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.

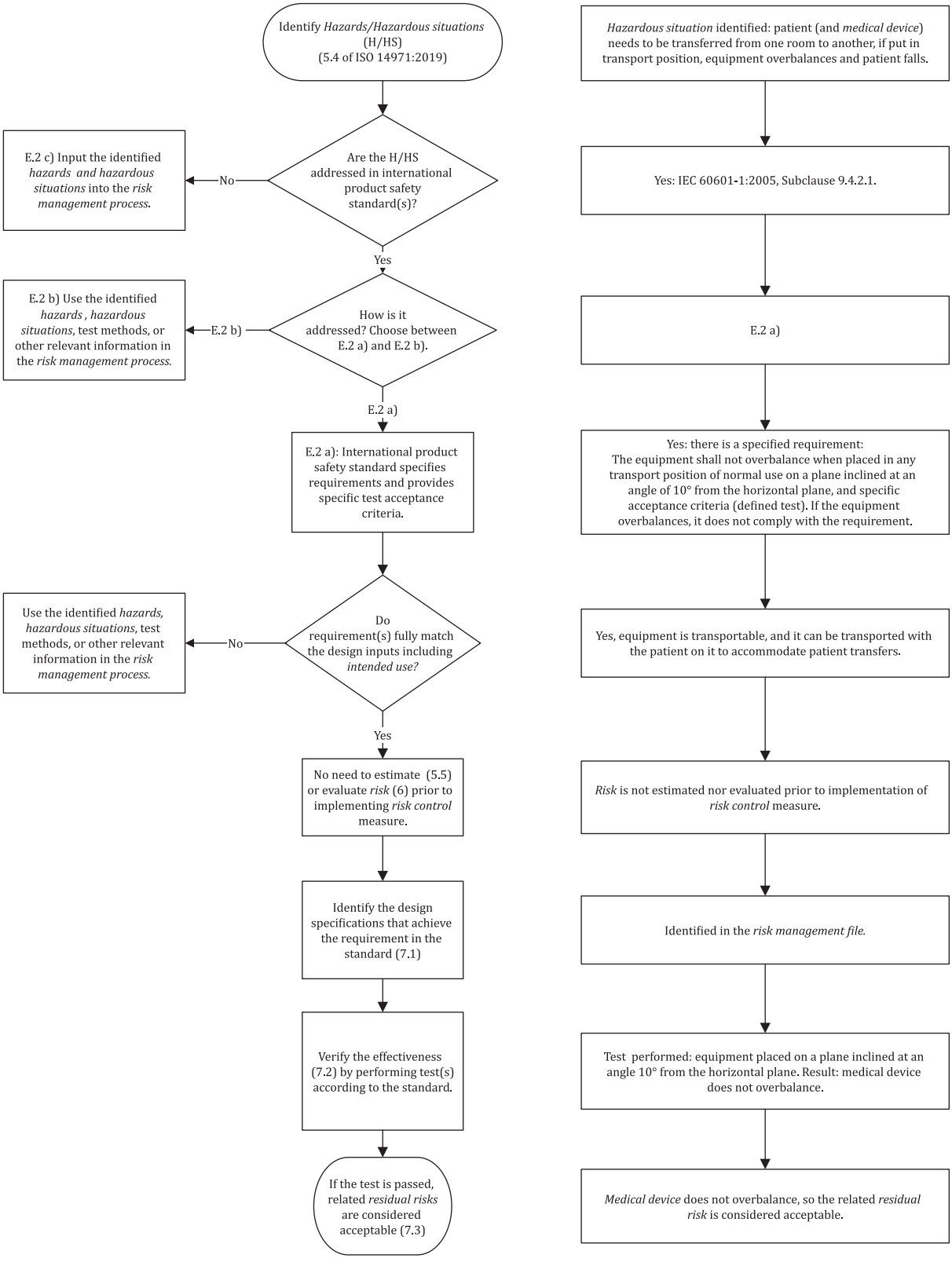

Figure E.1 — Use of international product *safety* standards and example of such standard that specifies requirements and provides specific test acceptance criteria

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.

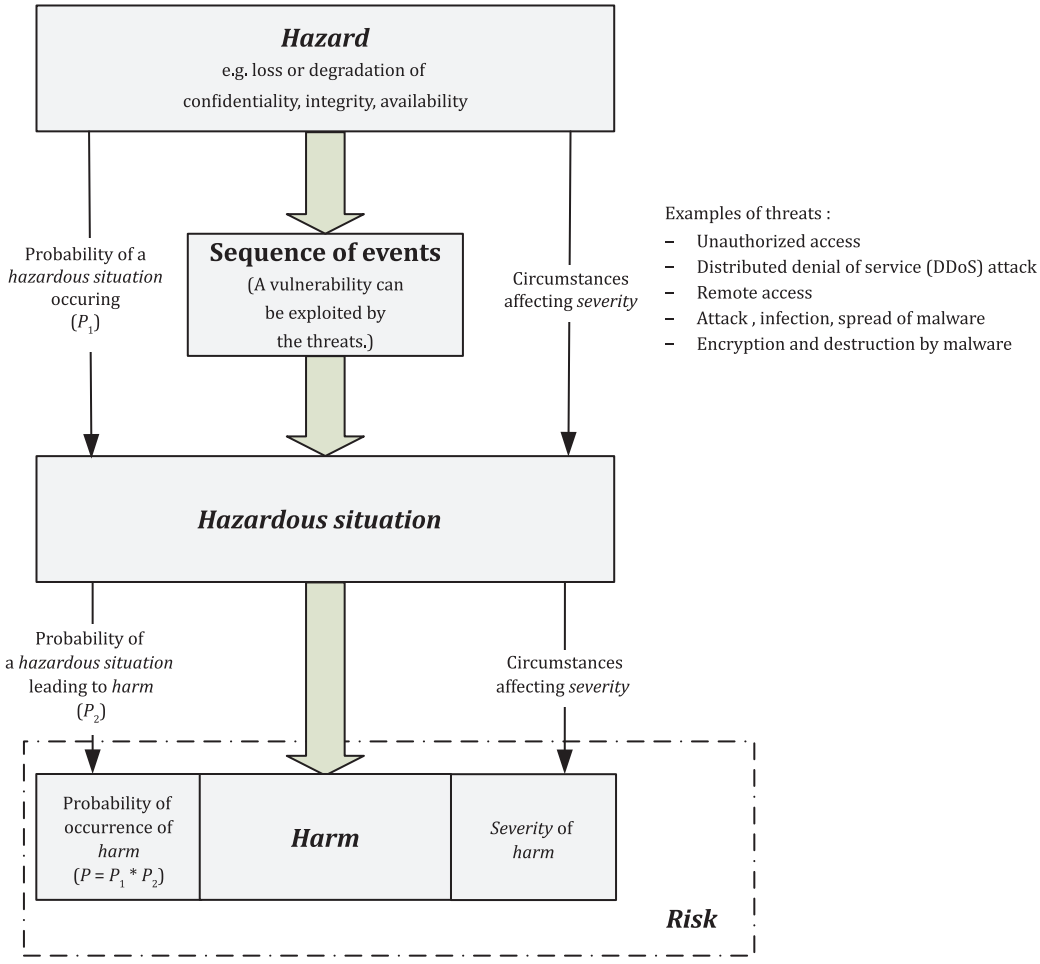

Figure F.1 — Relation between *hazard*, *hazardous situation*, *harm* and security terminology

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.

