CHAPTER 4

The Basics

Abstract

As in any other discipline, risk management also has its own jargon, or special vocabulary. It is imperative that you learn this vocabulary and use it correctly and consistently. Without this common language, it is not possible to reliably convey meaning. This increases the probability of miscommunication, confusion, and the potential for errors.

Keywords: Vocabulary; jargon; hazard; safety; risk; hazard theory; integral system; distributed system

4.1 VOCABULARY OF RISK MANAGEMENT

As in any other discipline, risk management also has its own jargon, or special vocabulary. It is imperative that you learn this vocabulary and use it correctly and consistently. Just as important, you should teach this vocabulary to others who participate in producing risk management work products. Without this common language, it is not possible to reliably convey meaning.

Note that this vocabulary is not colloquial English. For instance, to a normal English-speaker the words: hazard, risk, or danger may sound synonymous. But in the jargon of risk management specific meanings are assigned to words.

Sloppy usage of the jargon increases the probability of miscommunication, confusion, and the potential for errors. Table 1 lists some of the most commonly used terms in medical device risk management.

Table 1 Special Vocabulary of Risk Management

Term	Definition
Basic Safety	freedom from unacceptable risk directly caused by physical hazards when ME equipment is used under normal condition and single fault condition [7]
Essential Performance	performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk [7]

(*Continued*)

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00004-7

Table 1 (Continued)

Term	Definition
Expected Service Life	time period specified by the manufacturer during which the medical electrical equipment or medical electrical system is expected to remain safe for use (i.e., maintain basic safety and essential performance) Note – Maintenance can be necessary during the expected service life [7]
Failure	the inability of an entity to achieve its purpose
Fault	an anomalous condition for a part
Harm	injury or damage to the health of people, or damage to property or the environment [8]
Hazard	potential source of harm [8]
Hazardous Situation	circumstance in which people, property, or the environment are exposed to one or more hazards [8]
Instruction for Use	information provided by the manufacturer to inform the user of the device's intended purpose and proper use and of any precautions to be taken [2] article 2, (14)
Intended Purpose	use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation [2] Article 2 (12)
Intended Use	use for which a product, process. or service is intended according to the specifications, instructions, and information provided by the manufacturer [8] Note – ISO 14971:2019 [1] equated Intended Use and Intended Purpose in [1] Section 3.6
Label	written, printed, or graphic information appearing either on the device itself, or on the packaging of each unit or on the packaging of multiple devices [2] Article 2 (13)
Reasonably Foreseeable Misuse	use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behavior [8]
Residual Risk	risk remaining after risk control measures have been implemented [8] including actions to avoid, or limit the harm
Risk	combination of the probability of occurrence of harm and the severity of that harm [2] article 2, (23)

(*Continued*)

Table 1 (Continued)

Term	Definition
Risk Analysis	systematic use of available information to identify hazards and to estimate the risk [9]
Risk Assessment	overall process comprising a risk analysis and a risk evaluation [9]
Risk Control	process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels [9]
Risk Estimation	process used to assign values to the probability of occurrence of harm and the severity of that harm [8]
Risk Evaluation	process of the estimated risk against given risk criteria to determine the acceptability of the risk [8]
Risk Management	systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk [8]
Risk Management File	set of records and other documents that are produced by risk management [1]
Safety	freedom from unacceptable risk [1]
Serious Injury	injury or illness that: [10] a) is life threatening, b) results in permanent impairment of a body function or permanent damage to a body structure, or c) necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure Note – Permanent impairment means an irreversible impairment or damage to a body structure or function excluding trivial impairment or damage.
System	a combination of products, either packaged together or not, which are intended to be inter-connected or combined to achieve a specific medical purpose [2] article 2 (11)
User	any healthcare professional or lay person who uses a device [2] article 2, (37)

Further elaborations:

Hazard – A Hazard is something, exposure to which could potentially cause Harm. Sometimes the Harm is directly caused, e.g., a sharp knife. But sometimes the Harm is caused indirectly. For example, if a medical device is expected to sustain life, and it fails, the patient could die not because the device did something to the patient, but

because there was an expectation of performance that was not delivered. This is also a Hazard.

Harm – Although not explicitly stated in the official definition, the authors of the standard have a broad interpretation of the term "Harm" including unreasonable psychological stress, and unwanted pregnancy. The intention behind including damage to property and the environment in the scope of Harm, is to consider the type of damage that could have safety consequences. For example, improper disposal of radioactive isotopes in a brachytherapy device may endanger sanitation workers. In addition, with today's environment of cybersecurity concerns, data should be included in the scope of 'property.' For example, loss of X-ray images could lead to retaking the X-ray images and exposure to additional radiation.

