptability can include combinations of qualitative requirements and quantitative limits for specific properties, preferably based on international standards.

ISO 14971:2019 requires that the criteria for the acceptability of the overall *residual risk* be established as well. These can be the same or different from the criteria for acceptability of individual *risks*. The method to evaluate the overall *residual risk* and the criteria for its acceptability are documented in the *risk management* plan. More detailed guidance on the criteria and methods are provided in Clause 8.

C.4 *Risk control*

Risk control is the *process* in which decisions are made and measures implemented by which *risks* are reduced to, or maintained within, specified levels. This *process* can be directed by the approaches included in the policy for establishing criteria for *risk* acceptability (see C.2). Two approaches to *risk control* are discussed below.

One possible approach is to consider the practicability of the *risk control* measures. Practicability (being practicable) refers to *risk control* options that are considered viable or capable of being put into

practice. This is not to be confused with practicality (being practical), which refers to measures that are useful or convenient. Practicability has two components, namely technical practicability and economic practicability.

Technical practicability refers to the ability to reduce the *risk* regardless of cost. The following are a few examples where technical practicability is questionable:

— using *risk control* measures that diminish the effectiveness of the *medical device* or compromise the *intended use* (e.g. reducing the power of an electrosurgical unit below its effective level), which also has a negative effect on the balance between *benefit* and *risk*;

— overly complex *procedures* for using the *medical device* so that the probability of *use error* is increased or the *intended use* is compromised, which has a negative effect on the balance between *benefit* and *risk* (see ISO 14971:2019, 4.2, Note 1);

— multiple alarms that create confusion and thereby hamper the operation by the user;

— including so many warnings or caution labels that the user is hampered in operating the *medical device*;

— communicating too many *residual risks* so that the user has difficulty understanding which ones are really important.

Economic practicability refers to the ability to reduce the *risk* without making the *medical device* an unsound economic proposition, because the *risk control* measures would make the *medical device* too expensive and therefore unavailable.

These decisions necessarily involve making trade-offs between accepting *risks* and the availability of treatments or diagnosis. Cost and availability implications are considered in deciding what is practicable to the extent that these impact upon the preservation, promotion or improvement of human health. The economic practicability in such decisions relates to the *benefits* for public health and for the society as a whole. However, economic practicability should not be used as a rationale for the acceptance of unnecessary *risk*.

Another possible approach to *risk control* is to consider the magnitude of the *residual risk*. This can include classifying the *risk* into one of three categories according to its magnitude:

a) the magnitude of *residual risk* exceeds the *manufacturer's* criteria for *risk* acceptability;

b) the *residual risk* is so small that it can be regarded as insignificant or negligible (i.e. removing it would not lead to a lower overall *residual risk*); or

c) the *residual risk* is between the two states specified in a) and b).

The policy can direct whether or not *risk* reduction efforts should continue for *residual risks* classified as insignificant or negligible (category b) before proceeding to *risk evaluation*.

In this approach the *manufacturer* may use a semi-quantitative *risk* chart or *risk* matrix as in Figure C.1 to support the *risk estimation* (see also 5.5). This *risk* matrix is divided into three regions corresponding to a) unacceptable *risk*, b) insignificant or negligible *risk*, and c) *risks* that require investigation to determine if further *risk* control is feasible. The estimated *risks* (R_1, R_2, R_3, ...) have been entered into the appropriate cells. *Risks* R_1 to R_3 are not acceptable. *Risks* R_4 and R_5 are investigated further, while R_6 is insignificant and can be acceptable depending on the *manufacturer's* policy.

Semi-quantitative probability levels	Qualitative *severity* levels: Negligible	Minor	Serious / Major	Critical	Catastrophic / Fatal
Frequent					
Probable	R_1	R_2			
Occasional		R_4		R_3	
Remote	R_6				
Improbable			R_5		

Key

unacceptable *risk*

investigate further *risk control*

insignificant or negligible *risk*

Figure C.1 — Example of a three-region *risk* matrix

C.5 *Risk evaluation*

In this step the *manufacturer* compares the estimated *risks* with the criteria for *risk* acceptability defined in the *risk management* plan and determines if the *residual risks* are acceptable or not. A *risk* matrix as shown in 5.5 and Figure C.1 can support the estimation and evaluation of *risk*, especially those *risks* for which no requirements or solutions in international standards exist.

C.6 Examples

The *manufacturer's* policy for determining acceptable *risk* can include multiple elements and approaches. Examples of the relation between the policy, the criteria for *risk* acceptability and the *risk evaluation* are given in Table C.1 for several of those elements and approaches.

Table C.1 — Examples of the relation between elements in the policy, the criteria for *risk* acceptability, and how the criteria are used in *risk evaluation*

Regulatory requirements	
Policy:	Criteria meet the *safety* requirements of the applicable regulations in each market in which the *medical device* is / will be marketed. For example, regulations require that the *medical device* maintains *safety* in single fault condition, including software failures.
Criteria:	The *medical devices* remain safe in single fault condition, including software failures.
Evaluation:	The *medical device* is tested and criteria based on testable limits in standards or regulations are applied. *Risk evaluation* can include inspection of test results, standard conformance reports or certificates.
International standards	
Policy:	Criteria are based on applicable international product and *process* standards.
Criteria:	1) Testable limits from international product standards are applied. 2) User interfaces are developed according to the *process* in IEC 62366-1[16].
Evaluation:	1) Inspection of compliance assessment reports for each standard. 2) Inspection of the usability engineering file.

Table C.1 *(continued)*

State of the art	
Policy:	Criteria are based on the generally acknowledged *state of the art*, as determined from similar *medical devices* available on the market and a review of literature on *intended use* and any alternative therapies or *medical devices*.
Criteria:	1) Leakage currents of the *medical device* are *state of the art*, demonstrated by compliance to the limits and tests regarding leakage current of IEC 60601-1[5]. 2) Dose accuracy of the delivery device are *state of the art*, as demonstrated by compliance to the limits and tests regarding dose accuracy of ISO 11608-1[23]. 3) Protection against mechanical failure caused by impact is on the same level as or better than a similar *medical device*, as demonstrated by comparative test such as drop test.
Evaluation:	Inspection of data and information demonstrating that the *medical device* conforms to or surpasses the limits based on the *state of the art*, based on international standards or comparison with a *medical device* on the market. *Risk evaluation* can include inspection and comparison of design specifications or comparative test results.
Stakeholder concerns	
Policy:	Criteria address known stakeholder concerns as identified in a review of medical and scientific literature on the *intended use* of the *medical device*, in usability studies, through feedback from advisory boards and/or focus groups, or during *post-production* monitoring.
Criteria:	1) *Risks* related to bovine materials are a public concern and are essentially eliminated by design. 2) *Risk* related to accidental multi-patient use of needle-based *medical devices* for drug delivery is a concern for clinical organisations, and therefore warnings are required for the *risk* to be deemed acceptable.
Evaluation:	*Risk evaluation* can include reviewing performance of the *medical device* against limits required by the stakeholders, or direct participation of stakeholders (in focus groups or similar) in *risk evaluation* activities. *Risk evaluation* can include comparing *risk estimations* with levels of *risk* that are considered acceptable by stakeholders.

Annex D
(informative)

Information for *safety* and information on *residual risk*

D.1 General

The purpose of this annex is to clarify the differences between "information for *safety*" and "disclosure of *residual risk*". It provides guidance on how information for *safety* can be provided, and how *residual risks* can be disclosed in such a way as to promote *risk* awareness.

D.2 Information for *safety*

Information for *safety* is a *risk control* measure that should be used only after the *manufacturer* has determined that (further) *risk* reduction by other measures is not practicable. The preferred options for *risk* reduction are implementing design features that make the *medical device* inherently safe and, if this is not possible, implementing protective measures. Even then, the *safety* of the patient, the user or others can still depend on certain actions to take or to avoid. Instructions on those actions constitute the information for *safety*.