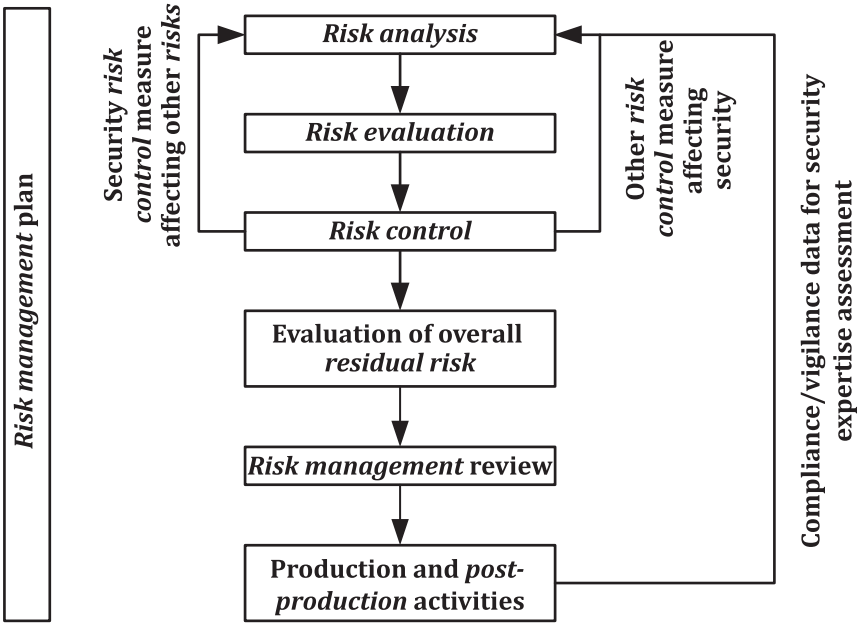

Figure F.2 — Possible interaction of security *risk control* measures with other *risk control* measures

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;

— measurement uncertainty associated with quantitative examination *procedures* (performance claims often represent 95 % of the results within medically defined target limits);

— misclassification of results as “abnormal” or outside a “normal” reference interval (determined empirically from the central 95 % of results in a “normal” population study);

— influence of interfering substances in the sample (e.g. cross-reacting antibodies, certain drugs or biochemical metabolites, or sample preparation materials);

— biological variability of the analyte itself (e.g. heterogeneity of natural proteins, population differences in normal analyte concentrations);

— chemical properties of the analyte itself (e.g. intrinsic instability, adhesiveness);

— variability of the patient sample matrix (i.e. “matrix effects”);

— the finite reliability of instrument components.

NOTE Medically defined performance requirements take into account the statistical distribution of examination results in the intended patient populations. The occurrence of a *hazardous situation* in normal use is considered an unavoidable contribution to the *residual risk*.

H.2.3.4 Identification of *hazards* from *use errors*

Use errors can cause one or more of the general *hazards* described in H.2.3.1. Non-routine laboratory *processes* can be especially prone to *use error*. Reasonably foreseeable *use errors* (i.e. resulting from readily predictable human behaviour) can be identified and potentially prevented by a usability engineering *process* during *IVD medical device* design and development. See IEC 62366-1[16] for information and guidance.

Use errors potentially leading to IVD *hazards* in the medical laboratory or at the point of care can include the following:

— overlooking special requirements (e.g. outside the normal laboratory routine);

— performing operations out of sequence, including pre-examination and post-examination *processes* (e.g. unclear instructions, confusing user interface);

— data entry errors (e.g. patient name, identification number, birth date or age, gender, etc.).

Use errors by patients performing self-testing can include the following:

— applying insufficient volume of sample (e.g. too little for accurate measurement);

— inserting reagent module improperly (e.g. before device is ready for measuring).

H.2.3.5 Identification of *hazards* from *reasonably foreseeable misuse*

A usability engineering *process* can also help *manufacturers* of *IVD medical devices* to prevent *hazards* and *hazardous situations* arising from *reasonably foreseeable misuse*. See IEC 62366-1[16] for guidance.

Examples of *reasonably foreseeable misuse* include the following:

— use of an *IVD medical device* prior to reading the instruction manual or completing training;

— disregard of warnings, instructions, or other information for *safety*;

— collection of an inappropriate sample type (e.g. serum when citrated plasma is specified);

— reporting examination results for contraindicated or unvalidated clinical use;

— using a self-testing *IVD medical device* in a critical care setting (e.g. accuracy might not be adequate);

— using unverified third-party calibrator, reagent, control material or accessory;

— storing materials in incorrect conditions (e.g. room temperature when refrigeration is specified);

— operation of an IVD instrument outside specified environmental conditions;

— disabling, overriding, or failing to enable *safety* features (e.g. to reduce annoyance to users);

— neglecting to perform prescribed instrument maintenance;

— connection to an information system without adequate network connectivity or security;

— malicious intent to create incorrect results or delay in treatment, including:

  — hijacked and impersonated device by third-party application or individual to alter results, producing incorrect results on connected digital applications;

  — corrupted device software configuration, producing incorrect results;

  — intercepted data in transit to delay results or send incorrect results to the user.

Reasonably foreseeable misuse by patients performing self-testing can include the following:

— dividing or reusing reagent test strips (e.g. to reduce cost);

— taking samples from an alternative site (e.g. other than fingertip due to pain);

— failing to clean and disinfect the venipuncture site (e.g. potential for contamination/infection);

— storing reagent strips in inappropriate environmental condition (e.g. overheated vehicle).

H.2.4 Identification of potential *harms*

ISO 14971:2019 requires *manufacturers* to estimate the *risks* associated with each identified *hazardous situation*, based on the probability of occurrence and the *severity* of possible *harm*. This requires the *manufacturer* to identify the potential *harms* (e.g. injuries) to patients with sufficient specificity to assign appropriate *severity* values.

For some examinations, a single *hazardous situation* can result in several different *harms* representing a range of *severities*. *Manufacturers* should determine which *harms* to include in the *risk analysis* to ensure a high degree of protection of health and *safety*, and document the rationale. All *harms* judged reasonably likely to occur should be included. Other *harms* can be added to the *risk analysis* if production or *post-production* information shows they were experienced.

NOTE Identifying potential *harms* for *risk analysis* and determining their *severity* and probability of occurrence requires an understanding of the clinical use of the IVD examination results. For this reason, participation of qualified medical experts in the *risk analysis* is essential.

Questions that might help to identify and classify potential *harms* include:

— Is the *intended use* a major determinant of therapy for a serious medical condition? If so, what *harms* might occur from a misdiagnosis or inappropriate therapy?

— Does the *intended use* involve detection of an infectious disease agent (e.g. hepatitis A or HIV)? If so, could a false negative result allow the infection to spread to others in the population?

— Is the *intended use* to detect and diagnose an inherited condition (e.g. sickle cell disease, hemoglobinopathy carrier, predisposition to Alzheimer's disease, increased *risk* of breast cancer, etc.)? If so, could a false negative result allow progression of an otherwise preventable or treatable disease? Could a false positive result lead to unnecessary medical intervention and potential *harm*?

