MODULE 6

PRODUCT ENGINEERING

UNIT 1

RISK ANALYSIS AND RISK MANAGEMENT

Juan Carlos Bañón Guillén • María Sánchez Melero • Marta Martínez Navarro

DESIRE

DESIGN FOR ALL METHODS TO CREATE AGE-FRIENDLY HOUSING

DESIRE is a European project funded by the Erasmus+ programme.
Project number 2020-1-SK01-KA202-078245.

ISBN 978-80-227-5275-6

DESIRE will provide professionals in the building industry and home furnishings sector with the tools and skills to apply Design4All methods as an integral part of the design process, with the aim to create or adapt age friendly housing as a solution for the wellbeing, comfort and autonomy of the older adults or dependents at home.

The DESIRE training platform consists of six modules and 21 units.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

PUBLISHED BY:
© DESIRE, 2023, www.projectdesire.eu
Slovak University of Technology in Bratislava by Publishing house SPECTRUM STU, Bratislava 2023

AUTHORS:
Miguel Ángel Silvestre Botella
Zuzana Čerešňová
Carina Dantas
Natália Filová
Juan Carlos Bañón Guillén
Miroslava Hlinčíková
Michal Kacej
Veronika Kotradyová
Dean Lipovac
Nastja Podrekar Loredan
Juliana Louceiro
Soňa G. Lutherová
María Sánchez Melero
Marta Martínez Navarro
Lea Rollová
Matic Sašek
Mária Šimková
Helena Tužinská
Ľubica Voľanská

ILLUSTRATIONS:
Zuzana Čerešňová
Natália Filová
Michal Kacej
Veronika Kotradyová
Markéta Kučerová
Lea Rollová
Lenka Suláková
Barbora Valábeková

GRAPHIC DESIGN:
Mária Šimková

TABLE OF CONTENTS

PRODUCT ENGINEERING

The aim of this module is to offer a broader and more advanced vision to project, direct and coordinate all activities related to the management of the entire product life process. This module will enable the participants to apply industrial design with an innovative character in a way that generates added value to products, improves competitiveness and enhances the brand in line with new consumer needs and requirements. All this from a quality and risk management and control perspective. As an added value, the subject of CE marking will be dealt with.

UNIT 1 – RISK ANALYSIS AND RISK MANAGEMENT

The walls of home are always a synonymous of security and protection. However, the objects and accessories that we like the most can become dangerous if the sources, before being put on the market, an exhaustive analysis of the risks is not made. This unit will offer a global vision of the regulations and methodology for effective management and analysis of risks in product design process.

1.1 WHAT IS IT AND WHY IS IT IMPORTANT?

The term risk is defined by the Royal Spanish Academy of Language as “a contingency or proximity of harm”. Therefore, being aware of these risks gives us an important advantage over their consequences.

Risk in an activity that may have two components: the likelihood or probability of a negative outcome occurring and the size of that outcome. Therefore, the greater the probability and the potential loss, the greater the risk.

In a broad sense, **risk analysis** is the systematic use of available information to determine the frequency with which certain events may occur and the magnitude of their consequences. It is a document that describes the methodology followed during the analysis for product evaluation, considering the way in which failures can occur.

IN A NUTSHELL

The basic concepts to be considered for risk analysis are:

- **Risk:** Probability of occurrence of a hazardous situation causing damage and the degree of severity of such damage.
- **Hazard:** Potentially harmful effect on the user or the environment.
- **Harm:** Physical injury or damage to health or the environment.
- **Severity:** Qualitative measure of the possible consequences of a hazardous situation.
- **Residual risk:** Risk identified by the risk analysis that remains after all appropriate safety measures have been taken.

The importance of carrying out a risk analysis lies in the fact that thanks to it, decisions can be taken to implement preventive measures to avoid potential dangers or reduce their impact, since its prior evaluation allows us to anticipate the circumstances.

