IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 22, 2019, accepted December 10, 2019, date of publication December 16, 2019,
date of current version December 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960235

FMECA Design Analysis: Risk Management for the Manufacture of a CBCT Scanner

ERNESTO IADANZA[1], **(Senior Member, IEEE), DILETTA PENNATI**[1], **LEONARDO MANETTI**[2], **LEONARDO BOCCHI**[1], **(Member, IEEE), AND MONICA GHERARDELLI**[1]

[1]Department of Information Engineering, University of Florence, 50139 Florence, Italy
[2]Biomedical Engineering Advisor, 50100 Florence, Italy

Corresponding author: Ernesto Iadanza (ernesto.iadanza@unifi.it)

ABSTRACT The identification and classification of the risks associated with the use of electromedical equipment is a critical part of its design, requiring the application of precise methods to analyse such risks. The result of this analysis leads to the preparation of documents assessing all possible risks associated with the manufacture of electromedical devices, from design to production and final use, including installation and maintenance activities, and after-sales surveillance. This process translates into a guarantee of device reliability. The more that is done to make the device design safe, the greater its reliability will be and the lower the frequency of failures. Failure Mode, Effects, and Criticality Analysis (FMECA) is one of the many risk analysis techniques proposed by the ISO 14971 standard. This method makes it possible to identify and evaluate the consequences of the failure of each component in a complex system and to quantify the extent of each failure using numerical indices. This paper describes the application of this methodology to a small Computer Tomography (CT) prototype device designed to investigate the extremities of the human body. This prototype uses Cone Beam CT (CBCT) technology, employing a divergent, cone shaped X-ray beam rather than the classic fan-shaped beam. A special bed is used in conjunction with the CT scanner to support the patient. This bed is not merely an added accessory but is part of a complex system.

INDEX TERMS FMECA, medical equipment, clinical engineering, risk management, risk assessment.

I. INTRODUCTION

Computed Tomography (CT) was developed in the 1970s with the aim of overcoming the limits of traditional radiography, which only provided a single projection of the district of interest with low contrast resolution [1], [2]. In a CT scanner, the source and detector rotate around the patient, acquiring a series of images from different angles obtaining computer generated projections. The final images are representative of the distribution of the μ(x,y) attenuation coefficient of the object in a predefined section. A CT exam generates a series of matrices (slices) that are approximately 0.5-10 mm thick. These slices are aligned perpendicularly to the axis of the scanned section, which represents a "slice" of the patient's body, in which the varation of μ between different tissues can be observed [3]. Over the years, four generations of tomography have been developed, which differ in the reciprocal rotation of source and detector and in the geometry of the radiated beam. Then the Spiral CT was developed to acquire even more slices at once, while the device rotates continuously so that it can acquire an entire volume in a single step [4]. This way, large regions of the body can be examined in just a few seconds. Cone Beam CT (CBCT) is widely used for examining small districts and for veterinary medicine. This technology uses a cone-shaped beam of ionizing radiation that fully scans the region to be analysed. A CBCT device, if compared to a Spiral CT device, is characterized by: smaller size, lower costs, different shape of the radiant beam, lower power radiation towards the patient and a single detector [5]. In addition, the patient can sit on a bed with a reclining backrest and the Region Of Interest (ROI) can be acquired with a single 360° rotation of the X-ray tube. Scanning the same ROI with a Spiral CT requires several rotations.

In this paper we are discussing a CBCT scanner prototype, intended for the investigation of smaller body districts (head and upper and lower limbs). The device is manufactured by a company, based in Italy, researching, developing and manufacturing innovative diagnostic imaging technology products.

The associate editor coordinating the review of this manuscript and approving it for publication was Yongquan Sun.

A thorough analysis of the applicable standards is required before identifying the nature of the risks that may arise from the use of any medical devices. These standards describe how to verify the requirements of the health, safety and environmental protection directives and contain the device's essential safety and performance requisites. Recently, the new European Union Medical Devices Regulation (MDR) 2017/745 [8] has come into force. Once a device compliance with essential requirements has been verified, the manufacturer can declare its conformity with Regulation 2017/745 and apply the CE mark. The manufacturer of Class IIb medical devices, such as CT scanners, must also apply to a Notified Body for approval of its manufacturing facilities and/or its product.