— Is the *intended use* to predict drug or device effectiveness? If so, could a false negative result cause the loss of therapeutic *benefits* and subsequent *harm*? Could a false positive result have harmful consequences?

— Is the *intended use* to screen transfusion or transplant donors? If so, could incorrect results cause transmission of disease to recipients or lead to rejection of a properly functioning organ?

— Is the *intended use* to monitor a critical body function? If so, what *harms* might occur from an incorrect result or a significant delay in receiving the result?

— If medical intervention occurred, would the outcome be irreversible (e.g. surgical resection, abortion), or would the outcome be reversible (with or without further medical intervention)?

— Does the *IVD medical device* require connection to a network or the internet, where modification or theft of a patient's data could occur (e.g. inadequate security)?

Guidelines for determining the *severity* of *harm* are found in 5.5.4.

H.2.5 Identification of *hazardous situations*

ISO 14971:2019 requires *manufacturers* to compile a comprehensive set of *hazardous situations* for the *risk analysis*, but leaves it up to the *manufacturer* to determine what constitutes a *hazardous situation* for the purpose of the *risk analysis* (see Annex C.4 of ISO 14971:2019 for general guidance). One approach is to review the sequence of events. See H.2.6 to identify an event or condition that (1) exposes the patient to the *hazard*, (2) is beyond any reasonable means of control by the *manufacturer* or the device user, and (3) enables the *manufacturer* to perform an objective *risk analysis*.

Examples of *hazardous situations* for *IVD medical devices* can include events such as:

— receipt of an incorrect laboratory result by a clinician;

— delay in therapy (e.g. due to failure of the *IVD medical device*);

— delay in reporting an urgent laboratory result to a clinician;

— inappropriate therapy (e.g. based on incorrect self-testing result);

— misidentification of a patient's sample (e.g. due to *use error*);

— reporting incorrect information with a patient's result (e.g. due to networking failure).

The following questions can be helpful to analyse *hazardous situations* related to incorrect outcomes:

— Is the condition that is the subject of the IVD examination such that a false negative or false positive result would still appear "believable" given the likely context of other diagnostic indicators, and therefore not be further confirmed before deciding on a course of clinical action/inaction?

— Are there few, limited or no other diagnostic tools available to confirm or deny a potentially false positive or false negative IVD test result?

H.2.6 Identification of foreseeable sequences of events

H.2.6.1 General considerations

Identification and analysis of the reasonably foreseeable sequences or combinations of events that can lead to a *hazardous situation* and potentially progress to *harm* is necessary to estimate the probability that the *harm* would occur. Understanding these activities and events can also help the *manufacturer* select the *hazardous situation* for *risk analysis* and identify opportunities for *risk* reduction and *risk control*.

The specific sequence of events to be analysed will depend on the particular *IVD medical device* and its *intended use*. When outlining the sequence of events, the *manufacturer* should consider the knowledge,

skills and abilities of the intended users, the use environment, and any events and circumstances that could increase or decrease the *risks*.

Although medical laboratories operate with control *procedures* designed to detect errors, the *manufacturer* should consider their effectiveness in detecting specific failure modes. Sporadic random failures are especially difficult for a laboratory to detect. Experienced clinicians know this and question any results that are inconsistent with other available information or their clinical impression. If the incorrect result is plausible, however, and if it influences the diagnosis or therapeutic decision, it could lead to inappropriate or delayed therapy and potentially *harm* to the patient.

Malfunctions of *IVD medical devices* can create *hazardous situations* if they cause a significant delay in the availability of IVD results needed for critical medical decisions. Although the user bears the primary responsibility to have a backup and recovery plan, a device failure can be a contributory factor. Clinically significant delays are more likely to occur at the point of care or in laboratories that support emergency care than in a laboratory performing routine examinations.

H.2.6.2 Description of the sequence of events

Risk scenarios for *IVD medical devices* typically involve longer sequences of events than for other *medical devices*. They include activities that are not under the direct control of the *manufacturer*, such as those performed by the device users (e.g. the medical laboratory or point of care user) and medical decisions and actions by the clinicians who ordered the examination results.

The description should start with the initiating event (typically the cause of the *hazard* being analysed) and the events directly under the control of the *manufacturer*, progress logically through the foreseeable decisions and actions of the device users, and end with the clinical decisions and actions leading to each of the *harms* identified as foreseeable outcomes.

The description should be as detailed as necessary to capture the main initiating and contributing events, but not so detailed so that minor inconsequential events hinder the analysis. *Manufacturers* can choose to divide complex sequences of events into shorter segments, so that the analysis can be performed by individuals with the required expertise. This approach is discussed in H.2.7.2. A diagram (e.g. flowchart, event tree) can be useful to document and communicate complex sequences of events.

a) Events under control of the *manufacturer*

The initiating event in the sequence leading to a *hazardous situation* can occur as a failure of the *manufacturer's* quality management system. A fault condition or potential for *use error* can be caused by activities under a *manufacturer's* direct control, such as:

— design and development;

— device labelling;

— manufacturing and supplier management;

— product inventory and distribution;

— equipment servicing;

— training and product support.

b) Events under control of the user of the *IVD medical device*

Use errors and device failures can happen during device operation in the laboratory or at the point of care. Activities to prevent or detect *hazards* and the actions taken in response by the user are under the direct control of the laboratory or point of care facility. These device users incorporate the protective measures and information for *safety* provided by the *manufacturer* into their own *risk management process*.

The users of *IVD medical devices* can also cause or contribute to *risks* to patients through misuse (see H.2.3.5), including failure to maintain adequate quality assurance *procedures*, contingency

and recovery plans, or security protection. Decisions to report or not report an examination result to a clinician are completely under the control of the medical laboratory or other users of the *IVD medical device*. The capabilities of the intended users and the use environments should be considered when analysing the sequence of events under control of users of the *IVD medical device*.

Examples of activities typically under the user's control, using information, materials and support from the *IVD medical device manufacturer*, include:

— selection, usage and storage of sample collection device used with the *IVD medical device*;

— collection, processing and storage of patient samples;

— system installation and setup, including user training, component or consumable qualification, and performance *verification*;

— selection, preparation, usage and storage of accessories, consumables, and parts (including expiry date management);

— calibration activities and metrological traceability;

— quality assurance activities (e.g. quality control, proficiency testing, delta checks);

— review and reporting of examination results;

— communication with clinicians (*intended use*, contraindication, recalled results, surveillance);

— local network and internet connectivity;

— biohazardous waste disposal;

— equipment maintenance, servicing, decommissioning and disposal;

— contingency and recovery planning (e.g. backup systems).

c) Events under control of the clinician

The events under control of the clinician normally begin with receipt and review of the examination result and a decision whether to accept the result as valid. Large errors are likely to be questioned and rejected (e.g. results contradicted by other diagnostic information, abnormal results incompatible with life), but plausible results are likely to be accepted as valid and potentially used for medical decisions.

NOTE Clinical decision making is specifically excluded from the scope of ISO 14971:2019. This refers to clinical decisions whether to use a particular *medical device* or *IVD medical device*, not to clinical decisions affected by incorrect or delayed IVD results.