Information for *safety* is instructive and gives the user clear instructions of what actions to take or to avoid, in order to prevent a *hazardous situation* or *harm* from occurring. This information can be provided in the form of warnings, (pre)cautions, contra-indications, instructions for use (including installation, maintenance and disposal), or training. ISO 14971:2019 requires the information for *safety* to be verified for effectiveness (for example by applying a usability engineering *process*) and to be traceable to the *risk assessment* in the *risk management file*.

In some cases, the text for information for *safety* is prescribed by local regulations.

When developing information for *safety*, it is important to identify to whom this information is to be provided and how it is to be provided. This can include an explanation of the *risk*, the consequences of exposure and what should be done or avoided to prevent any *harm*. The *manufacturer* should consider:

— the need to classify the information for *safety*, based on the level of *risk*;

— the level of detail necessary to convey the information for *safety*;

— the location for the information for *safety* (e.g. a warning label on the *medical device*);

— the wording, pictures or symbols to be used to ensure clarity and understandability;

— the intended recipients (e.g. users, service personnel, installers, patients);

— the appropriate media for providing the information, (e.g. instructions for use, labels, warnings in the user interface);

— regulatory requirements.

Information for *safety* can be communicated in different ways, depending on when in the *medical device life cycle* the information is to be communicated, e.g. via the user interface of a menu-driven *medical device*, as cautionary statements in the *accompanying documentation*, or in an advisory notice.

Information for *safety* can be given in various forms, such as warning labels attached to the *medical device*, warning statements in the instructions for use, instructions on a graphical user interface, or instructions in training videos. Some examples are given below.

— Warning: Do not step on surface.

— Warning: Do not remove cover, *risk* of electric shock.

— Warning: Do not use haemolyzed serum samples. These can interfere with the measurement and affect the accuracy of the result.

D.3 Disclosure of *residual risk*

Residual risk is the *risk* that remains after all *risk control* measures have been implemented. *Residual risks* can relate to the possible occurrence of side-effects or after-effects related to the use of a *medical device*. ISO 14971:2019 requires the *manufacturer* to inform users about significant *residual risks*.

Disclosure of *residual risk* is descriptive and provides the user with information necessary to understand the *residual risks* associated with the use of the *medical device*. The aim is to disclose information in the *accompanying documentation* to enable the user, and potentially the patient, to make an informed decision that weighs the *residual risks* against the *benefits* of using the *medical device*. The *manufacturer* examines the *residual risks* and determines what information the user needs to receive. The decisions of the *manufacturer* regarding the disclosure of *residual risk* are recorded in the *risk management file*.

The disclosed information can be significant in the *process* of clinical decision making. Within the framework of the *intended use*, the user can decide in which clinical settings the *medical device* can be used to achieve a certain *benefit* for the patient. The disclosure of the *residual risk* can also be useful for the user or the hospital organization to prepare the patient for possible side-effects or *harms* that can occur during or after the use of the *medical device*. Note that user and patient can be the same person, for example for *medical devices* used in the home healthcare environment.

When developing information on the disclosure of *residual risks*, it is important to identify what is to be communicated and to whom the information is directed. The *manufacturer* should consider:

— the level of detail of the information;

— the wording to be used to ensure clarity and understandability;

— the intended recipients (e.g. users, service personnel, installers, patients);

— the means and media to be used.

When determining the appropriate level of detail, the *manufacturer* should consider whether summarizing information is more appropriate than providing detailed information from the *risk management file*. The nature and extent of the information should be commensurate with the *residual risk* and the knowledge and experience of the intended recipient of the information.

Some examples are given below to illustrate the *residual risks* associated with using *medical devices* and the side-effects that are normally disclosed.

— Linear accelerators can be used to treat tumours. The *residual risks* of radiation therapy for tumours include the possibility of erythema or epilation.

— When undergoing magnetic resonance imaging (MRI), the patient can be in an enclosed space. Some patients can experience claustrophobia.

— Mechanical ventilation to assist or replace spontaneous breathing can lead to complications such as airway injury, alveolar damage or pneumothorax.

— After undergoing lithotripsy of kidney stones, about 10 % of patients have blood in their urine or feel pain in the kidneys as small stone fragments pass, while about 2 % of patients incur an infection of the urinary tract.

— Potential complications from using an ophthalmic surgical laser include swelling, inflammation or pain in the eye. Mild light sensitivity occurred in 1 % of patients until 6 weeks after surgery.

— Patients with an implantable cardioverter defibrillator (ICD) system can experience inappropriate shocks, imagined (phantom) shocks, dependency, depression, fear of shocks while awake.

See H.5 for additional guidance on the disclosure of *residual risk* for *in vitro diagnostic medical devices*.

Annex E
(informative)

Role of international standards in *risk management*

E.1 General

International standards can play a significant role in *risk management* by providing requirements for the *safety* of products and/or *processes*. ISO/IEC Guide 63[20] provides guidance on the development and inclusion of *safety* aspects in international standards for *medical devices*. International standards are developed by experts in the field and are considered to represent the generally acknowledged *state of the art*.

When performing *risk management*, the *manufacturer* first considers the *medical device* being designed, its *intended use*, its characteristics related to *safety*, and the associated *hazards* and *hazardous situations*. *Manufacturers* can select and apply product standards and *process* standards that contain specific requirements to assist in managing the *risks* associated with those *hazards* and *hazardous situations* during the *life cycle* of the *medical device*.

For *medical devices* that satisfy the requirements and the compliance criteria of these standards, the *residual risks* related to those *hazards* and *hazardous situations* can be considered acceptable unless there is *objective evidence* to the contrary (for example reports of adverse events, product recalls or complaints). The requirements of international standards (such as engineering or analytical *processes*, specific output limits, warning statements, or design specifications) can be considered *risk control* measures that are intended to address the *risks* of specific *hazardous situations*.

In many cases, the standards writers have performed and completed elements of *risk management* and provide *manufacturers* with solutions in the form of design requirements and test methods for establishing conformity. When performing *risk management* activities, *manufacturers* can take advantage of the work of the standards writers and not repeat the analyses that led to the requirements of the standard. International standards, therefore, provide valuable information on *risk* acceptability that has been validated during a worldwide evaluation *process*, including multiple rounds of review, commenting and voting to reach international consensus.

E.2 Use of international product *safety* standards in *risk management*

An international product *safety* standard can establish requirements that, when implemented, result in acceptable *risk* for specific *hazardous situations* (e.g. design solutions, *safety* limits). The *manufacturer* can apply these requirements in the following way when managing *risk*.

a) Where an international product *safety* standard specifies requirements addressing particular *hazards* or *hazardous situations*, together with specific acceptance criteria, compliance with those requirements is presumed to establish that the *residual risks* have been reduced to acceptable levels, unless there is *objective evidence* to the contrary. For example, IEC 60601-1[5] provides leakage current limits that are considered to result in an acceptable level of *risk* when measured under specified conditions. In this example, further *risk management* would not be necessary. The following steps are taken in this case.

    1. Identify characteristics related to *safety* and identify *hazards* and *hazardous situations* associated with the *medical device*.

    2. Identify those *hazards* and *hazardous situations* that are completely covered by the international product *safety* standard.

3. For those identified *hazards* and *hazardous situations* that are completely covered by the international product *safety* standard, the *manufacturer* can rely on the requirements in the international standard to demonstrate acceptable *risk*.

4. To the extent possible, the *manufacturer* should ensure that the design specifications of the *medical device* conform with the requirements in the standard that serve as *risk control* measures.

   NOTE For some international product *safety* standards, the possibility of identifying all specific *risk control* measures is limited. One example is electromagnetic compatibility testing in IEC 60601-1-2[6] for complex *medical devices*.