Safety – Ref. [8] advises that the term "safety" be used as a noun, rather than as a descriptive adjective, to avoid misinterpretation of "safety" as an assurance of freedom from risk. Ref. [8] further advises that wherever possible, the term "safety" be replaced with an indication of objective. For example, "Protective helmet" instead of "safety helmet"; "protective impedance device" instead of "safety impedance". The word "safety" is used as a noun in these phrases: "safety and reliability," "degree of safety." Note that this is an advisory, not a requirement.

All medical devices carry a certain amount of Residual Risk, and the users should be made aware of such Residual Risks.

Risk – Although the definition of risk is simply "combination of the probability of occurrence of Harm and the severity of that Harm," there are many factors that play a role in the level of risk which is experienced by people. For example, exposure to a hot object causes burns. But it matters how hot the object is, how long the hot object contacts the person, where on/in the body the hot object contacts the person, and the physical properties of the hot object – compare a hot spoon vs. hot oil. Also, typically when a Harm happens, actions are taken to ameliorate the Harm. ISO/IEC Guide 63 [8], 3.10, Note 1, advises that in risk calculation the possibility to avoid or limit the Harm should be included.

Hazard Analysis vs. Risk Analysis – Sometimes, the terms 'Hazard Analysis' and 'Risk Analysis' are used interchangeably. This is incorrect. The purpose of Hazard Analysis is the identification of Hazards and the foreseeable sequence of events that could realize those Hazards. In contrast, Risk Analysis is about estimation of the potential risks due to the identified Hazards. Hazard analysis precedes Risk Analysis and identifies the Hazards. Risk Analysis estimates the risks of Harms that could ensue from the identified Hazards.

Intended Use vs. Intended Purpose – The guidance document: MDCG 2020-6 [11], Section 1 states that 'intended use' and 'intended purpose' should be considered

to have the same meaning. This is an evolutionary conflation of the semantics of these two terms. To understand the distinction, we can examine the definition of Intended Purpose in the EU MDR [2]: "use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation." Historically, Intended Use meant how a device was meant to be used, e.g., single use vs. multi-use, by what type of user, e.g., clinician vs. lay person, and in what way, e.g., a rectal thermometer is intended for insertion in the anus, but the Intended Purpose is to measure body temperature.

Intended Purpose/use vs. Indication (for use) – The guidance document: MDCG 2020-6 [11] Section 1 states that an Indication is a clinical condition that is to be diagnosed, prevented, monitored, treated, alleviated, compensated for, replaced, modified or controlled by the medical device, while Intended Purpose/use describes the effect of a device.

All devices have an Intended Purpose/use, but not all devices have an Indication. For example, a sterilizer has a purpose, but not an Indication.

4.1.1 Reasonably Foreseeable Misuse

ISO 14971 [1] requires that the manufacturer identify and document the Hazardous Situations related to the Intended Use, and Reasonably Foreseeable Misuses of the medical device. The risks associated with each Hazardous Situation must be estimated, evaluated, and controlled.

The definition for the term "Reasonably Foreseeable Misuse" was introduced in the 3rd edition of ISO 14971 [1]. The definition originates in ISO/IEC Guide 63 [8].

The definition is: "use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behavior." Although this definition helps, there is still confusion and debate about what constitutes a Reasonably Foreseeable Misuse. First, what is 'reasonable'? In whose judgement? Second, what is 'readily predictable'? Predictable by who? Should every wild and imaginative idea about misuse be considered as *reasonably foreseeable*?

Note 2 of the definition in [1,8] says "Reasonably foreseeable misuse can be intentional or unintentional." This confuses use-errors, which are unintentional, with off-label uses, which are intentional. In the opinion of this author, it is better to distinguish intentional vs. unintentional misuses. Intelligent and proper design of a medical device can help reduce use-errors when using a medical device. But healthcare professionals can intentionally and successfully apply a medical device for a use that was not intended by the manufacturer.

Risks from use-errors can be managed within usability engineering and included within the normal product risk management. Off-label uses are circumstances in which the user and the device are both successful in performing their functions. Your risk management team may imagine a large number of ways in which your medical device could be used off-label. The question is: which imagined off-label uses (misuses) should be included in the Risk Analysis?

The following six tests are offered as a means to determine if a misuse should be included in the Risk Analysis as a *Reasonably Foreseeable Misuse*.

1. Deliberate
   There is a deliberate decision by the user to use the device in the manner that they want.
2. Well-intentioned
   The User intends to do well by the patient, i.e., no harm is intended.
3. Beneficial
   The User believes a Benefit can be derived for the patient from the misuse.
4. Feasible
   The misuse is feasible, i.e., it is technically, financially, and skill-wise within the capability of the user to do the misuse.
5. Safe
   The user can safely use the device for the purpose that they wish to use the device.
6. Ethical
   The user is acting ethically. They have disclosed the truth about the intended misuse and have the consent of the patient and the hospital. (This is not relevant when a patient is using the device on him/herself.)