IN A NUTSHELL

TECHNICAL FILE:

Each risk analysis process shall be reflected in a written document which shall be part of the Technical File. This document shall contain at least:

1. Full description of the product.
2. Any assumptions adopted for the analysis.
3. Hazards identified.
4. Hazardous situations identified.
5. Information and data used for the evaluation.
6. Safety measures implemented to reduce and/or eliminate the hazards.
7. Residual risks after the implementation of the safety measures.
8. Final result of the product risk assessment.

More specifically, considering the ISO 14971 definition of the application of risk management in medical devices, then risk analysis is described as “the systematic use of available information to identify hazards or potential sources of harm and to estimate risk, understood as the combination of the probability of occurrence of harm and the severity of that harm”.

This concept has two components:

1. Probability of the harm occurring, i.e., the frequency with which it is likely to occur.
2. Consequences of the harm, i.e. how severe it may be.

The aim is to anticipate all risks that may arise during the design, manufacture, transport, storage and use of the product in order to provide solutions that guarantee the highest possible level of safety.

IN A NUTSHELL

SAFETY OF MACHINERY – GENERAL PRINCIPLES FOR DESIGN – RISK ASSESSMENT AND RISK REDUCTION STANDARD (ISO 12100):

A recent addition to the furniture industry, Safety of machinery – General principles for design – Risk assessment and risk reduction standard (ISO 12100) applies to many of them. It defines risk analysis as "the combination of machine boundary specification, hazard identification and risk estimation".

Risk analysis according to ISO 12100 comprises:

1. Determination of the limits of the machine
2. Identification of hazards
3. Risk estimation

By applying this standard, the manufacturer can anticipate possible risks, the designer is provided with tools to ensure that the machine (in this case, the piece of furniture) is safe and besides, a risk assessment is obtained throughout the life cycle of the furniture that allows us to anticipate the consequences. It is, therefore, the ideal way to ensure that the piece of furniture meets the expected safety requirements.

Moreover, risk management refers to the process of identifying and assessing risks, as well as creating a plan to reduce or control them in order to reduce the effect they could have on the company.

Through risk management, we can proactively identify, analyse and respond to risk factors throughout the life of a project or product and control potential future events.

IN A NUTSHELL

RISK MANAGEMENT:

ISO 14971 states that: "Risk management is a complex issue because each stakeholder may assign a different value of acceptability of risks in relation to the expected benefits". Even so, the manufacturer must estimate the risk of the device and act based on how that risk compares to the (previously defined) risk acceptability levels to comply with the standard, as well as define the necessary acceptance/rejection criteria, determine the test parameters, add safety features, etc. This risk management system should consider the entire life cycle of the device, not just the design stage.

As described in ISO 12100, risk assessment is defined as "the overall process comprising risk analysis and risk evaluation". Risk assessment is a series of logical steps to systematically analyse and assess the risks associated with machinery.

The objective of the application of risk assessment according to ISO 12100 is to reduce risk as much as possible, considering four factors. The process itself is iterative and several successive applications may be necessary to reduce the risk, making best use of available technology. When carrying out this process, these four factors are to be considered in the following order of preference:

- the safety of the machine during all phases of its life cycle
- the suitability of the machine to perform its function
- the operability of the machine
- the costs of construction, operation and decommissioning of the machine.

1.1.1 Example: Medical devices – Application of risk management to medical devices (ISO 14971:2020)

Within the furniture sector, a medical device is any product intended by the manufacturer to be used by humans for any of the medical purposes specified in ISO 14971 standard. A medical device may be:

- diagnosis, prevention, monitoring, treatment or alleviation of a disease,
- diagnosis, prevention, monitoring, treatment or alleviation of an injury,
- research, replacement, modification or support of the anatomy or a physiological process,
- the maintenance or prolongation of life,
- conception control,
- disinfection of a medical device,
- to provide information with in vitro examination of human body derivatives, and without exerting its main action in or on the human body by pharmacological, immunological or metabolic means, but to whose function such means may contribute.