Alignment with US requirements is necessary if the device is also intended for that market. The regulation of medical devices in the United States is governed by the Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) [9]. The FDA's regulatory reference is the Federal Food Drug & Cosmetic Act (FD&C Act) [10], a set of laws passed by Congress in 1938 to empower the Administration's oversight over the safety of food, drugs and cosmetics. To comply with this Act, the FDA issues, publishes, and implements a set of regulations which are set out in the Code of Federal Regulations (CFR), a general code of permanent regulations issued by the Executive and Federal Agencies [11].

Considering the intended use of the device discussed here and its mode of operation, the applicable standards are listed below:

- IEC 60601-1:2007 [12] gathers the general requirements for basic safety and essential performance necessary to eliminate the risks deemed to be unacceptable.
- IEC 60601-1-2:2018 [13] is a collateral standard, which contains the general requirements and tests for electromagnetic compatibility.
- IEC 60601-1-3:2009 [14] contains the general requirements for radiation protection in diagnostic X-ray equipment.
- IEC 60601-44:2011 [15] sets out the particular requirements for the basic safety and essential performance of X-ray equipment for computed tomography.
- IEC 60601-2-54:2011 [16] particular requirements for the basic safety and essential performance of X-ray equipment for radiography and radioscopy.
- IEC 61223-3-5:2005 [17] applies to computed tomography equipment components that affect the quality of the image and the dose sent to the patient and indicates the parameters that need to be tested.
- IEC 62366-1:2016 [18] provides a process for a manufacturer to analyse, specify, develop and assess the usability of a medical device as concerns safety. This "usability engineering" process enables manufacturers to assess and mitigate risks caused by usability issues. These might be linked to incorrect use or use errors that are part of the normal employment of the device but that are not reasonably foreseeable.

With regard to CFR requirements, the section of interest is Title 21 - part 1020, which regulates ionising radiation emitting products [19], [22]. These requirements partially overlap those in the IEC standards, yet they define different limits, especially concerning radiological testing.

The risks associated with the use of all electromedical equipment must be identified and classified as it is being designed. The international standard ISO 14971:2013 [23] regulates risk management applied to medical devices. This standard specifies a procedure that enables manufacturers to identify any hazards associated with medical devices, including in vitro diagnostic medical devices, to estimate and assess the associated risks, to control those risks, and to monitor the effectiveness of those controls. The requirements of the standard apply to all phases of the medical device life cycle. Appendix G to that same standard [23] proposes several risk analysis techniques, which are not mutually exclusive, but which can sometimes be used in a complementary manner.

Risk analysis techniques can be classified into two groups, depending on the two approaches used to study the risks of a given system [24]:

1) An inductive approach, where the analysis of the causes determines the consequences.

2) A deductive approach, where, instead, the causes are deduced from the consequences.

Some techniques are more appropriate for use in prototyping, whereas others require a deeper understanding of the device's behaviour during use. Below are the techniques suggested by the standard for prototyping, which are the most widely used in the field of medical devices:

- Fault Tree Analysis (FTA): a top-down deductive technique, aimed at analysing the effects of faults on a complex system. While the method is very powerful for understanding the resilience of a system also to multiple faults, it is not suitable for finding all possible initiating faults.
- Failure Mode and Effects Analysis (FMEA)/Failure Mode, Effects and Criticality Analysis (FMECA): a bottom-up inductive technique, very good in finding all the possible failure modes and assessing them. A weak point of this method is that it does consider each failure mode as independent from the others.
- Hazard and Operability Study (HAZOP): a technique dating back to the 1960s, very powerful for examining complex processes, specifically for assessing the risks the workers are exposed to, in their work environments.
- Hazard Analysis and Critical Control Points (HACCP): a systematic approach to guarantee food safety, very focused on the physical hazards in production processes.