If a foreseen misuse meets the above six tests, then it can be construed as a Reasonably Foreseeable Misuse. Malice is excluded from the analysis. That is, if the user intends to harm a patient, such action is not included in the risk management of the medical device.

It is a very good idea to consult with other departments such as sales, marketing, and clinical staff to get insights into how the device might get misused in the field.

Tip Consider the situation when multiple generations of the same medical device are used simultaneously, e.g., in a hospital. Could that create a Hazard?

4.2 HAZARD THEORY

In order to receive Harm, there must be exposure to Hazard(s). Fig. 2 illustrates a model that is called Hazard Theory. Hazards either naturally exist, such as UV rays in sunlight, or they are created through a sequence of events. Let's examine the created hazards. Hazard Theory states that an initiating event starts a progression of events that

culminate in a Hazard. The Hazard is the last stop in the chain of events that lead to the Hazard. The chain of events could be long, or very short.

Once the Hazard is created, or when it naturally exists, it takes exposure to that Hazard to create a Hazardous Situation. Some exposures are automatic. For example, if an implanted device presents a Hazard, exposure is automatic since the device is already in the patient's body. Other exposures require a chain of events. For instance, imagine a worker in a radioactive environment is wearing protective clothing. The worker scratches the protective clothing, which leads to a tear in the fabric, which leads to exposure to radioactive particles.

A Hazardous Situation may arise as a result of external circumstances. For example, a surgical robot may rely on navigational data from a third-party device to guide the cutting instruments inside a patient's body. A failure in the third-party navigational input would result in a Hazardous Situation due to no failure of the robot itself.

Circumstances surrounding the Hazard and exposure affect the Severity of the Harm. For example, falling down could lead to injuries. But the height of the fall, and the softness of the surface onto which a person falls have an influence on the Severity of the Harm received.

In the BXM method the complete spectrum of Harm severities is considered. That is, given a Hazardous Situation, everything from nothing to death is considered. Therefore, it can be said that once the Hazardous Situation has been achieved, the probability of receiving Harm is 100%.

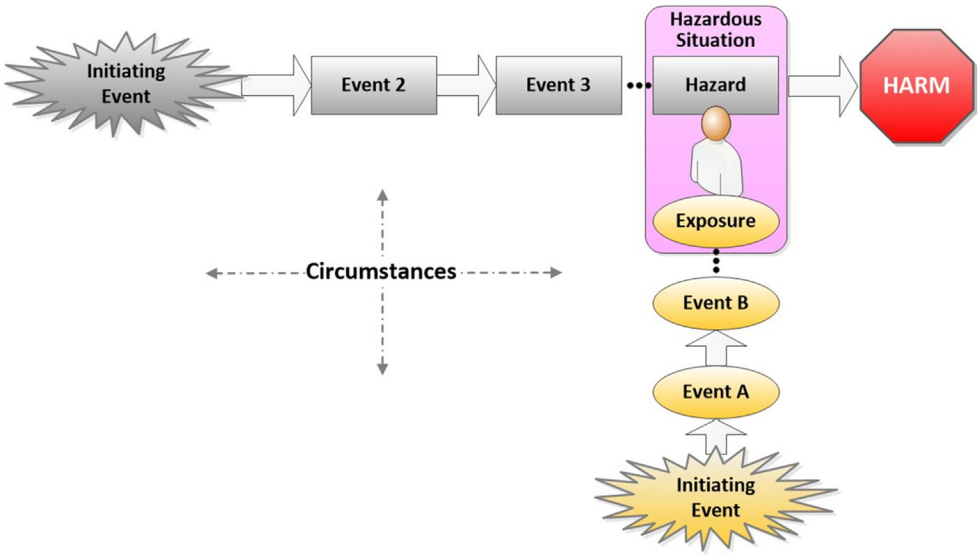

Figure 2 Hazard Theory.

4.3 SYSTEMS AND SYSTEM TYPES

The systems that are under consideration are engineered system, not natural systems such as an ecosystem, or social/governmental systems. The definition of engineered systems per INCOSE is "An engineered system is a system designed or adapted to interact with an anticipated operational environment to achieve one or more intended purposes while complying with applicable constraints."

More generally, INCOSE defines: "A system is an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not."

Systems have functions, behaviors, characteristics, physical structures and connectivity, both internal to the system, and external to the system. Sometimes systems exhibit unintended behaviors that were not recognized in advance, e.g., sneak paths. These could present hazards under non-failure conditions.

The Systems that are subjected to the risk management process can be classified into two categories:

a. Integral Systems
These are Systems that are observable as one integral piece from the perspective of the user. They do not require any assembly or integration by the user. Example: a blood glucose monitor.

b. Distributed Systems
These are Systems that comprise multiple components from the perspective of the user and require integration by the user. Example: a spinal cord stimulation System shown below with six individually integral components. Each integral component is separately approved, packaged and delivered to the user. Final assembly and integration into a working System is done by the user.

Reprinted with the permission of Medtronic ©.