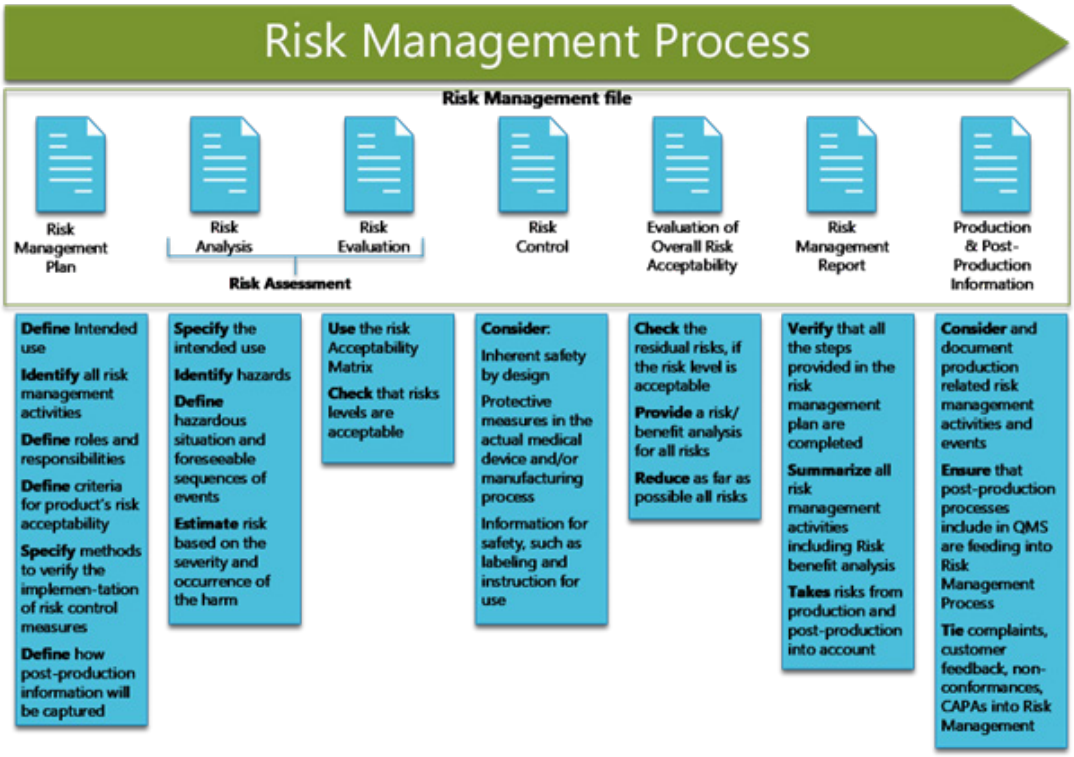

Figure 6.1.1 Steps of the Risk Management process.

Thus, chairs, beds, handles or any support product introduced in healthcare environments and used by people in any of the processes mentioned by this standard could be included in this definition.

IN A NUTSHELL

ISO 14971:2020

ISO 14971 standard specifies a process to be followed by the manufacturer to identify the hazards associated with medical devices, to estimate and evaluate the associated risks, to control such risks and to monitor the effectiveness of the controls.

The requirements of this standard are applicable to all stages of the medical device life cycle, from design to post-market and recall. These requirements also provide manufacturers with a framework within which experience, knowledge and judgement are systematically applied to manage the risks associated with the use of the medical device. This document addresses the processes for managing risks associated with medical devices. Risks may relate to injury, not only to the patient, but also to the user and others and may also relate to damage to property (e.g., objects, data, other equipment) or to the environment.

For a correct risk management according to this standard, the manufacturer is obliged to:

- Identify the risks and avoid the potential hazards,
- Document the process and update documents and procedures in case new ones appear or the existing one's change.

Regulation (UE) 2017/745 pays particular attention to managing these risks: anticipating them, combating them, documenting them, testing the absence before marketing and feeding the system with post-sale experience. In short, it closes the circle around risks, aims to control the known risks and to provide quick and effective responses to the unanticipated ones.