5. *Verification* of the implementation of the *risk control* measures for these *hazardous situations* is obtained from a review of the design documentation. *Verification* of the effectiveness of the *risk control* measures is obtained from the tests and test results demonstrating that the *medical device* meets the relevant requirements of the international product *safety* standard.

6. If the relevant requirements are met, the associated *residual risk* is considered acceptable. The use of the standard should be documented in the *risk management file* to support the acceptance of the *residual risk*.

b) Where an international product *safety* standard does not completely specify requirements and associated tests and test acceptance criteria, the situation is more complex. In some cases, the standard provides specific tests related to known *hazards* or *hazardous situations* without specific test acceptance criteria (e.g. IEC 60601-2-16[8]). In some other cases, the standard only identifies specific *hazards* or *hazardous situations* without further requirements (e.g. some clauses of IEC 60601-1[5]). The range of alternatives is too large to provide specific guidance on how to use such standards in the *risk management process*. *Manufacturers* are encouraged, however, to use the content of such standards in their *risk management* of the particular *medical device*.

c) Where an identified *hazard* or *hazardous situation* is not specifically addressed in international product *safety* standards, the *manufacturer* addresses that *hazard* or *hazardous situation* in the *risk management process*. The *manufacturer* estimates and evaluates the *risk* and, if necessary, controls the *risk*.

See Figure E.1 for a flowchart and an example outlining the use of international product *safety* standards.

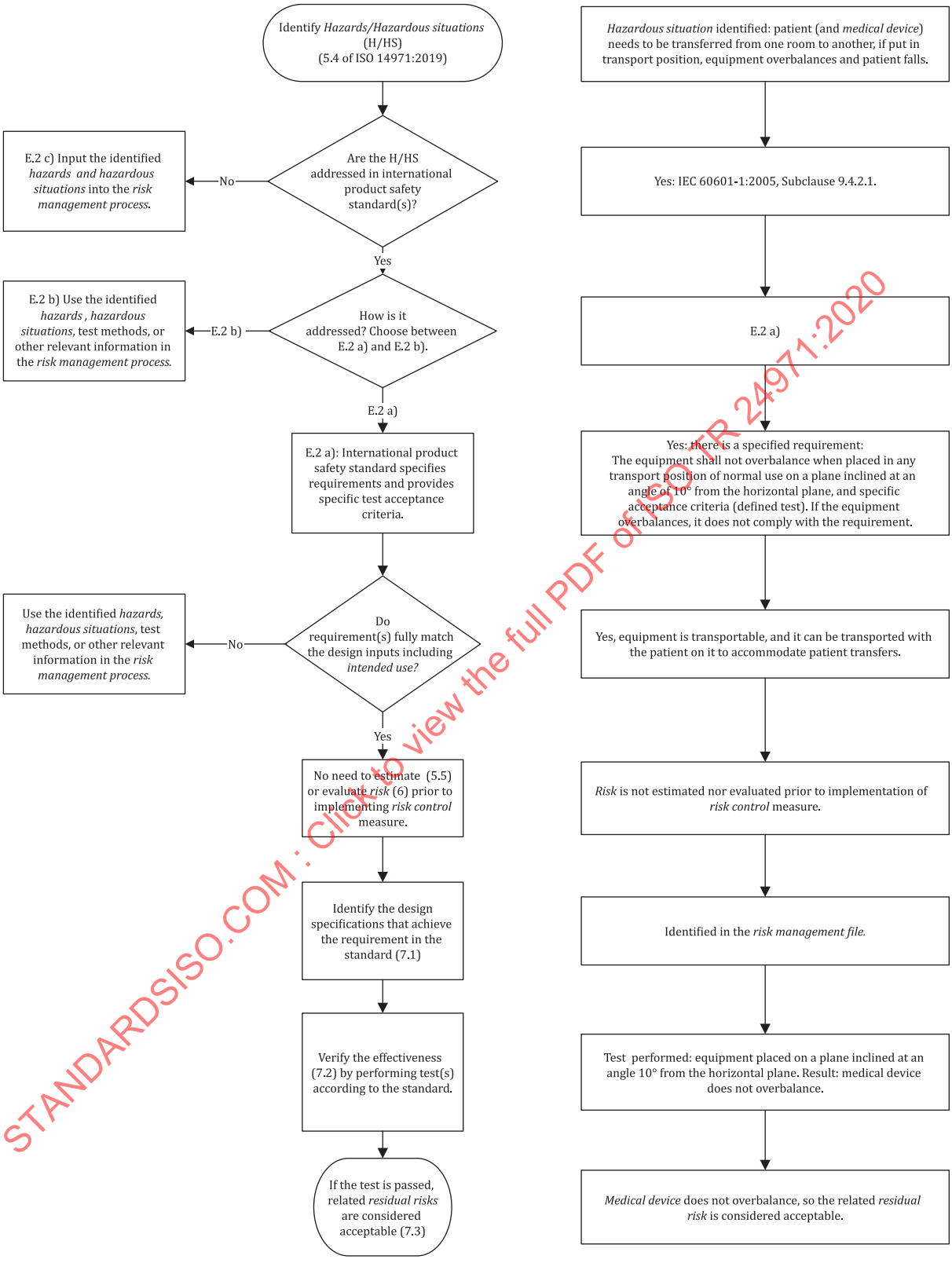


Figure E.1 — Use of international product *safety* standards and example of such standard that specifies requirements and provides specific test acceptance criteria

E.3 International *process* standards and ISO 14971

International *process* standards, as shown in the examples below, can often be used in conjunction with ISO 14971. This is performed in several ways:

— The international *process* standard requires application of ISO 14971 as part of the implementation of the international *process* standard; or

— The international *process* standard is intended to be used in *risk management*.

In either case, proper use of the international *process* standard requires attention to the interfaces between that standard and ISO 14971 in order to achieve acceptable levels of *risk* for the *medical device*. The standards should work together such that inputs, outputs and their timing are optimized. Some examples are given below to demonstrate this ideal situation.

a) IEC 62304*, Medical device software – Software life cycle processes*

The relationship between IEC 62304 and ISO 14971 is well-described in the introduction to IEC 62304:2006 and AMD1:2015[15]:

"As a basic foundation it is assumed that *medical device* software is developed and maintained within a quality management system (see 4.1 of IEC 62304:2006 and AMD1:2015[15]) and a *risk management process* (see IEC 62304:2006 4.2 and AMD1:2015[15]). The *risk management process* is already very well addressed by the International Standard ISO 14971. Therefore IEC 62304 makes use of this advantage simply by a normative reference to ISO 14971. Some minor additional *risk management* requirements are needed for software, especially in the area of identification of contributing software factors related to *hazards*. These requirements are summarized and captured in IEC 62304:2006 Clause 7 and AMD1:2015[15] as the software *risk management process*.

Whether software is a contributing factor to a *hazardous situation* is determined during the *hazard* identification activity of the *risk management process*. *Hazardous situations* that could be indirectly caused by software (for example, by providing misleading information that could cause inappropriate treatment to be administered) need to be considered when determining whether software is a contributing factor. The decision to use software to control *risk* is made during the *risk control* activity of the *risk management process*. The software *risk management process* required in this standard has to be embedded in the device *risk management process* according to ISO 14971."