A risk analysis was performed at the design stage of the CBCT device prototype in question. The FMECA methodology was applied because of the following advantages:

- Simplicity of application: all what is needed is a spreadsheet and some simple calculations.

- Possibility of studying complex units in detail: the method allows the user to go as deep as he likes, in itemising the analysed device, down to the single screw.
- Suitability of the methodology for new system design: being a proactive technique, it can be applied to devices that do not exist yet, as opposed to other techniques that need you to wait for a fault to happen to track back the root causes.
- Ability to be updated if new failure events occur: a key point in risk management is to periodically reassess the risks. For example, the frequency of occurrence of a failure mode could be modified after one or more accidents happened, as well as its severity.

The analysis generated a risk analysis table. This table considers the device's mechanical, electrical, electronic and software components. The risks identified were quantified according to the FMECA method. This way, all the possible risks linked to the manufacture of the device, from design to production, were considered and documented, thus improving the device reliability and a reduction of failures [25].

II. METHODS AND INSTRUMENTS

The proposal to build a CBCT device to scan the human body's extremities was part of the "Smart&Start Italia" project [26] funded by the Italian Ministry of Economic Development.

A. THE CBCT DEVICE

The CBCT unit comprises a very small CT scanner that is well suited for its intended purpose. The scanner can generate digital radiology images, CT images and fluoroscopy sequences. The patient bed is an additional component.

The scanner's dimensions were designed not to encumber the clinical facilities where it is employed. It is provided with wheels making it easily portable from one department to another. Furthermore, there was the objective of limiting the costs while providing a viable alternative to conventional spiral CT scanners for diagnostic examinations of specific areas.

Because the device includes its software, which is considered one of its components, they must be certified together.

The scanner's intended use is described below:

- Mode - Initially, only the CT mode will be implemented, reserving the addition of the DR (Digital Radiography) and fluoroscopy modes for future developments.
- Type of emission - The system uses a pulsed X-ray emission. Therefore, in addition to selecting the voltage and current settings at the tube, the pulse duration in milliseconds (ms), must also be set.
- Target - The device is intended to be used to scan adult patients only: emission parameters and calculation of the dose delivered to the patient are not designed for paediatric use.
- Regions of interest - Given the scanner's compact size, the regions that can be scanned are the upper limbs (hand, wrist, forearm and elbow), the lower limbs (foot, ankle and knee) as well as the head.
- Application – Initially, the device will be used for diagnostic purposes only, without considering intraoperative usage. Scans will focus on the hard tissues (bones) involving the regions of interest above.
- Users - Use of the device is restricted to legally qualified medical/diagnostic professionals (physicians, radiology technicians) who are competent or have been trained through an appropriate course.

1) PROTOTYPE DESCRIPTION

The device's base unit, the scanner, comprises two main subunits:

- A gantry, which is the rotating element needed to obtain the radiological images. The gantry contains the imaging chain, the flat panel sensor, the motors, the power supplies and the electronics. On one side of the gantry is the Human Machine Interface (HMI), where the operator can rotate the gantry as needed and turn the patient positioning lasers on or off. The device activation key and the imaging chain power button are placed on the opposite side. An emergency stop button is placed on both sides of the gantry, and it disconnects all power to the machine, interrupting both rotation and acquisition. This button can be quickly accessed, in any position the operator happens to be.
- The gantry rests on a base equipped with adjustable feet and wheels, which make the scanner unit portable. During installation, the wheels are raised, and the feet lowered by a hydraulic lifting system. Inside the base, there is a PC and an isolation transformer.

The reclining patient bed is manufactured according to strict technical specifications, making it suitable for the required use. The motorized bed, which is controlled by pedals, enables the operator to control the bed positioning. This allows raising the patient up, lowering the backrest and leg support as well as to achieve the Trendelenburg or anti-shock position. Depending on the area to be scanned, the bed can be adjusted for a supine or seated configuration. Any shifting movement necessary to position the patient is done manually. Therefore, the bed is equipped with swivel casters and brake pedals. The patient body positioning parts, giving support to the regions of clinical interest, are made of radiolucent carbon fibre. The arm support, which is anchored to the bed by special clamps (on the right and left sides), enables the operator to adjust the height of the patient's arm as required.