1.2 METHODOLOGY

Among other aspects, 14791 determines that there must be a risk management plan that includes the scope of planned risk management activities, identifying and describing the medical device and the life cycle phases for which each element of the plan applies; the assignment of responsibilities and authority; the requirements for review of risk management activities; or criteria for risk acceptability, among other aspects.

The risk management process includes the following actions:

Risk analysis: This phase involves an understanding of the risk, i.e. determining its consequences and probabilities, taking into account the presence and effectiveness of existing controls. The methods used for this risk analysis can be qualitative, semi-quantitative or quantitative.

- Qualitative assessment is often expressed with “high”, “medium” and “low” levels to define consequences, probabilities or level of risk.
- Semi-quantitative methods mainly use linear or logarithmic numerical rating scales.
- Quantitative analysis works with realistic numerical values and obtains the same type of results. The problem is that sometimes, in addition to these values, other factors that are difficult to quantify or simply missing data must be considered.

Risk assessment: Decisions are made about future actions based on the knowledge of risk that has been obtained during the analysis phase.
Risk control: The process of making decisions and implementing measures by which risks are reduced to or kept within specified levels.
Overall residual risk assessment: An overall process comprising a risk analysis and a risk assessment. This considers the contributions of all residual risks, in relation to the benefits of the intended use, using the overall residual risk acceptability method and criteria defined in risk management.
Risk management review: Verification of compliance with the implementation of the risk management plan. This review should at least ensure that:

- the risk management plant has been properly implemented
- the overall residual risk is acceptable,
- there are appropriate methods implemented for collecting and reviewing information in the production and post-production phases.

Production and post-production information: Active review of all documentation generated by the manufacturer in the production and post-production phases where considerations should be given to the appropriateness of the methods of data collection and processing.

Risk identification is the stage in management where uncertainty factors are identified. This stage is particularly important because failure to identify risks would make subsequent management ineffective.

This standard requires manufacturers to determine objective criteria for risk acceptability, but does not specify acceptable levels of risk, so it does not specify an exact methodology with which to perform risk management but leaves it to the manufacturer to decide which of all existing methodologies best suits his/her type of organisation and product, as long as the results obtained from such application comply with the instructions given therein.

Some methodologies used in risk management are:

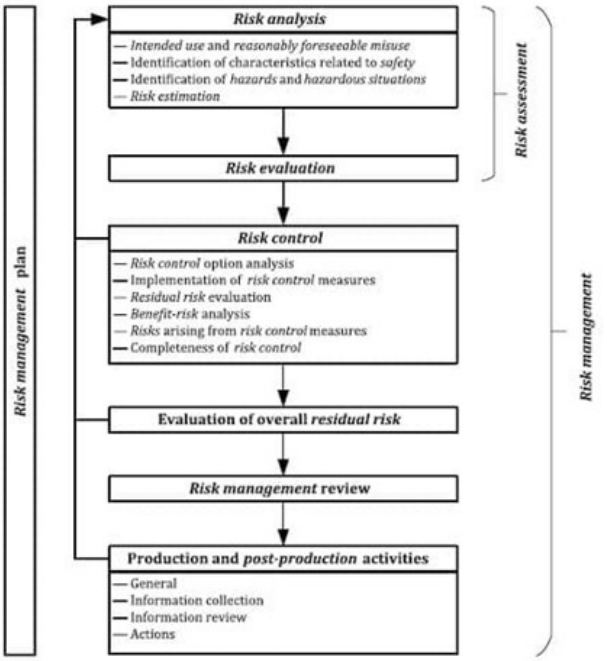

Figure 6.1.2 Schematic representation of the risk management process according to ISO 14791

6.2.1 Delphi method

DEFINITION:

This method consists of a group communication process to predict results based on the opinions of a group of experts. It is a strategic method to prevent risks or predict certain situations by repeatedly consulting experts in an area. In this way, information is obtained about certain events, their probability and possible consequences. Qualitative but precise information is obtained about future situations.