IEC 62304 makes a normative reference to ISO 14971 and specifically requires:

— software development planning (see IEC 62304:2006 5.1 and AMD1:2015[15]), which requirements are consistent with the *risk management* plan required by ISO 14971; and

— a software *risk management process* (see IEC 62304:2006 Clause 7 and AMD1:2015[15]), which requirements are based upon ISO 14971.

b) IEC 62366-1 *Medical devices – Application of usability engineering to medical devices*

The flow diagram in Figure A.4 of IEC 62366-1:2015[16] demonstrates the relationship and interconnection of the two parallel and interconnecting *processes* of *risk management* and usability engineering. IEC 62366-1[16] identifies several specific clauses where the usability engineering *process* can supplement and interact with *risk management* as described in ISO 14971:

— 5.1 of IEC 62366-1:2015[16] requires the *manufacturer* to prepare a use specification, which can be an input to determining the *intended use* according to ISO 14971;

— 5.2 of IEC 62366-1:2015[16] requires the *manufacturer* to identify user interface characteristics that could be related to *safety* as part of a *risk analysis* performed according to ISO 14971;

— 5.3 of IEC 62366-1:2015[16] requires the *manufacturer* to identify known or foreseeable *hazards* and *hazardous situations*, which could affect patients, users or others, related to the use of the *medical device*, as part of a *risk analysis* performed according to ISO 14971;

— 5.9 of IEC 62366-1:2015[16] requires the *manufacturer* to perform a summative evaluation on the final user interface of the *medical device* as part of *risk management*.

c) ISO 10993-1, *Biological evaluation of medical devices — Part 1: Evaluation and testing within a risk management process*

ISO 10993-1[22] is a guidance document for the biological evaluation of *medical devices* within a *risk management process*, as part of the overall evaluation and development of each *medical device*.

Annex B of ISO 10993-1:2018[22] provides guidance on the *risk management* approach according to ISO 14971 for the identification of biological *hazards* associated with *medical devices*, the estimation and evaluation of the *risks*, the control of those *risks*, and monitoring the effectiveness of the *risk control* measures.

This approach combines the review and evaluation of existing data from all sources, with the selection and application of additional tests (where necessary), thus enabling a full evaluation to be made of the biological responses to each *medical device*, relevant to its *safety* in use.

The biological evaluation should be conducted in a manner similar to that used for other product *risks*, and should include a *risk analysis* (what are the *hazards* and associated *risks*?), a *risk evaluation* (are they acceptable?), *risk control* (how will they be controlled?), and an evaluation of overall *residual risk*. The biological evaluation should take account of:

— the physical and chemical characteristics of the various choices of materials;

— any history of clinical use or human exposure data;

— any existing toxicology and other biological *safety* data on product and component materials.

The amount of data required and the depth of the investigation can vary with the *intended use* and can depend on the nature and duration of patient contact.

According to ISO 10993-1[22], expert assessors should determine if the available information is sufficient to determine if the overall *residual risk* associated with biological *hazards* is acceptable. This conclusion is documented in the Biological Evaluation Report, which becomes an element of the *risk management file*. In agreement with the *processes* defined in ISO 14971:2019, if the evaluation of overall *residual risk* concludes that the identified *risks* are acceptable, no further *risk control* is needed. Otherwise, appropriate measures should be taken to further control the *risks*.

d) ISO 14155, *Clinical investigation of medical devices for human subjects — Good clinical practice*

ISO 14155[26] addresses good clinical practice for the design, conduct, recording and reporting of pre-market and post-market clinical investigations carried out in human subjects to assess the clinical performance or effectiveness and *safety* of *medical devices*. This is relevant to the estimation of clinical *risks* and the assessment of the *benefit-risk* balance for *medical devices*.

Annex F
(informative)

Guidance on *risks* related to security

F.1 General

The *risk management process* described in ISO 14971:2019 can be applied to *hazards* and *risks* associated with the security of the *medical device*. *Risks* related to data and systems security are specifically mentioned in the scope of ISO 14971:2019 to avoid any misunderstanding that a separate *process* would be needed to manage *risks* related to the security of *medical devices*. This does not preclude the possibility of applying specific standards, in which specific methods and requirements are provided for the assessment and control of security *risks*.

Breaches of data and systems security can lead to *harm*, e.g. through loss of data, uncontrolled access to data, corruption or loss of diagnostic information, or corruption of software leading to malfunction of the *medical device*.

Security in this document includes cybersecurity and data and systems security.

F.2 Terminology used in security *risk management*

Security *risk management* often employs different terminology than ISO 14971:2019. Nevertheless, correspondence exists between the terms used in security *risk management* and those used in ISO 14971:2019. The following defined terms originate from IEC Guide 120[4]. Other definitions such as those from AAMI TIR 57[1] are also used in security *risk management*.

— **Security:** a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences (see 3.13 in IEC Guide 120:2018[4]), where hostile acts or influences could be intentional or unintentional.

NOTE In 2.6 of AAMI TIR 57:2016[1] and 2.5 of IEC 80001-1:2010[19], security is defined as an operational state of a *medical device* in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity and availability. This can be seen that security is focused on hostile acts as events that can contribute to *risk*, and that security is considered to be a state of inviolability as being free from unacceptable *risk* (similar to *safety*, see 3.26 in ISO 14971:2019).

— **Threat:** potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause *harm* (see 3.16 in IEC Guide 120:2018[4]). Threat corresponds to an event or a sequence of events that can exploit a vulnerability leading to a *hazardous situation* (see 3.5 in ISO 14971:2019).

— **Vulnerability:** flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy (see 3.18 in IEC Guide 120:2018[4]). Vulnerability can be seen as a type of event or circumstance (see Table C.2 in ISO 14971:2019).

— **Confidentiality**: property that information is not made available or disclosed to unauthorized individuals, entities, or *processes* (see 3.6 in IEC Guide 120:2018[4]).

— **Integrity**: property of accuracy and completeness (see 3.9 in IEC Guide 120:2018[4]).

— **Availability**: property of being accessible and usable upon demand by an authorized entity (see 3.5 in IEC Guide 120:2018[4]).

The relationship between a *hazard*, sequence of events, *hazardous situation*, and *harm* relating to security can be represented as shown in Figure F.1.