2) HARDWARE COMPONENTS

There are numerous device components forming a highly complex and sophisticated system. As mentioned above, the device's heart is inside the scanner unit and it comprises these main components:

- Monobloc. This is an integrated system, including both the X-ray tube and the high voltage generator that powers the tube, which was used to reduce the device's overall dimensions. Two filaments are fitted to obtain two different focal points and therefore images with greater or lesser detail. The device is provided with a cooling system to prevent overheating.

- Inverter. This component is used to convert direct current into alternating current voltage at the monobloc's operating frequency (20 kHz).
- Electronics. A series of electronic boards is necessary to manage and control the X-ray imaging chain operation.
- Collimator. This is made up of four metal plates that limit the X-ray beams, so that they radiate only the region of interest. These also limit radiation leakage (i.e. emissions that leave the monobloc, but which are not part of the primary beam) and thus reduce patient exposure.
- Flat panel detector. Image acquisition is performed by a detector combining a layer of scintillator crystals with a CMOS sensor.
- Lasers. These are used to position the patient in the gantry isocentre.
- Chiller. The heat exchanger or chiller cools the oil in the monobloc through heat exchange, by circulating a coolant (usually glycol). After exchange, the liquid is cooled again with a fan.
- Motors. The gantry rotation and the shifting of the flat panel are activated by two separate DC motors.
- Mechanical thrust bearing. The thrust bearing is a type of axial bearing, for low rotation speeds, which is used when a structural part (in this case the front of the gantry, which contains the source-detector system) needs to rotate with respect to another part (in this case the fixed back of the gantry) along a single axis, ensuring the linkage between the parts. This consists of two concentric steel rings, whose relative rotation is made by means of rolling elements, which can be ball or cylindrical roller bearings.
- Main Board. Communication among the different components is managed by a main board, which governs the operation of the machine. The flow of signals moving inside the device is managed by an Ethernet switch.
- PC. The PC has three hard disks: one for the operating system, one for the software and the "raw" acquired data and one for the database, where the reconstructed data is stored.

There are also several short circuit and overcurrent safety breakers and components that keep the machine safe in the event of a failure. The main safety function can be activated manually, by pressing the emergency stop button, which disconnects all power from the machine, or automatically through special safety relays.

3) CONNECTIONS

The connection among the different components described above is shown in Figure 1. As can be seen, the device is equipped with two isolation transformers, one of which has a unity gain, which separates the different components from the mains power supply: they are equipped with an electrostatic protective grounded shield, to prevent any interference and eddy currents on the primary from being transmitted to the secondary. Most of the components are powered with direct current through switching type power supplies, except for the radiology image chain, which operates at 230 VAC mains voltage.

This block diagram is useful when identifying possible failure chains.

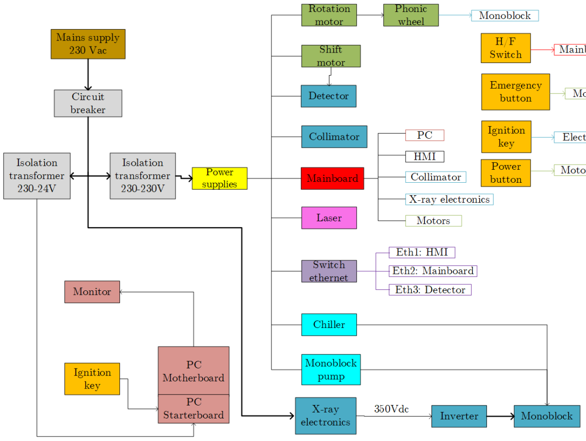

FIGURE 1. Connections among device components.