When *IVD medical devices* are used at the point of care, such as a physician's office, clinic or specialized hospital unit, clinicians are usually involved in the collection, handling, inventory, and storage of patient samples, and can perform many or all of the activities of the *IVD medical device* user. In such cases, the opportunities for the *manufacturer* to influence clinical activities through information for *safety* in the *accompanying documentation* can be greater. The sequence of events identified for *risk analysis* should reflect the use of the *IVD medical device* in the actual use environment.

The *risk analysis* should consider any reasonably foreseeable clinical use. Clinical use contraindicated or not explicitly addressed in the *accompanying documentation* could be considered *reasonably foreseeable misuse* for the purposes of *risk management*. It should be noted that *accompanying documentation* written for *IVD medical device* users in the laboratory does not always reach the clinicians who order and act upon the examination results.

Examples of decisions and activities typically under the clinician's control, potentially with guidance and support from the laboratory, include:

— comparing the result to expected values;

— requesting confirmatory or corroborating examinations;

— proceeding without the examination result (if delayed);

— establishing a clinical diagnosis;

— initiating or withholding therapy.

H.2.7 Estimation of the probability of occurrence of *harm*

H.2.7.1 General considerations

The *risk analysis* should consider the entire sequence of events as described in H.2.6.2. The probability of a patient being harmed is the combined probability of each event in the sequence of events associated with a particular *hazard* and the potential *harm*. The approach used to estimate the probability of occurrence of *harm* can depend on the complexity of the sequence of events. An important consideration is to ensure the analysis can be performed by individuals with the appropriate knowledge and expertise pertaining to the *IVD medical device* being analysed, including its analytical and clinical use and the technologies involved. The *manufacturer* can analyse the entire sequence of events as a whole or divide it into segments, based on which approach is more suitable for an objective *risk analysis*. Examples of applying different *risk analysis* approaches to common *IVD medical device* scenarios are given in H.7.

For *IVD medical devices* involving short sequences of events, such as self-testing or point of care devices, the *risk analysis* can be relatively straightforward. A cross-functional team of experts can be assembled to develop estimates of the probability of occurrence of *harm* for each identified *hazardous situation*, based on their expert judgment, supplemented with available analytical and clinical information (e.g. premarket studies, experience with similar products, relevant *post-production* information). The cross-functional team should include experts familiar with the design, construction, use and servicing of the device, the use environment (e.g. medical laboratory, point of care, patient's home), and the clinical use of the examination results. For software-containing devices designed to communicate with other devices and/or a network, the team should also include expertise in connectivity and security.

For complex sequences or combinations of events, segmenting the analysis at the *hazardous situation* can make more efficient use of expert resources by applying their specialized knowledge and expertise to the analysis of relevant sequences of events. This is called the "P_1 x P_2" approach, which is explained in more detail in the next subclause.

H.2.7.2 Particular guidance for using the "P_1 x P_2" approach

The approach illustrated in Figure C.1 of ISO 14971:2019 can be useful for complex *risk* scenarios with extended sequences of events. For example, events from an incorrect result can extend beyond the medical laboratory to the decisions and actions of a clinician, which are largely beyond any reasonable means of *risk control* by the laboratory or the *manufacturer*. The probability that a *hazardous situation* would occur (P_1) and the probability that *harm* would result from that *hazardous situation* (P_2) are estimated separately by appropriate experts. The probability P_1 is related to the analysis in the laboratory using the *IVD medical device* and producing the result and the probability P_2 is related to the use of the result by the clinician and the decisions and actions based on that result. These probabilities are combined to obtain the overall probability of occurrence of *harm* ($P = P_1 \times P_2$).

For an *IVD medical device* intended for medical laboratory use, the sequence of events can be divided into analytical and clinical segments, with the *hazardous situation* defined as an incorrect result reported to a clinician, a clinically significant delay in reporting the result, or failure to report an important examination result. The probability of each segment can be estimated separately as follows:

— P_1 is the probability that the *hazardous situation* would occur; and

— P_2 is the probability that a specific *harm* would result from that *hazardous situation*.

Figure H.1 illustrates one way to apply the "P_1 x P_2" approach to a typical *risk* scenario involving an *IVD medical device*, in this case a blood analyser performing glucose measurements in a medical laboratory. The figure depicts the entire sequence of events, starting with the failure of the *manufacturer's* calibrator value assignment *process* and ending with the possibility of multiple patient *harms*.

The *hazard* in this example is an incorrect (falsely high) glucose measurement result caused by inaccurate calibrator values assigned by the *manufacturer*. The first two events in this scenario are under the control of the *manufacturer*. The subsequent events leading to a *hazardous situation* occur in the laboratory beyond the *manufacturer's* direct control, but these are potentially controlled by information for *safety* provided by the *manufacturer* in the *accompanying documentation*. The remaining events occur beyond the direct control of the laboratory, so the *hazardous situation* in this scenario (i.e. exposure to the *hazard*) can be defined as the event beyond any reasonable means of *risk control* by the *manufacturer*. For an efficient *risk analysis* in such cases involving incorrect IVD results, the *hazardous situation* can be defined as the event when the laboratory reports and/or the clinician receives the incorrect result.

In this *risk analysis*, the probability of the *hazardous situation* occurring (P_1) and the probability of the *hazardous situation* leading to *harm* (P_2) can be estimated separately by the appropriate subject matter experts. The two probabilities can then be combined to give an estimate of the overall probability of *harm*.

P_1: Probability of occurrence of the *hazardous situation*

The individuals assigned to estimate the probability P_1 should be familiar with the design, construction, use and servicing of the *IVD medical device*, as well as have an adequate understanding of the use environment (e.g. medical laboratory, point of care, patient's home). Expert knowledge of the medical applications is generally not needed to analyse the P_1 events.