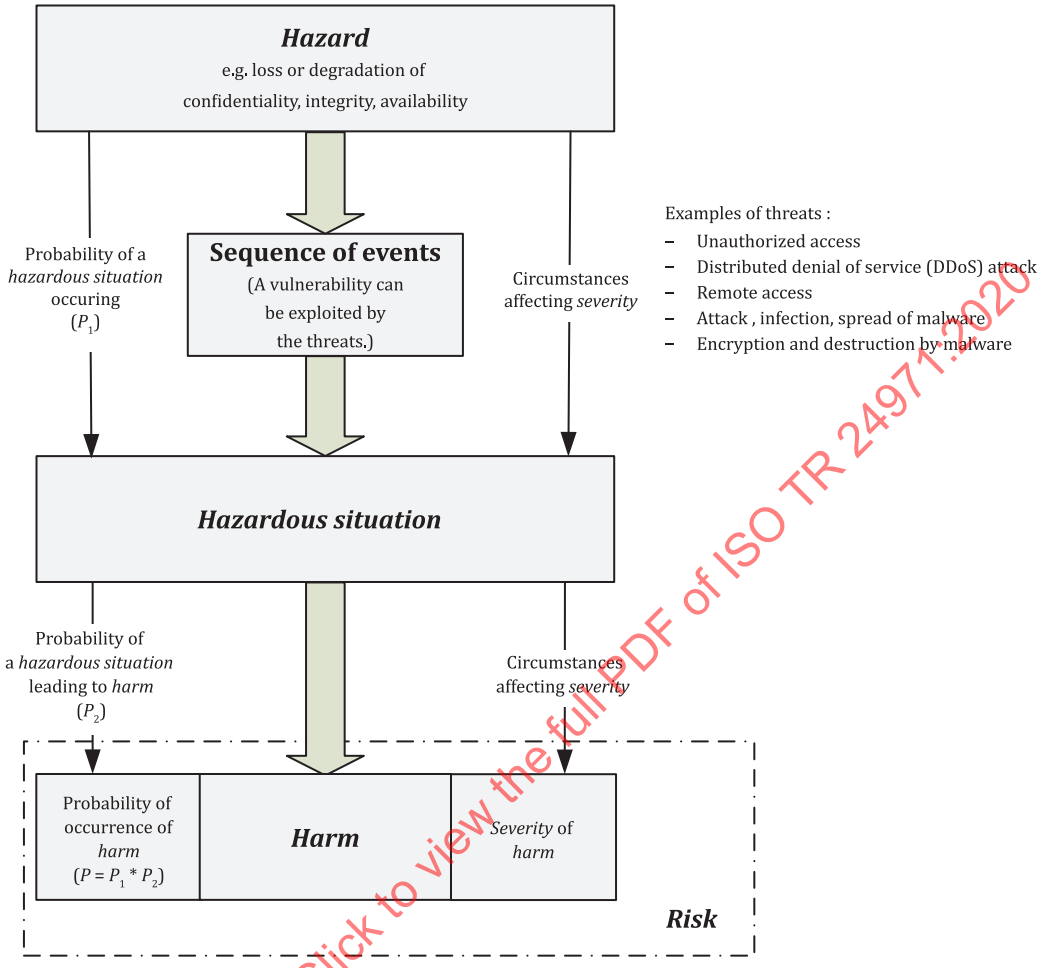


Figure F.1 — Relation between *hazard*, *hazardous situation*, *harm* and security terminology

F.3 Relation between ISO 14971 and security

A common misconception is that ISO 14971:2019 would only apply to the health of people, disregarding that the definition of *harm* includes damage to property and the environment. This misconception is often discovered during discussions of security, where it is assumed that ISO 14971:2019 is restricted to *risks* related to the patient and the user and would not cover *risks* related to security.

It should be noted that the definition of security from IEC Guide 120[4] is not on the same level as the definition of *safety*. *Safety* is related to the final outcome of *risk management,* while security looks at the effects of hostile acts or events on the characteristics and performance of the system.

The definition of *harm* in ISO 14971:2019 applies to people, property, and the environment, with the potential for some overlap. For example, damage to an electronic health *record* (damage to property) can additionally result in incorrect diagnosis which can lead to patient injury (damage to people). It is noted that the scope of security *risk management* is often broader. Several examples of security *hazards* that can lead to *harm* are shown in Table F.1.

Table F.1 — Examples of *hazard*, sequence of events, *hazardous situation* and *harm* in the situation of security *hazards*

Hazard	Sequence of events	*Hazardous situation*	*Harm*
Loss of data integrity	1) The vulnerability of unnecessarily opened network port is exploited. 2) Dose setting data of infusion pump is modified by unauthorized access.	Incorrect dosage data leading to infusion fluid not being delivered as intended.	Deterioration of health. Death.
Loss of data integrity	1) The vulnerability of unnecessarily opened network port is exploited. 2) Patient data or diagnostic results are modified by unauthorized access.	Modified data leading to incorrect clinical decisions or *procedures*, or lack of treatment.	Deterioration of health. Unnecessary surgery.
Loss of data availability	1) The vulnerability of unnecessarily opened network port is exploited. 2) *Medical device* performance is reduced or is terminated by DDoS attack or ransomware.	Delay of therapy. Inability of diagnosis.	Loss of *medical device* functionality. Deterioration of health.
Loss of data confidentiality	1) The vulnerability of unnecessarily opened network port is exploited. 2) Disclosure of personal health information.	Denial of insurance coverage leading to lack of treatment.	Psychological stress. Deterioration of health.

Additionally, when differentiating between these domains, the terms "safety risk management" and "security risk management" are sometimes used. This document follows the suggestion from ISO/IEC Guide 63[20] which states that the term "*safety*" should not be used as an adjective. It should be kept in mind that the goal of security *risk management* is also to achieve *safety* (i.e. freedom from unacceptable *risk*) when using the ISO 14971 framework to manage *risks* related to security.

It is noted that the definition of security from IEC Guide 120[4] includes unintentional acts, such as the accidental release of personal health information that is not due to a malicious attack, and that security *hazards* related to normal use should also be evaluated, such as displaying personal health information to unauthorized persons.

F.4 Characteristics of security *risk management*

Security *risk management* follows a similar *process* as management of other *risks* in that the *process* steps include establishing criteria for *risk* acceptability, performing *risk analysis*, *risk evaluation*, *risk control*, evaluation of overall *residual risk*, etc. The specific details regarding the data sources used, analysis tools and techniques, and validation can vary, but the overall *process* is the same.

ISO 14971:2019 requires the evaluation of *risks* arising from *risk control* measures. It is possible that new *risks* are introduced by security control measures or vice versa. For example, a security control measure is to require the user to enter a password before use, but on a life-saving *medical device* (e.g. an automatic external defibrillator) the potential for delays due to a forgotten password might be unacceptable, and therefore different options should be considered. This relationship is illustrated in Figure F.2.

Management of *hazards* related to security can require different methods and approaches than management of other *hazards*, similar to differences in methods for controlling *risks* related to usability or reliability.

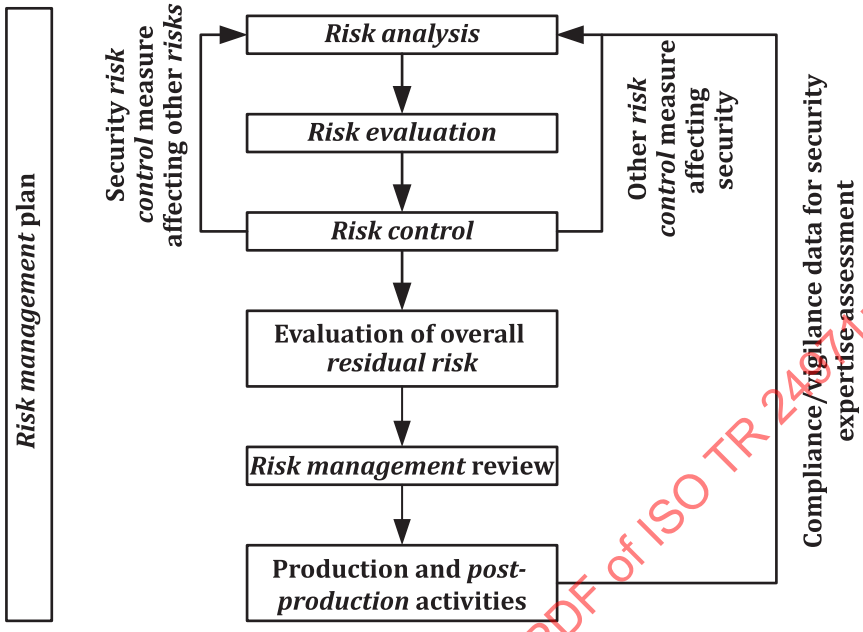


Figure F.2 — Possible interaction of security *risk control* measures with other *risk control* measures

Severity is defined as the "measure of the possible consequences of a *hazard*" (see 3.27 in ISO 14971:2019). *Severity* is often represented in degrees of degradation of a person's health. A low *severity* can be defined as temporary discomfort or a light injury requiring no medical intervention, a medium *severity* as an injury requiring medical intervention, and a high *severity* as an injury requiring immediate medical intervention and possibly leading to permanent impairment or even death. In security *risk management*, a secure data system maintains high confidentiality, integrity, and availability. Therefore, the *severity* of *harm* related to the damage to a secure system could consider among others the consequences of loss or degradation of these three factors.

Harm is often injury or damage to the health of people and related to basic *safety* (e.g. electric shock) or the *intended use* of the *medical device* (e.g. radiation exposure during X-ray imaging). In security *risk management*, the *harm* is often damage to property and related to information on the *medical device* itself (e.g. disclosure of personal health information, modification or corruption of software or data), or information available on connected devices (e.g. loss of connectivity, access to credit card information).