It is a method characterised by heterogeneity. These experts belong to different branches of activity making the study observed from different perspectives. It should also be noted that the experts do not know the identity of the other participants. In this way, they do not feel pressured or conditioned by the other participants.

APPLICATION:

The key to the method is consensus, the convergence of opinions. In this way, the experts will draw up a questionnaire which will then be analysed. If no consensus has been reached, another questionnaire is drawn up with the processed information. The process is repeated until there is consensus among the experts.

The aim of this method is to reduce as much as possible the different predictive possibilities or forecasts. Thus, one could say that it simplifies the outcome of a complex project thanks to the group opinion of several expert individuals, leading to a possible decision making.

Four of the main features of the Delphi method are:

- Experts remain anonymous
- Group heterogeneity.
- All responses are considered in a statistical way.
- It is an iterative process and controlled question feedback

PHASES:

1. Identify the reason for carrying out the process.
2. Define objectives.
3. Select the team of experts.
4. Prepare and hand out questionnaires.
5. Analysis of the results.
6. Redistribution of the questionnaire.

Each opinion is evaluated, and a difference or quantitative average of the group consensus is obtained. In addition, questionnaires can be carried out as many times as required until the objectives are met. Although it is a method included in qualitative research (experts make qualitative comments), quantitative techniques are also used.

Figure 6.1.3 The Delphi Method

The application of this predictive method has the following benefits: a greater degree of objectivity than purely qualitative research; credibility by reaching consensus; opinions are not categorical, as it encourages the exchange and mixing of different opinions; it avoids conflicts between experts and increases the possibility of being creative; it promotes freedom of expression and keeps all experts on equal footing, without favouring any one expert.

6.2.3 What if-analysis

DEFINITION:

This methodology is usually used in the first phase of management when risks are just being identified. Afterwards, this technique can be complemented by a more in-depth analysis of the risks and their causes through additional techniques. It is a qualitative risk identification technique that is usually applied to any unusual design condition of the facility or operations.

It is a very flexible and creative method that consists of scheduling meetings between collaborators who have in-depth knowledge of the process being analysed without any limitation as to the areas that can be covered by the questions. What-if analysis can be used in any area that is of interest for study. The kick-off meeting is scheduled for brainstorming, and questions that may help in making problems visible are developed. The name What-if comes from the type of questions generated.

In subsequent meetings the expert group will find answers to address the questions that were asked, seeking causes, consequences and recommendations.

This method basically consists of defining trends, formulating questions, developing answers and evaluating them appropriately, including the widest range of likely consequences, and does not require special quantitative methods or concrete planning to answer these questions.

APPLICATION:

Specific information on the process is used with the aim of creating enough questions to be asked at the best time and over the lifetime of the organisation's facilities. This method can be performed at any stage in the life of the process using the available information and process knowledge and can introduce appropriate changes during the lifetime of the industrial facility. Through its application, it questions the outcome of the presence of undesired events that may cause adverse consequences within a process or manufacturing plant.

PHASES:

This type of analysis encourages questions beginning with “What if...?”. Using them, an experienced group identifies possible accidents, their consequences and existing safety levels, later suggesting alternatives for risk reduction. Identified potential accidents are not ranked and are not given quantitative implications.

Its main objectives are:

- To identify events that can lead to major hazards
- To increase the operability of facilities.
- To identify more effectively all conditions and situations that are more likely to be hazardous, as they may be the result of applying inadequate controls.
- To provide different suggestions to start an operational process reducing the risk the installation may generate.

6.2.4 Failure Modes and Effects Analysis (FMEA)

DEFINITION:

It is a structured analytical methodology used to anticipate and identify failures that may arise in the process of creating a product or system, in order to avoid them. It is one of the most common tools to prevent potential failures during product development and is applied when designing new products, services or processes.