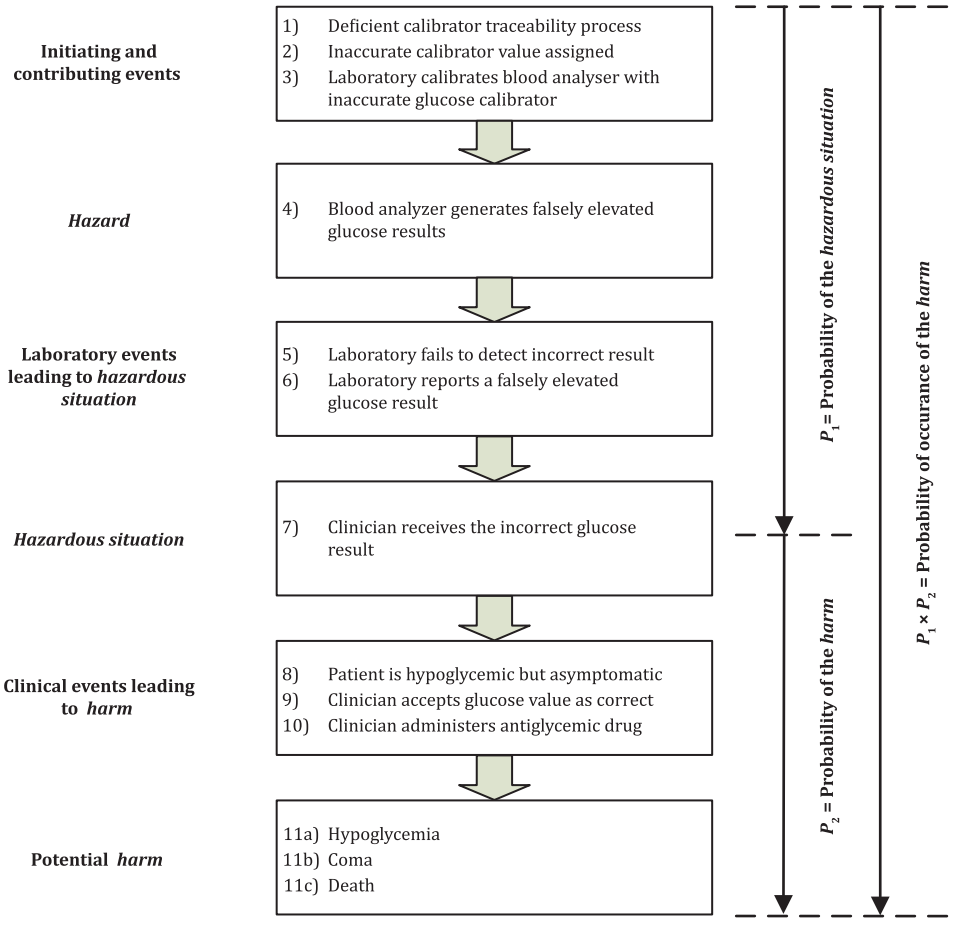

Figure H.1 — Illustration of the sequence of events for a laboratory scenario involving an incorrect glucose measurement from an *IVD medical device*

P_2: Probability of *harm* occurring from a *hazardous situation*

The individuals assigned to estimate P_2 should be familiar with the medical use of the IVD results. Probability P_2 can be estimated using expert clinical judgment and experience with similar IVD examinations, informed by adverse event data, medical literature and information from *post-production*. Detailed understanding of the performance of the *IVD medical device* or how the results were generated and reported is generally not needed to estimate P_2.

H.2.7.3 Guidance for estimating the probability of occurrence of *harm*

The questions in Table H.1 are intended to stimulate systematic analysis of the sequence of events and guide the development of suitable probability estimates. The questions should be adapted as appropriate for the type of *IVD medical device*, the specific *intended use* and the *risk estimation* approach used.

Questions 1 to 4 pertain to the analytical segment of the sequence of events, and can help a *manufacturer* estimate P_1. Questions 5 to 8 pertain to the clinical segment of the sequence of events, and can help a *manufacturer* estimate P_2.

Table H.1 — Questions to help estimate the probability of occurrence of *harm*

What is the likelihood that …	Points to consider
1. … the initiating event would occur (i.e. a device failure or *use error*)?	— How effective are prevention/detection measures? — Can probability be estimated? If not, set probability = 100% — Would frequency depend on use environment? Address worst case. — Can specific faults, failure modes and/or *use errors* occur in a reasonably foreseeable combination to cause a *hazard*?
2. … an incorrect result would be generated by the *IVD medical device* failure or *use error*?	— How effective are measures intended to ensure accurate results? Or detect an unacceptable change in analytical performance? — Would conventional quality control *procedures* cause the incorrect examination results to be rejected? — What is the influence of the use environment (e.g. medical laboratory, point of care, patient's home)? Analyse different use environments separately. — Would the device prompt a user to correct problem (e.g. "not enough blood") in time to obtain a valid examination result upon repeat?
3. … the incorrect result or incorrect ancillary information would be reported to the clinician?	— Are abnormal results for the examination reviewed against critical value limits, or otherwise verified prior to reporting to the clinician? — Are rare or unexpected results automatically confirmed prior to reporting (e.g. new-born screening programs)?
4. … a clinically significant delay in reporting the examination result (or ancillary patient information) would occur?	— Is the result critical for a timely diagnosis or therapeutic decision? — How much of a delay would create a *hazardous situation*? — Would the time necessary to troubleshoot a malfunction or out of control situation cause a clinically unacceptable delay? — Would a backup *procedure* to ensure timely availability of results be an expectation of standard laboratory/medical practice? — Could a second examination be performed and the result be reported within the time required for a critical result?

Table H.1 *(continued)*

What is the likelihood that ...	Points to consider
5. ... the clinician will believe the incorrect result to be valid?	— Would a clinician recognize the result as incorrect for reasons such as inconsistency with a patient's clinical status, contradicted by other clinical data, or being physiologically implausible? — Would a competent clinician question, repeat or corroborate a result that did not fit the clinical impression? — Do current standards of medical practice require confirmation (e.g. two independent HbA1c measurements for a diagnosis of Diabetes Mellitus Type 2)?
6. ... an incorrect medical decision and/or intervention (or lack of intervention) will occur due to the incorrect result?	— Are the results used for diagnosis, therapy or monitoring? — Will the result be the primary basis for a particular medical decision? Or only used in the context of signs, symptoms, other examination results and the patient's medical history? — Do positive or "abnormal" results always lead to a particular medical decision or treatment, or only to further investigation? — Would a false negative or false "normal" screening result cause the clinician to miss a treatable medical condition?
7. ... an inappropriate medical decision or action will be caused by failure to receive a timely IVD result?	— To what degree is the result used to guide the intervention or therapy, given the signs, symptoms, medical history and other examination results that would be available to the clinician?
8. ... patient *harm* will be caused by the inappropriate medical decision or action?	— How urgent is an immediate decision or intervention for the patient? — What are the medical consequences of the inappropriate action or delay in taking necessary action? — To what extent would the condition of the patient increase the probability of occurrence of *harm*? — Are there implications for individuals other than the patient, such as: — potential for transmission of infectious agents to others? — exposure of an embryo or foetus to teratogenic agents or radiation? — antimicrobial resistance due to unnecessary exposure? — false rejection of an organ for transplant? — need for family counselling due to a false diagnosis? — parental anxiety from false positive new-born screening result?

H.3 *Risk control*

H.3.1 General

Since the decisions and actions of the clinicians are largely beyond any reasonable means of *risk control* by the *manufacturer*, *risk control* activities should focus on reducing the probability of events under the control of the *manufacturer*. This includes providing information for *safety* and verifying the effectiveness of information for *safety* to users in the laboratory. If the *manufacturer* uses the P_1 x P_2 approach, this means that *risk control* measures are directed at reducing probability P_1.

H.3.2 Inherently safe design and manufacture

Risks to patients are generally reduced by lowering the probability that incorrect results will be reported or that clinically significant delays will occur (e.g. by ensuring that performance characteristics meet medical requirements). For quantitative measurements of analytes such as blood glucose, electrolytes, enzymes and therapeutic drugs, limiting the magnitude of errors can reduce the frequency of inappropriate medical decisions.

Examples of design features that control the accuracy and reliability of the examination results include the following:

— trueness of the calibrator values (e.g. traceability to a recognized reference standard);

— measurement uncertainty (e.g. precision of the measuring system);

— analytical specificity of IVD reagents (e.g. optimized components);

— detection limit or quantitation limit (e.g. improved measurement technology);

— reliability of the instrument (e.g. minimize hardware or software failures);

— discrimination between positive and negative samples (e.g. robust cut-off value);

— eliminating mistake-prone procedural steps (e.g. automation, mistake-proofing);

— component version traceability and positive sample identification (e.g. bar-coding);

— software functionality (e.g. *state of the art* coding standards);

— system ease of use (e.g. usability engineering);

— data network and internet connections (e.g. security);

— reduced reagent or calibrator variability (e.g. lot-to-lot specifications, supplier requirements);

— prevention of spurious results (e.g. intermittent component failures);

— stability of reagents, calibrators or control materials (e.g. microbiological control).