Probability of occurrence of *harm* is often a function of design and manufacturing, material selection, tolerances, design margins, etc. These factors can often be predicted with high levels of confidence. In security *risk management*, probability of occurrence is often a function of motivation, financial gain, as well as function of opportunity, e.g. open vulnerabilities. These factors are not easily estimated. Additionally, the probability (likelihood) of a vulnerability being exploited can quickly change from "remote" to "every time" once vulnerability information is published on the internet.

F.5 Prioritizing confidentiality, integrity, and availability

When evaluating security-related *risks*, the *manufacturer* ensures that the security priorities (confidentiality, integrity and availability) properly take the *intended use* of the *medical device* into account. For some applications, integrity of information is of high concern and a loss of integrity could result in changes to a patient's medical *record* (e.g. changes in drug orders or medical data/images). In other instances, loss of confidentiality could be more important, because disclosure of personal health information can create a potential for blackmail.

Another example of loss of confidentiality is a situation where design features are not encrypted (data at rest or in transit). Reverse engineering of those features could compromise operation of the *medical device* and result in injury to the patient. Loss of availability of the *medical device* can result in delay of diagnosis or delay of treatment. Especially for life supporting or life-saving *medical devices*, loss of availability or a reduction in effectiveness can be most important to the health of people. These examples indicate that *risks* related to security can impact the patient's health, depending on the *intended use* of the *medical device*.

Annex G
(informative)

Components and devices designed without using ISO 14971

G.1 General

This guidance assumes that the *manufacturer* has already established a *risk management process* compliant with ISO 14971:2019. It does not replace or eliminate any of the requirements in ISO 14971:2019 for a *medical device*, but recommends a way for the *manufacturer* to remediate deficiencies that might exist in the *risk management file*.

For various reasons, a *manufacturer* might not have followed all the *processes* and requirements described in ISO 14971:2019 for each constituent component of a *medical device*, such as proprietary components, software components, subsystems of non-medical origin, or for *medical devices* already available on the market. In such cases, the *manufacturer's risk management* documentation could be limited and insufficient for the purpose of demonstrating compliance with ISO 14971:2019. In most cases, however, a wealth of information about the *medical device* and its constituent components is available. For example, information on the actual use could be acquired through a review of *post-production* data for the *medical device* or for similar *medical devices* on the market. Relevant reliability and production data and previously compiled *safety*-related documentation could also be available.

This annex aims to provide a *manufacturer* with guidance on how available information can be used to build an initial *risk management file* that can be maintained in the future.

NOTE "*Medical device*" includes its subsystems, components and software components of medical origin and of non-medical origin.

Using available information, the *manufacturer* can establish *risk management* documentation that would be the basis for building an initial *risk management file* for the particular *medical device* under consideration. This documentation could be sufficient evidence to demonstrate that the *risks* for the particular *medical device* are acceptable, and that the *medical device* is safe for its *intended use*. On the other hand, the *manufacturer* could decide that additional *risk control* measures are appropriate. For example, comparison to the generally acknowledged *state of the art* could indicate that additional actions are warranted in order to become fully compliant with ISO 14971:2019.

G.2 *Risk management* plan

ISO 14971:2019 requires that all *risk management* activities be planned, especially those activities for the creation of a *risk management file* demonstrating that the *medical device* is safe for its *intended use*. The mandatory elements of a *risk management* plan are given in ISO 14971:2019.

In establishing a *risk management* plan, particular attention should be given to:

a) *risk management* activities for the remaining phases of the *life cycle* of the *medical device* (especially maintenance, decommissioning and disposal, where applicable);

b) the assignment of responsibilities and authorities;

c) requirements for review of *risk management* activities from now on;

d) the criteria for *risk* acceptability, based on the *manufacturer's* policy for determining acceptable *risk*, including criteria for accepting *risks* when the probability of occurrence of *harm* cannot be estimated;

e) a method to evaluate the overall *residual risk* and criteria for acceptability of the overall *residual risk*;

NOTE 1 The criteria under d) and e) can be supported by production and *post-production* information.

f) *verification* activities, both for existing *risk control* measures and for new *risk control* measures that are considered necessary;

g) activities for the collection and review of production and *post-production* information, and how this information is used to determine if the *risks* associated with the *medical device* are acceptable.

NOTE 2 The design documentation or other documentation can include some *verification* evidence.

G.3 *Risk management file*

Since the *medical device* was designed without using ISO 14971:2019, the *manufacturer* should start building a *risk management file*. It is likely that some *risk control* measures have already been implemented but without recorded traceability to the *hazards* and *hazardous situations* associated with the *medical device*. Therefore, the *manufacturer* could begin by identifying the solutions already adopted for the *medical device* and then by identifying the *hazards* and *hazardous situations* that are controlled by these solutions. These solutions are now considered *risk control* measures and are documented in the *risk management file*.

Such approach to build a *risk management file* can consist of the following steps.

1. Documenting the *intended use* of the *medical device*, the *reasonably foreseeable misuse* and the characteristics related to *safety*. *Reasonably foreseeable misuse* can be derived from the information about actual use gathered during the *post-production* phase. The questions in Annex A can be useful to determine the characteristics related to *safety*.

2. Identifying all solutions already adopted in the *medical device* that can be considered *risk control* measures.

3. Identifying all *hazards* and *hazardous situations* associated with the *medical device* and the possible *harm* that can result from them.

4. Determining if any *hazard* or *hazardous situation* exists for which no *risk control* measure is implemented. In those cases, the *manufacturer* should estimate and evaluate the *risk* and apply ISO 14971:2019. For *hazards* and *hazardous situations* for which *risk control* measures are implemented, the *manufacturer* should verify their effectiveness and estimate and evaluate the *residual risk*. For *residual risks* that are not judged acceptable using the criteria for *risk* acceptability defined in the *risk management* plan, the *manufacturer* should consider further *risk control* and apply ISO 14971:2019.

5. Documenting traceability for each identified *hazard* and *hazardous situation* to the *risk control* measures. The traceability can be documented with the following elements:

   — the identified *hazards* and *hazardous situations*;

   — the possible *harm* that can occur;

   — the *risk control* measures;

   — *verification* of implementation and effectiveness; and

   — the acceptability of any *residual risks*.

6. Evaluating the overall *residual risk* according to ISO 14971:2019 Clause 8.

7. Reviewing the execution of the *risk management* plan according to ISO 14971:2019 Clause 9 and documenting the results in a *risk management* report.

The *records* and other documents generated during these steps form the initial *risk management file*.

Annex H
(informative)

Guidance for *in vitro diagnostic medical devices*

H.1 General

H.1.1 *Risk management* for *IVD medical devices*

The purpose of this annex is to provide guidance for the application of particular aspects of ISO 14971:2019 to *in vitro diagnostic medical devices*. This guidance is focused on the indirect *risks* to patients from incorrect or delayed in vitro diagnostic results, and is intended to supplement the general guidance provided throughout this document. *Risks* to device users, other persons and the environment are addressed elsewhere in this document. *Manufacturers* of other diagnostic *medical devices* might also find these guidelines useful.

Throughout this annex, "clinician" is used as a general term to mean a healthcare provider who sees patients and who orders, interprets and acts upon IVD examination results. For definitions of other terms commonly used in the IVD industry and laboratory medicine, see ISO 18113-1[34].

Because *IVD medical devices* and their *intended use* are so diverse, this annex can only provide general guidance, with the intent to foster critical thinking, cross-functional analysis and informed decision-making within the *manufacturer's risk management process*. The questions and examples in this annex are intended to guide those with appropriate scientific, engineering and clinical expertise to develop and execute effective *risk management* plans for *IVD medical devices*. They are not intended to be exhaustive nor necessarily represent best practice for all *IVD medical devices*. Each *manufacturer* should determine what is applicable to their particular *IVD medical devices*.