Thus, a modal analysis is aimed at discovering all the possible failures of a product during the industrial design process and at avoiding such failures or, where appropriate, limiting their effect.

There are different types:

1. Modal analysis of failures and functional effects.
2. Modal analysis of failures and design effects.
3. Modal analysis of failures and process effects.

APPLICATION:

This method is used to prevent situations that jeopardise the design and operations of a company's products or services so that detection procedures can be established to prevent these situations. Its purpose is to study possible failures ("failure modes") and then classify them according to their importance. From there, we will obtain a list that will help us to prioritise which are the most dangerous, most annoying for the user, most difficult to detect or most frequent, and which are the least relevant, which we should not worry about, either because they are infrequent, or because they have very little negative impact, or because they are easy for the company to detect before bringing the product to the market.

This tool is particularly useful to reduce risks and potential failures that may generate waste, defects or negative consequences for the final user.

PHASES:

Steps in the analysis:

1. List all the possible failure modes

The first thing to do is to create a working group of 4 or 5 people who have knowledge of the product being developed. They should be from different disciplines and include different profiles, such as designers, engineers, technicians and even final users. In this way, we will get a broader vision.

With the group assembled, we proceed to list the "failure modes" of the design: faults that the finished product could have, which can range from aesthetic, functional and safety defects to problems related to misuse. Here it is important to consider what the expected use of the product will be.

2. Set the priority index

Now we will have a long list of possible failure modes. All should be included in a table in which the following data should be encompassed:

AMFE							
Elemento / Función	Modo de fallo	Efecto	S	O	D	NPR = S*O*D	Acciones propuestas
describir elemento	describir modo de fallo	describir efecto	1 a 10	1 a 10	1 a 10	1 a 1000	proponer acción de mejora si sale un NPR alto

Failure modes must then be ranked according to their importance. For this purpose, each of them shall be assigned three values:

S: severity level (severity of the failure as perceived by the user).

O: occurrence level (probability of occurrence of the failure).

D: detection level (probability that we do not detect the failure before the product is used).

Each failure mode will be assigned S, O and D values, ranked on a scale from 1 to 10.

VALUE	DETECTION (D)	MEANING
1	ALMOST ALWAYS	The defect is obvious. It is highly unlikely to go undetected by existing controls.
2-4	**FREQUENTLY**	**The defect, although obvious and easily detectable, it may escape a first check, although it would certainly be detected later.**
5-7	SOMETIMES	The defect is of such nature that it is difficult to detect with standard procedures.
8-10	**HARDLY EVER**	**The defect cannot be detected. It will certainly be perceived by the customer.**

VALUE	OCCURRENCE (O)	MEANING
1-4	NOT EXPECTED	There is only a very remote possibility of danger occurring.
5-6	**UNUSUAL**	**It is unusual throughout the product lifecycle.**
7-8	OCCASIONAL	The hazard may occur at some point in the product lifecycle.
9-10	**FREQUENT**	**The hazard occurs repeatedly during the use of the product.**

VALUE	SEVERITY (S)	MEANING
1-2	MINOR	It does not cause injury.
3-4	**MODERATE**	**Damage curable with normal therapeutic measures within a short period of time.**
5-8	MAJOR	Damage requiring medical intervention. Healing usually takes considerable time.
9-10	**CATASTROPHIC**	**Damage requiring urgent surgical intervention. It may cause permanent injury or death.**

Once S, O and D have been estimated, we will multiply them to obtain the RPN (Risk Priority Number)

RPN = S × O × D

(Risk Priority Level = Severity × Occurrence x Detection)

This value will mean the importance of the analysed failure mode.

3. Prioritize failure modes and seek solutions

Once the RPN is calculated for all the failure modes, we will rank them from high to low. Failure modes with the highest RPN will be the ones that need to be addressed first. If a failure mode is unacceptable, severity can be reduced:

- Acting so that if it occurs, it will be less severe (S will decrease)
- Acting so that it happens less frequently (O will decrease)
- Acting so that if it occurs, it is detected before delivering the product to the customer (D will decrease).