4) DEVICE REGULATORY COMPLIANCE AND SAFETY FEATURES

a: DEVICE CLASSIFICATION

Pursuant to Regulation 2017/745 [8], active devices intended to emit ionising radiation fall into class IIb. The elements forming the device would belong to different classes, if considered individually. When examining the whole system, the classification assigns the highest degree of severity overall. As a consequence, even if the bed is a Class I medical device, when it becomes part of a radiology system, it must also meet the essential requirements for Class IIb.

From a mechanical standpoint, according to the definitions in IEC 60601-1, the considered system is a mobile (transportable) device [12]. This classification is fundamental during testing steps because the system, not being anchored to the floor, is subject to greater instability. The same definition also applies to the patient bed.

From an electrical standpoint, according to IEC 60601-1, the system belongs to Class I electromedical equipment. In addition, neither the scanning unit or the bed are considered permanent installations because they are equipped with a mains power cord, which can be disconnected whenever the device is to be moved to another room.

The outer casings and the gantry are considered "Type B" (protected against electric shock) because they are the "applied part", which are parts of an EM device that under normal use come into physical contact with the patient. The patient bed is also considered to be a Class I device, which is not permanently installed. Also, it can be classified as a Type-B applied part [12] .

b: NATURE OF THE RISKS

The ISO 14971 [23] standard defines "risk" as the "combination of the probability of the occurrence of harm and the severity of that harm," with "harm" meaning "physical injury or damage to the health of people, or damage to property or the environment". The term "hazards" is defined as "potential sources of harm".

In order to identify the risks associated with the use of the device in question, Annex C of the standard proposes a series of questions to determine the characteristics of the medical device that might affect safety. These questions concern the manufacture, intended uses and the users, any reasonably foreseeable misuse and the final disposal of the medical device. The characteristics identified for the device under examination are collected in the System Safety Related Characteristics (SSRC), in Table 1.

Considering these characteristics and the requirements found in the reference standards, the risks have been classified as mechanical, thermal, electromagnetic and radiological.

c: EVIDENCE OF CONFORMITY

The standards listed in the Introduction provide for a series of conformity tests, which verify that the requirements of the standard itself have been met. Mechanical, electrical, thermal, electromagnetic compatibility and radiological conformity were performed on the prototype.

B. THE RISK MANAGEMENT PROCESS

Risk management consists of several phases; the main steps are illustrated in Figure 2 [23].

Starting immediately, at design stage, the risk management process continues during the whole life of the machine and ends only when the device is disposed. This paper focuses on the first phase of the risk management process: the risk analysis.

As mentioned above, the method chosen among the various techniques proposed in Appendix G to ISO 14971 is the FMEA/FMECA analysis. Using this technique, the consequences of a failure mode for each individual component can be systematically identified and evaluated. This is an inductive method, whereby components are analysed, observing individual failures, one at a time. Being also a "bottom-up" method, the analysis propagates up to the system higher function levels [23].

The reference standard for FMEA/FMECA analysis is the IEC EN 60812 [27], which describes and provides examples for studying the failures of a complex system. The scheme used for doing the FMEA analysis is not universal, as it can be modified according to its application.

TABLE 1. **System safety related Characteristics for CBCT device in study (Annex C ISO 14971:2013-05).**