H.3.3 Protective measures in the *IVD medical device* or manufacturing *process*

Examples of detection features in the *IVD medical device* or reagent kit intended to prevent conditions that can cause incorrect or delayed results include:

— liquid level sensors to ensure sufficient sample volume (e.g. detect “short draws”);

— fault detection systems (e.g. spectrophotometer drift, inadequate temperature control);

— sample quality checks (e.g. hemolysis, icterus, lipemia);

— controls to detect and remove sample artefacts (e.g. foam or fibrin clots);

— built-in controls to verify correct calibrator or reagent lots (e.g. bar code readers);

— alarms and error messages to alert users to fault conditions and recovery *procedures*;

— software that identifies questionable results for reflex testing, review or suppression;

— incoming inspections of supplied components;

— in-*process* acceptance testing and final-product acceptance testing.

NOTE Recommendations for detection methods to be implemented by the user, such as quality control testing, confirmatory examinations or critical value notifications, are considered information for *safety*, not protective measures.

H.3.4 Information for *safety*

Information for *safety* is provided to users of *IVD medical devices* to prevent the occurrence of a *hazard* or a *hazardous situation*. This can be an effective *risk control* measure if (1) such information instructs users what actions to take or avoid, (2) the intended users are capable of following the instructions, and (3) it can be reasonably expected that they will follow those instructions. The adverse consequences of ignoring the information for *safety* should be clear.

The information for *safety* can be used in the *risk management process* of the medical laboratory or by other intended users. Examples of information for *safety* that enable users to control *risks* include warnings, instructions and other information addressing:

— chemical or biological *hazards* associated with the *IVD medical device*;

— contraindicated medical conditions or clinical applications;

— sample collection, storage and preparation;

— identification of inappropriate sample types;

— interfering substances detectable by the user (e.g. visible haemolysis);

— causes of *hazards*, including potential *use errors*;

— incompatible system components and accessories;

— utilities and facilities where the *IVD medical device* is to be installed (e.g. use environment);

— improper reagent storage or use beyond the expiry date;

— installation, servicing and disposal of the *IVD medical device*;

— quality control samples and frequency;

— validated measuring intervals and dilution instructions for samples when the measured values are above the upper limit of the measuring interval;

— biological reference intervals and medical decision points;

— validated cleaning methods for reusable items;

— preventive maintenance *procedures*;

— interface and connectivity requirements;

— backup and recovery in case of system failure.

NOTE The information for *safety* can be subject to regulations or international standards, such as ISO 18113 (all parts)[34].

H.3.5 Role of standards and analytical performance criteria

Few international product standards define the generally acknowledged *state of the art* for *IVD medical devices*. ISO 15197[28] (self-monitoring devices for blood glucose) and ISO 17593[32] (self-monitoring devices for oral anticoagulant therapy) are examples. However, some international standards for *IVD medical devices* address certain aspects of inherent *safety*, which can provide evidence that the *risks* from specific *hazardous situations* have been reduced to the *state of the art*.

For example, ISO 17511[31] defines a *process* for establishing the metrological traceability of IVD calibrator values to higher order reference materials that define the *state of the art* for accuracy of patients' results. The Joint Committee for Traceability in Laboratory Medicine (JCTLM) maintains the IVD Reference Measurement Systems Database online at http://www.bipm.org/jctlm/. Conformance to ISO 17511[31] using a JCTLM-approved reference measurement system can provide evidence that the *manufacturer* has reduced the *risks* associated with the accuracy of its examination results to the generally acknowledged *state of the art*.

Other examples of IVD standards with potential relevance to *risk control* include ISO 17822-1[33] (nucleic acid-based detection systems), ISO 20776[36] (antimicrobial susceptibility), ISO 20916[37] (clinical performance studies), ISO 23640[40] (stability of IVD reagents), IEC 61010-2-101[11] (*safety* of IVD equipment), IEC 61326-2-6[13] (electromagnetic compatibility of IVD equipment), and IEC 80001-1[19] (networked *medical devices*).

Widely recognized performance criteria for certain analytes can be found in publications of the World Health Organization (WHO), as well as publications of international and national public health agencies, standards organizations, professional medical societies and regulatory authorities.

The *manufacturer* is responsible for justifying the extent that such standards and performance criteria apply to their particular *IVD medical device* and its *intended use*, and as required by ISO 14971:2019, for verifying that all relevant *hazardous situations* have been considered.

H.3.6 User education and training

For complex user interfaces, difficult examination *procedures*, or critical clinical applications, information for *safety* can take the form of training and education programs offered by the *manufacturer* to help avoid *use errors*. Training materials suitable for use in continuing education programs can also be provided.

For example, the product standard for oral anticoagulation monitoring systems (ISO 17593[32]) requires the *manufacturer* to provide a validated training program for clinicians and an education program for patients and other users of these devices. The experts who developed the International Standard considered these *risk control* measures necessary to ensure the *risks* of use in the home environment were acceptable.

In determining the degree of *risk* reduction attributable to information for *safety*, consider that:

— the use environment, competence and capabilities of device users can vary widely;

— quality control and quality assurance practices are not uniform around the world; and

— information about contraindicated medical use and interfering drugs provided to *IVD medical device* users might not always reach the clinicians who order the examinations.

H.4 *Benefit-risk* analysis

Guidance on performing a *benefit-risk* analysis is provided in 7.4.

If it is not possible to describe the *benefits* of an *IVD medical device* directly, surrogate endpoints can be established. Examples include the ability of an *IVD medical device* to identify a specific disease, to provide diagnosis at different stages of a disease, to predict future disease onset, and/or to identify patients likely to respond to a given therapy.

H.5 Disclosure of the *residual risks*

H.5.1 General considerations

Annex D explains that the aim of disclosing the *residual risks* is to provide information to the device user, and potentially the clinician and the patient, so they can weigh the *risks* of using the *IVD medical*

device against its *benefits* and make informed decisions about the *risk* acceptability. *Manufacturers* should take into account the information needed by medical laboratories and clinicians to evaluate the inherent *residual risks* and determine the need for further *risk* reduction measures.

Disclosure of *residual risks* for *IVD medical devices* can take different forms, including information provided in the *accompanying documentation* about the performance specifications ("claims"), limitations of the *IVD medical device* or examination *procedure*, and/or potential causes of *hazards* and *hazardous situations* that could not be eliminated by the *manufacturer*. The disclosure of *residual risks* is in addition to the *risk control* measures provided to users as information for *safety*.

NOTE The disclosure of *residual risks* in the *accompanying documentation* can also be prescribed by national regulations or international standards, such as ISO 18113 (all parts)[34].

H.5.2 Performance specifications

Description of the relevant analytical performance characteristics and the results of clinical performance studies (see ISO 20916[37]), allow the medical laboratory director and clinicians to evaluate the utility of the *IVD medical device* for its intended medical applications.