This way your initial RPN can be compared to your final RPN.

6.3 ANALYSIS AND RISK MANAGEMENT IN THE DESIGN PROCESS

When a product comes to market (medical or otherwise), it will not be perfect, even after carrying out the appropriate tests. In an ideal situation, after the tests and trials, all the faults and deviations in the initial design would have been found and improvements would have been introduced in a new design so that it would reach the end customer as a perfect product, in terms of quality or usability.

Due to the complication of controlling all aspects related to the design and development of a product, some details may be left unattended and will be carried over into the product. Therefore, the manufacturer must make a great effort to avoid errors, since correcting any deficiencies will mean a great economic investment, time and loss of brand image. Carrying out a complete and exhaustive risk analysis during the first stages of the product creation process will increase its reliability, quality and safety.

6.3.1 Risks in the design of medical devices

ISO 14971 requires the manufacturer to establish a risk management process as part of the design and development of a medical device, although it should be emphasised that the risk management process does not end with design and production but continues into the post-production phase.

When designing a medical device, inherently safe design must be taken into account, i.e., the features that the product is provided with during design must meet all the safety requirements and must not be able to be modified during the whole process.

Risk analysis, therefore, becomes a mandatory phase in the design process of any medical device, as many of the problems that occur after the product has been manufactured and even with products already launched on the market can sometimes be avoided by careful risk assessment during the conceptualisation and design stage.

Successful risk management is essential to the design and development of safe and effective medical devices. Unfortunately, manufacturers too often consider it as an isolated activity that must be performed simply to comply with a regulatory requirement, unaware of the costs at all levels if not considered. Early exploration of potential risks allows risk to be used as a tool during concept selection.

6.3.2 Hazards in machine design

In the process of designing machinery or furniture considered as such, according to ISO 12100, inherently safe design measures are the first and most important step in the risk reduction process. These measures consist of avoiding hazards or reducing risks by appropriate selection of design features for the product itself and/or the interaction between exposed persons and the product.

Inherently safe design are preventive measures that eliminate hazards or reduce the risks associated with hazards by changing design or functional features without the use of guards or protective devices. As such, they become effective features that cannot be modified, as safeguards, even if well designed, can fail or be breached.

When designing any piece of furniture that can be included within the definition of a machine in the standard, different geometrical factors and physical aspects must be taken into consideration.

By **geometric factors** we mean the final shape of the product, which must be designed to acquire the appropriate characteristics to ensure that the user has a correct vision during handling, thus avoiding any risk derived from the movement of the product both for the user himself and for other people exposed in dangerous areas.

It is also intended to ensure that the product design does not contain sharp edges or angles, protruding parts and that the existing mechanical parts that can lead, among other things, to the shearing or crushing of some parts of the body, have the appropriate separation to ensure that they can enter easily or, on the contrary, cannot enter the product. In addition, the final design must ensure that it can be handled from an appropriate position that does not involve physical effort that could lead to injury.

On the **physical side**, the design shall include features to limit the driving force, mass and speed of moving parts and emissions of noise, vibration, substances or radiation.

In addition to these two factors, it is also advisable to consider the properties of the materials used in terms of fatigue, wear, toxicity, etc., the use of intrinsically safe power supplies and the application of ergonomic principles among others.

In both cases, it is essential to comply with these aspects when designing and developing products, otherwise we would be introducing into the market a dangerous product without enough quality that will have consequences not only at an economic level for the manufacturer but also for the customer's use and safety.

REFERENCES

Auster, A. (2020). Risk Management for Medical Devices: ISO 14971:2019. https://kvalito.ch/risk-management-for-medical-devices-iso-149712019/

Cuofano. G. (2022). ¿Qué es el método Delphi? https://fourweekmba.com/es/metodo-delphi/

International Organization for Standardization (ISO) (2019). Medical devices – Application of risk management to medical devices. (ISO 9241-210:2019).

LIST OF PICTURES