H.1.2 Context for IVD *risk management*

Managing *risks* to patients can be challenging for *manufacturers* of *IVD medical devices*. These *risks* are indirect, often characterized by extended sequences of events that involve "competent intermediaries" such as trained users who use *IVD medical devices* to perform IVD examinations and clinicians who rely on the examination results. ISO 15189[27], the international standard for quality and competence of medical laboratories, requires medical laboratories to control *risks* to patients. To support this requirement, ISO 22367[38] was developed to describe a *risk management process* for medical laboratories based on the same principles and concepts described in ISO 14971:2019. This will promote effective *risk* communication between *manufacturers* of *IVD medical devices* and medical laboratories.

The information for *safety* and the disclosure of *residual risks* from the *manufacturer's risk management process* are important inputs to the medical laboratory's *risk management process*. Conversely, the needs of users of *IVD medical devices* for such information and the laboratory's feedback from using the *IVD medical devices* are important inputs to the *manufacturer's risk management process*. It is incumbent upon the *manufacturer* to include the user needs for *risk management* information as design input when developing or modifying an *IVD medical device*.

When a *manufacturer* supplies an *IVD medical device* to a medical laboratory, any *risks* that could not be controlled through design or protective measures are transferred to the laboratory along with the information for *safety* to control those *risks*. The *manufacturer* also discloses any *residual risks* in the *accompanying documentation*, so that the laboratory director can evaluate these *risks* and determine their acceptability.

Manufacturers can provide information for *safety* to inform users of *IVD medical devices*, but they cannot influence the actions of clinicians who order, receive and act upon the examination results.

Some *IVD medical devices* are intended for use by clinicians at the point of care, while self-testing *IVD medical devices* are actually used by patients. Although similar *risk* scenarios can exist for these devices, the user's ability to control the *risks* can be more limited. Therefore, it is important that point of care devices and self-testing devices are designed with *risk control* measures appropriate for the (intended) users and the (intended) use environment outside laboratories.

H.2 *Risk analysis*

H.2.1 *Intended use* and *reasonably foreseeable misuse*

H.2.1.1 Analytical and clinical use

Most *IVD medical devices* have two users. It is important to consider:

— a user who performs all or part of an examination ("analytical use"); and

— a clinician who receives, interprets and acts on the examination results ("clinical use").

In the case of *IVD medical devices* intended for self-testing, the patient can be the only user.

H.2.1.2 Device description

Each *risk analysis* begins with identifying and documenting a clear description of the *IVD medical device* and its specific role in producing the examination result. Questions to consider when describing the *IVD medical device* include:

— Is the device used alone to produce examination results or in combination with other devices?

  — If the device is a standalone analytical system, is it automated (software, robotics)?

  — If used in combination with other *IVD medical devices* to form a system, what is its role in producing the examination result (e.g. sample collection system, sample receptacle, measuring instrument, software, databases, reagents, calibrators, control materials, or accessory)?

  — If part of a system, how does the *IVD medical device* interact with other components of the system?

— Are other reagents or accessories necessary but not provided?

— Does the device employ new or novel technology (e.g. for measurement, communication)?

— Does the device employ digital information technology for documenting and/or transmitting examination results to clinicians or communicating with mobile applications?

— Do software applications provide diagnostic or treatment recommendations?

— Does the *IVD medical device* communicate with a *medical device* that immediately administers treatment based on the IVD result (e.g. an *IVD medical device* that measures blood glucose levels and communicates with an implanted insulin administration system)?

H.2.1.3 Analytical use

The *intended use* of the *IVD medical device* includes the analyte(s) intended to be detected or measured; acceptable sample types; calibration, quality control and preventive maintenance activities; and the use environment. It is important that *reasonably foreseeable misuse* is also considered (see H.2.3.5).

Questions to consider when identifying the analytical use of the *IVD medical device* include:

— What analyte is the device intended to measure or examine?

— Will the examination results be qualitative, semi-quantitative or quantitative?

— Will the device be used in the pre-examination, examination or post-examination phase?

— What specimens can be analysed (e.g. serum, plasma, blood, urine, other body fluids, tissues)?

— Do other substances potentially found in these samples interfere with the analytical *process*?

— In nucleic acid sequencing *procedures*, is the amplicon sensitive to contamination from environmental sources of DNA/RNA?

— Are there any additional limitations for use in specific use environments (e.g. medical laboratories, emergency room, operating room, ambulance, intensive care unit, neonatal care unit, nursing home, physician's office, screening clinics, or the patient's home)?

— Does the *IVD medical device* interface, connect or communicate with other devices or networks?

— Who will be using the *IVD medical device* to perform examinations, and what training and qualifications will be appropriate?

H.2.1.4 Clinical use

The intended clinical use of the *IVD medical device* (called indications for use in some jurisdictions) includes the medical conditions and patient populations for which the examination results are used. *Manufacturers* can rely on internal or external clinical experts to understand the following:

— how the IVD examination results will be used in clinical decision making;

— the medical decision points and degree of accuracy required;

— whether clinicians can recognize incorrect results (e.g. based on magnitude of error or consistency with other clinical information);

— what actions the clinician would take in the event of an abnormal or unexpected result;

— the clinical significance of delayed results, if any;

— potential adverse consequences of unnecessary medical intervention.

Additional questions to consider when identifying the clinical use include:

— Will the examination results be used for:

  — diagnosis in order to cure, treat or prevent a disease or other condition?

  — measuring body fluid constituents to determine a patient's state of health?

  — monitoring therapeutic drug levels to ensure an effective dose?

  — determining the *safety* of donated blood or organs?

  — screening a population for the presence or absence of a specific marker?

  — predicting the effectiveness of a therapeutic alternatives ("companion diagnostic")?

  — predicting the *risk* of developing a medical condition?

  — applications other than the *intended use*?

— What injury, illness or condition will the results be used to detect, diagnose, predict or monitor?

— Who will use the IVD examination results: medical specialists, general clinicians or patients?

— Is the role of the examination results in medical decisions to be used:

  — as the basis for immediate medical decisions?

— with other relevant information to guide a medical decision?

— Which patient populations will primarily experience the *benefit* from the IVD examinations?

— Should any patient populations be explicitly contraindicated?

H.2.2 Characteristics related to patient *safety*

H.2.2.1 General considerations

In addition to biological, chemical, electrical, mechanical and security characteristics in common with other *medical devices* (see Annex A), *IVD medical devices* have analytical performance and reliability characteristics that determine the suitability for their intended clinical use. Some *IVD medical devices* can perform multiple examinations simultaneously, and their clinical performance can rely on the interpretation of patterns of results (e.g. multiplex assays). *IVD medical devices* that employ digital information technology can also have characteristics related to their ability to store and transmit an examination result or ancillary information to where it is needed for a medical decision. Failure to meet a performance, reliability or communication requirement can initiate a sequence of events that might result in *harm* to a patient.

H.2.2.2 Performance characteristics related to patient *safety*

a) Quantitative examinations measure a quantity in a representative specimen taken from a patient. The results are usually expressed as a concentration or percentage. The required analytical performance depends on the medical application, but false high, false normal or false low results can potentially affect a diagnosis, cause inappropriate or delayed therapy, and lead to patient *harm*. The type and *severity* of *harm* can depend on the magnitude of error at medical decision points.