The description of the performance characteristics should be sufficiently detailed so the laboratory or other users can:

— verify that the *IVD medical device* is performing as intended by the *manufacturer*;

— determine the measurement uncertainty associated with the examination results; and

— know that the examination results will meet the medical needs of the clinicians.

Results of performance evaluations conducted in actual or simulated use conditions can be summarized and presented in the *accompanying documentation*.

Examples of potentially relevant performance characteristics are given in H.2.2.2.

H.5.3 Limitations of the *IVD medical device*

ISO 18113-1[34] requires that the analytical and clinical limitations of the *IVD medical device* be disclosed in the *accompanying documentation*. The limitations describe situations in which the *IVD medical device* might not perform as intended and can therefore be a means of disclosing *residual risks*, such as:

— interfering substances not detectable by the user (e.g. drugs, biological metabolites);

— specific patient populations in which the performance characteristics might not apply;

— values outside the measuring interval (where performance characteristics are not validated);

— patient populations where reference intervals or medical decision points might not apply;

— primary sample types that have not been validated for the *intended use*;

— circumstances and factors that might affect examination results, but have not been studied.

H.5.4 Generally recognized limitations of use

Some events or circumstances that can lead to a *hazardous situation* are considered general knowledge in laboratory medicine. These *risks* are addressed by standard medical or laboratory practices and are typically not described in the instructions for use to avoid overwhelming users with unnecessary details. The *manufacturer* should consider whether additional information is appropriate to ensure that users are aware of the *risks* associated with these events or circumstances, keeping in mind the

hazard of communicating so many *risks* that users might have difficulty understanding which ones are important to control. For example:

— Implicit in warnings, instructions and other information for *safety* is the understanding that failure to follow them can result in *hazards* and *hazardous situations*. It is not expected that *manufacturers* will specifically call out all such violations as *residual risks*. Failure to follow an explicit warning or instruction is considered misuse (see H.2.3.5).

— It is expected that electromechanical equipment will occasionally fail and require servicing, and that biological materials used beyond their expiry date can become unstable and fail.

— It is also expected that laboratories will implement a contingency plan (e.g. backup systems or an alternative laboratory) to ensure that essential services are available during such situations (see ISO 15189[27]).

H.6 Production and *post-production* activities

H.6.1 General considerations

Establishing an effective system to monitor *post-production* information (complaints, adverse events and product nonconformities) can be a challenge for *manufacturers*, particularly for devices intended for use in medical laboratories, because reliable data to monitor the actual frequency of *hazardous situations* and *harms* can be difficult to obtain. Monitoring the occurrence of *hazards* and their causes is more straightforward, since this feedback can be provided directly by the device users who experience the events. Reports of device failures, *use errors* and medical incidents should be collected and analysed, and the observed frequencies should be compared to the anticipated frequencies (allowing for the possibility of underreporting by busy laboratories).

When establishing a system for collecting *post-production* information, *manufacturers* can use the product *risk analysis* to develop a classification and coding scheme for anticipated *harms*, *hazardous situations*, *hazards*, and their causes, which can facilitate *risk*-based prioritization of investigations. Events can be classified according to the estimated *severity* of the potential *harms*, as well as the probability that incorrect or delayed results would lead to *harm*. Such a tool can be useful for complaint handling, post-market surveillance and adverse event reporting as well as product failure investigations.

H.6.2 Monitoring analytical performance

An effective system to collect production and *post-production* information for *IVD medical devices* requires monitoring of analytical performance data available from both internal and external sources.

Internal sources of performance data can include production data routinely collected during product release testing, value assignment activities, stability monitoring *processes* and product failure investigations.

External sources of performance data can include data routinely obtained from voluntary participation in external quality control and proficiency testing programs, user performance evaluations, and instrument installation and servicing activities.

H.6.3 Monitoring clinical performance

Medical laboratories generally have no way to know that a reported result was incorrect and could have led to an inappropriate medical decision, intervention or injury unless they receive a complaint from the clinician. For this reason, the *severity* of any reported *harms* and their frequency should be carefully monitored as part of *post-production* activities.

In addition to monitoring customer feedback about clinical incidents, the *manufacturer* should investigate more sources to learn about new and emerging *hazards* or *hazardous situations* occurring with similar products. Such sources can include adverse event and recall databases maintained by

regulatory authorities, as well as reports from public safety institutes, national medical laboratory associations and the medical literature.

H.7 Examples of *risk* scenarios for *IVD medical devices*

H.7.1 General

The following generic examples illustrate different *risk analysis* approaches for *hazardous situations* created by common types of *IVD medical devices*. These examples are not intended to represent the only recommended approach, and might not be appropriate for all such devices or *intended use*. *IVD medical device manufacturers* have the responsibility to decide the appropriate *risk analysis* approach to use for their devices. The *risk management* plan should document the approach to be used throughout their *life cycle*, along with the rationale for selecting it.

H.7.2 Automated medical laboratory analyser: incorrect examination result

In this scenario, a patient is being diagnosed by a clinician who orders an IVD examination from the central medical laboratory. If the result generated by the *IVD medical device* is incorrect and is reported to the clinician, a sequence of events leading to *harm* could occur as follows:

a) initiating event occurs (e.g. a device fault or *use error*);

b) *IVD medical device* produces a clinically incorrect examination result (i.e. a *hazard*);

c) device user fails to detect the incorrect result (or its cause);

d) device user reports the incorrect result to the clinician (i.e. a *hazardous situation*);

e) clinician does not identify the result as incorrect;

f) incorrect result misleads clinician to a misdiagnosis;

g) clinician inappropriately intervenes/does not intervene; and

h) patient is injured by the clinician's intervention/non-intervention (i.e. experiences *harm*).

In the scenario outlined above, the sequence of events from an incorrect result *hazard* extends through the medical laboratory to a clinician, whose decisions and actions are largely beyond any reasonable means of *risk control* by the *manufacturer*. For the purposes of this *risk analysis*, the patient can be considered to be in a *hazardous situation* when an incorrect result is received by the clinician, because after that event the patient is exposed to the possibility of *harm* from any clinical decisions and actions based on the incorrect result.

This definition of the *hazardous situation* allows the *risk analysis* to be divided into the analytical and clinical segments, separated by the *hazardous situation*. Each segment can be analysed and documented separately by cross-functional teams of appropriate experts, which can focus on the events relevant to their expertise. The results of the two analyses can be combined to obtain the overall probability of *harm*.

This approach makes efficient use of the technical and medical specialists. It also allows the creation of clinical *risk analysis* reports for the *risk management file*, which can be used to support updates to the *risk analysis* in the event of design changes, as well as to determine the *severity* and the probability of occurrence of *harm* from any *hazardous situations* encountered during *post-production* monitoring.

H.7.3 Personal (self-testing) device: incorrect classification of glycaemic status

In this scenario, a patient diagnosed with Type 2 Diabetes Mellitus regularly monitors his or her blood glucose concentration and self-administers an antiglycaemic drug when the results indicate hyperglycaemia. Although the patient was actually hypoglycaemic, the *IVD medical device* incorrectly

gave an elevated result and the antiglycaemic drug caused the patient to become even further hypoglycaemic. A sequence of events leading to *harm* could occur as follows:

a) initiating event occurs (e.g. device fault or *use error*);

b) personal *IVD medical device* produces a clinically incorrect glucose result (i.e. a *hazard*);

c) patient does not identify the result as incorrect;

d) incorrect result misleads patient to inappropriate therapeutic decision (i.e. a *hazardous situation*);

e) patient administers antiglycaemic therapy; and

f) patient becomes significantly hypoglycaemic (i.e. experiences *harm*).