   The relevant performance characteristics of quantitative *IVD medical devices* can include:

   — trueness of the measured values (bias, traceability to a reference standard);

   — measurement precision (repeatability, intermediate precision, reproducibility);

   — analytical specificity (influence of interfering or cross-reacting substances);

   — analytical sensitivity (ability to discriminate between quantity limits or ranges);

   — detection limit (lowest quantity that can be reliably detected);

   — quantitation limit (lowest quantity that can be accurately measured);

   — measuring interval (range of values over which the analytical performance was validated).

b) Semi-quantitative examinations provide a clinically useful approximation of the quantity being measured. Values are typically assigned based on an ordinal scale or are reported as a quantity limit, and can be expressed numerically (e.g. within a specified range of values, or greater or less than a specific quantity, titer or serial dilution) or relatively (e.g. as +3, +2, +1 or trace amount). Common examples of semi-quantitative examinations are urine "dipsticks," tablets that detect the presence of ketones, and serological agglutination *procedures*.

   Microscopic examinations can also be considered semi-quantitative if the results are reported as the number of cells observed in a low-power or high-power field. For example, a urine microscopic examination might report a value of 0 to 5 red blood cells in a high-power field.

   The performance characteristics of semi-quantitative *IVD medical devices* can include:

   — analytical sensitivity (ability to discriminate between quantity limits or ranges);

   — analytical specificity (influence of interfering or cross-reacting substances)

   — detection limit (lowest quantity that can be reliably detected);

— precision of the measured signal values (repeatability, reproducibility).

c) Qualitative examinations determine the presence or absence of an analyte, and results are reported as positive, negative or indeterminate. Cut-off values and relevant databases can define positive or negative results. A positive result when the analyte is absent or a negative result when the analyte is present can affect the diagnosis or treatment.

The performance characteristics of qualitative *IVD medical devices* can include:

— analytical sensitivity (fraction of true positive results in samples containing the analyte);

— analytical specificity (fraction of true negative results in samples containing the analyte);

— diagnostic sensitivity (fraction of true positive results in patients with disease);

— diagnostic specificity (fraction of true negative results in patients without disease).

H.2.2.3 Reliability characteristics related to patient *safety*

When clinicians depend on IVD examination results for urgent medical decisions, such as in emergency or intensive care settings, timely results can be as important as accurate results. Failure to produce a result when it is needed can delay necessary medical intervention.

The reliability characteristics of *IVD medical devices* can include:

— system reliability (mean time between failures, mean time to failure);

— component compatibility (including versions and critical tolerances);

— software reliability (error-free operation);

— reagent or control stability;

— system usability (avoidance of *use errors*).

H.2.2.4 Digital information technology characteristics related to patient *safety*

Correct identification of the patient and the sample is clearly essential. Some examinations also require ancillary information about the patient, the sample, or the examination for proper interpretation of the results. If an *IVD medical device* is designed to collect, store and report such information with the examination result, device characteristics leading to data corruption or alteration can contribute to misdiagnosis or inappropriate therapy.

The ancillary patient information required by the clinicians can include:

— correct patient name and sample identification;

— patient details (age, gender, population, genetic factors, medications, nutritional state);

— sample details (sample type, description, acquisition time);

— measurement details (measurement *procedure*, units of measure, measurement uncertainty);

— application details (cut-off points, reference intervals).

Digital information technology characteristics that can affect patient *safety* include:

— connections between devices and/or networks (wireless or wired);

— internet data transmission;

— interface with digital applications (networked or mobile);

— applications that emulate results from an *IVD medical device*;

— embedded software applications (e.g. interpretation or treatment recommendations);

— unshielded data transfer (e.g. ESD susceptibility);

— digital data storage (e.g. susceptibility to corruption, manipulation or deletion);

— disruption of other connected devices (creating additional *hazards*).

H.2.3 Known and foreseeable *hazards* to patients

H.2.3.1 Identification of *hazards*

From the standpoint of the patient, an IVD examination result would be considered a *hazard* if it could lead to (1) inappropriate medical intervention that can result in *harm*, or (2) lack of medical intervention necessary to prevent being harmed. The following general *hazards* could cause or contribute to potentially harmful medical decisions. The specific *hazards* should be identified in terms of the magnitude and direction of error, the extent of delay, or the ancillary information that is incorrect or missing.

In addition to *hazard* identification for the *IVD medical device* itself, *hazard* identification related to connectivity should be evaluated. The increased use of *IVD medical devices* connected to other devices or systems, either directly or through a computer network, wireless technology or the internet, has created new challenges for their safe operation. The need to ensure effective *IVD medical device* functionality and *safety* has become more important with the increasing use of connected devices, and the frequent electronic exchange of health information produced by *IVD medical devices*. Identifying failures that can cause the *hazards* described below, due to connectivity, should be performed as part of the *risk management process* for the *IVD medical device*.

a) Incorrect examination result

For quantitative and semi-quantitative examinations, results are considered incorrect if the difference from a correct value exceeds the error limit required for the clinical application. Analytical performance requirements are typically established during the design input *process*.

Some medical decisions can be influenced by the magnitude of the examination result, so the clinical significance of an incorrect result can depend on the magnitude of the difference between the measured value and the true value.

For qualitative examination *procedures*, in which only a positive or negative result is provided, (e.g. HIV and pregnancy examinations), examination results are either correct, incorrect or indeterminate.

b) Delayed examination result

An examination result or its ancillary information is considered delayed if it is needed for a medical decision and the clinician does not receive it in time to support a critical therapeutic or intervention decision. Criteria can be established to define what constitutes a clinically significant delay for the medical application (e.g. urgent care situation).

c) Incorrect information accompanying the result

The consequences of an error in the ancillary information provided with an IVD examination result depends on how the information is used in clinical decision making, and whether the error could cause or contribute to *harm*.

H.2.3.2 Identification of *hazards* from fault conditions

IVD medical devices that fail during use can lead to one or more of the general *hazards* defined in H.2.3.1. Fault conditions potentially leading to *hazards* can include the following:

— within-batch or batch-to-batch inconsistency (e.g. reagents, calibrators, controls);

— non-traceable value assignment (e.g. calibrators, proficiency materials, assayed controls);

— reagent non-specificity (e.g. interfering factors, antibodies);

— sample or reagent carryover (e.g. pipetting instruments);

— measurement imprecision (e.g. system-level);

— unstable materials (e.g. during transportation, storage or use);

— system malfunctions (e.g. hardware, software, components, accessories);

— digital technology failures such as:

  — software/firmware vulnerability to intrusion (e.g. data modification or theft);

  — data transfers resulting in incorrect or missing results, inappropriate treatment recommendations, or delays from loss of function due to environmental conditions (e.g. electrostatic discharge, ESD);

  — connections disrupting the performance of the connected *medical device*, creating unsafe conditions for the patient;

  — digital applications incorrectly connected to another device or digital application;

  — corruption during data storage that causes incorrect information or delayed results; or

  — delays in availability of results or patient information due to loss of network connectivity.

When the *IVD medical device* is used with digital software applications, failures leading to a delay of results include:

— smart device operating system changes, resulting in application not being available and causing delay of treatment, or in unexpected behaviour causing incorrect recommendation for treatment;

— smart device data storage capacity or rate of transfer data limitations, resulting in delay of treatment or incorrect recommended treatment;

— time inconsistencies between application and smart devices, resulting in delay of treatment or incorrect results (specifically related to out-of-date results appearing as valid).

H.2.3.3 Identification of *hazards* from normal use

Inherent limitations in *IVD medical device* technology can occasionally lead to one or more of the general *hazards* to patients described in H.2.3.1, even though all warnings, precautions and instructions for use were followed, the device functioned as intended, and the analytical performance met the claims of the *manufacturer*. Every examination result is subject to unavoidable sources of variability. Even when the analytical performance has been optimized to minimize the *risks*, an occasional result in normal use can be a *hazard* for an individual patient.

Hazards potentially occurring in normal use can include inaccurate results due to the following:

— inherent false negative and false positive rates of qualitative examination *procedures* caused by the uncertainty of statistically assigned cut-off values;