In the scenario outlined above, the sequence of events from an incorrectly elevated blood glucose measurement that caused incorrect classification of the patient's glycaemic status is largely limited to the events under the control of the *manufacturer* and decisions and actions by the patient based on information for *safety* provided by the *manufacturer*. For the purposes of this *risk analysis*, the patient can be considered to be in a *hazardous situation* when an event occurs that could lead directly to *harm* (e.g. self-administration of antiglycaemic drug).

In this case, there is no practical advantage to segmenting the sequence of events. The entire *risk analysis* can be performed efficiently by a single cross-functional team of the appropriate technical and medical specialists.

H.7.4 Portable *IVD medical device* for the point of care: critical result delayed

In this scenario, a patient suspected of internal injuries is being treated in an urgent care facility, which performs an IVD examination to assess potential organ damage. Although the user followed the instructions for use, the *IVD medical device* displayed an error message and the examination result was not available when the clinician needed to decide whether or not to undertake an emergency *procedure*. A sequence of events leading to *harm* could occur as follows:

a) initiating event occurs (e.g. device fault or *use error*);

b) *IVD medical device* fails to produce a clinically necessary examination result (i.e. a *hazard*);

c) device user cannot repeat the examination within the required timeframe;

d) result is not available to the clinician to support intervention decision (i.e. a *hazardous situation*);

e) clinician takes critical decision / action without *benefit* of the examination result;

f) clinician's decision / action is not appropriate for the patient's condition); and

g) patient is injured by the clinician's action/inaction (i.e. experiences *harm*).

In the scenario outlined above, the sequence of events led the clinician to perform an emergency *procedure* without an assessment of internal organ damage. For the purposes of this *risk analysis*, the patient can be considered to be in a *hazardous situation* when the expected result was not received at the time it was needed, after which time the patient is exposed to clinical decisions and actions initiated without *benefit* of the examination result.

The *manufacturer* can consider whether to analyse the entire sequence of events as a whole or to divide it into segments based on which approach is more suitable for an objective *risk analysis*.

Bibliography

[1] AAMI TIR 57:2016, *Principles for medical device security — Risk management*

[2] GHTF/SG3/N18 2010, *Quality management system — Medical devices — Guidance on corrective action and preventive action and related QMS processes* (available from http://www.imdrf.org/documents/doc-ghtf-sg3.asp)

[3] GHTF/SG5/N4 2010, *Post-market clinical follow-up studies* (available from http://www.imdrf.org/documents/doc-ghtf-sg5.asp)

[4] IEC Guide 120:2018, *Security aspects — Guidelines for their inclusion in publications*

[5] IEC 60601-1, *Medical electrical equipment — Part 1: General requirements for basic safety and essential performance*

[6] IEC 60601-1-2, *Medical electrical equipment — Part 1-2: General requirements for basic safety and essential performance — Collateral Standard: Electromagnetic disturbances — Requirements and tests*

[7] IEC 60601-1-8, *Medical electrical equipment — Part 1-8: General requirements for basic safety and essential performance — Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems*

[8] IEC 60601-2-16, *Medical electrical equipment — Part 2-16: Particular requirements for basic safety and essential performance of haemodialysis, haemodiafiltration and haemofiltration equipment*

[9] IEC TR 60601-4-1, *Medical electrical equipment — Part 4-1: Guidance and interpretation — Medical electrical equipment and medical electrical systems employing a degree of autonomy*

[10] IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

[11] IEC 61010-2-101:2015, *Safety requirements for electrical equipment for measurement, control and laboratory use — Part 2-101: Particular requirements for in vitro diagnostic (IVD) medical equipment*

[12] IEC 61025, *Fault tree analysis (FTA)*

[13] IEC 61326-2-6, *Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 2-6: Particular requirements — In vitro diagnostic (IVD) medical equipment*

[14] IEC 61882, *Hazard and operability studies (HAZOP studies) — Application guide*

[15] IEC 62304:2006 and AMD1:2015, *Medical device software — Software life cycle processes— Amendment 1*

[16] IEC 62366-1:2015, *Medical devices — Part 1: Application of usability engineering to medical devices*

[17] IEC TR 62366-2, *Medical devices — Part 2: Guidance on the application of usability engineering to medical devices*

[18] IEC 62502, *Analysis techniques for dependability — Event tree analysis (ETA)*

[19] IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities*

[20] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[21] ISO/DIS 10017, *Quality management—Guidance on statistical techniques for ISO 9001:2015*

[22] ISO 10993-1:2018, *Biological evaluation of medical devices — Part 1: Evaluation and testing within a risk management process*

[23] ISO 11608-1, *Needle-based injection systems for medical use — Requirements and test methods — Part 1: Needle-based injection systems*

[24] ISO 13485:2016, *Medical devices — Quality management systems — Requirements for regulatory purposes*

[25] ISO Handbook: ISO 13485:2016, *Medical devices – A practical guide*

[26] ISO 14155, *Clinical investigation of medical devices for human subjects — Good clinical practice*

[27] ISO 15189, *Medical laboratories — Requirements for quality and competence*

[28] ISO 15197, *In vitro diagnostic test systems — Requirements for blood-glucose monitoring systems for self-testing in managing diabetes mellitus*

[29] ISO 16142-1, *Medical devices — Recognized essential principles of safety and performance of medical devices — Part 1: General essential principles and additional specific essential principles for all non-IVD medical devices and guidance on the selection of standards*

[30] ISO 16142-2, *Medical devices — Recognized essential principles of safety and performance of medical devices — Part 2: General essential principles and additional specific essential principles for all IVD medical devices and guidance on the selection of standards*

[31] ISO 17511, *In vitro diagnostic medical devices — Measurement of quantities in biological samples — Metrological traceability of values assigned to calibrators and control materials*

[32] ISO 17593, *Clinical laboratory testing and in vitro medical devices — Requirements for in vitro monitoring systems for self-testing of oral anticoagulant therapy*

[33] ISO/TS 17822-1, *In vitro diagnostic test systems — Qualitative nucleic acid-based in vitro examination procedures for detection and identification of microbial pathogens — Part 1: General requirements, terms and definitions*

[34] ISO 18113 (all parts), *In vitro diagnostic medical devices — Information supplied by the manufacturer (labelling)*

[35] ISO/TR 20416, *Medical devices — Post-market surveillance for manufacturers*

[36] ISO 20776 (series), *Clinical laboratory testing and in vitro diagnostic test systems — Susceptibility testing of infectious agents and evaluation of performance of antimicrobial susceptibility test devices*

[37] ISO 20916, *In vitro diagnostic medical devices — Clinical performance studies using specimens from human subjects — Good study practice*

[38] ISO 22367, *Medical laboratories — Application of risk management to medical laboratories*

[39] ISO 22442 (series), *Medical devices utilizing animal tissues and their derivatives*

[40] ISO 23640, *In vitro diagnostic medical devices — Evaluation of stability of in vitro diagnostic reagents*

ICS 11.040.01

Price based on 87 pages