1	Contact to patient/operator *(surface or invasive contact, implantation, period and frequency of contact)*
2	Energy delivered/extracted to/from patient *(type of energy, control, quantity, intensity, duration, levels higher than similar devices)*
3	Measurements taken *(variable measured, accuracy and precision of measurement results)*
4	Device interpretative *(algorithms used, confidence limits, unintended application of algorithms)*
5	Unwanted output of energy *(noise, vibration, heat, radiation, leakage currents, electric and magnetic fields)*
6	Unwanted output of substances *(substances used in manufacturing, discharge of chemicals, waste products, body fluids)*
7	Device susceptible to environmental influences *(operational, transport and storage environments, EMI, vibrations, power and cooling supplies)*
8	Device influencing the environment *(power and cooling supplies, toxic materials, electromagnetic disturbances)*
9	Maintenance and/or calibration necessary *(carried out by user or a specialist, need of special substances or equipment)*
10	Device containing software *(SW intended to be installed, verified, modified or exchanged by user or a specialist)*
11	Device subjected to mechanical forces *(forces under the control of user or controlled by interaction with other persons)*
12	Factors which determine the device lifetime *(ageing, battery depletion)*
13	Installation or use requiring special training *(novelty of device, skill and training of person installing the device)*
14	Information for safe use provided *(information provided directly to user or by third parties, training, installation skills)*
15	User interface design features contribute to user error *(indicators, controls, symbols, ergonomics, visibility, audibility, SW menus)*
16	Device with connecting parts or accessories *(wrong connections, similarity to other products, feedback on connection integrity)*
17	Device with a control interface *(slip, blunders, visibility, reversibility of settings or actions, mapping, kind of controls)*
18	Device displaying information *(visibility, clarity, units, colour coding, visual capability of user, accessibility of critical information)*
19	User interface can be used to initiate user action *(possibility to initiate a deliberate action to enter a controlled operation mode)*
20	Device can be deliberately misused *(incorrect use of connectors, disabling safety features, neglect of recommended maintenance)*

TABLE 1. ***(Continued).*** **System safety related Characteristics for CBCT device in study (Annex C ISO 14971:2013-05).**

21	Device hold data critical to patient care
	(consequence of data being modified or corrupted)
22	Device intended to be mobile or portable
	(grips, handles, wheels, brakes, mechanical stability and durability)
23	Device not permanently installed
	(unfixed plug, plug polarity, risk of detachment during operation)
24	Device availability
	(corrective/preventive maintenance procedures, spare parts availability)

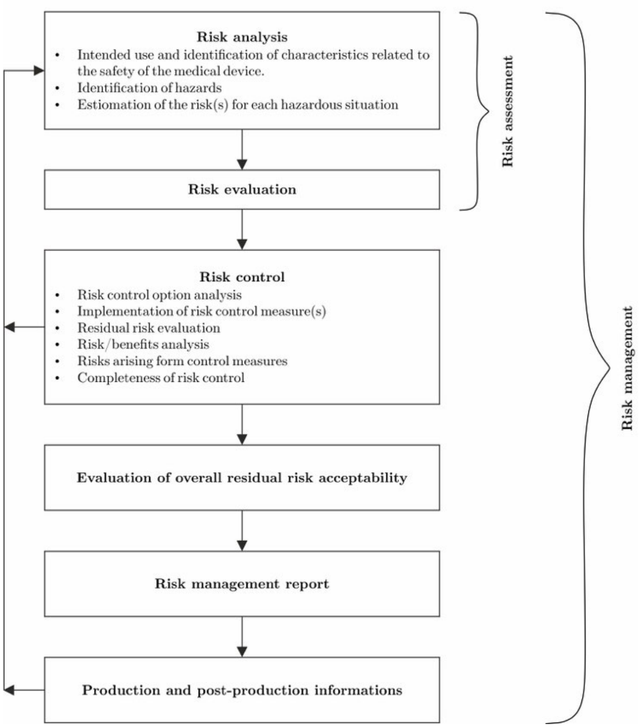
Risk analysis
Intended use and identification of characteristics related to the safety of the medical device.
Identification of hazards
Estiomation of the risk(s) for each hazardous situation
Risk evaluation
Risk control
Risk control option analysis
Implementation of risk control measure(s)
Residual risk evaluation
Risk/benefits analysis
Risks arising form control measures
Completeness of risk control
Evaluation of overall residual risk acceptability
Risk management report
Production and post-production informations
Risk assessment
Risk management

FIGURE 2. **The risk management process according to ISO 14971 [24].**

In the following are defined the terms which recur in the course of the analysis [28]:

- Failure mode: this is the objective evidence of the failure, i.e. how it is manifested.
- Cause of the failure: this is the combination of factors, such as design defects, chemical/physical processes or incorrect application of certain procedures, which can lead to a malfunction, directly or through a deterioration process.
- Failure effect: this is the consequence of the failure, which is reflected by the status or the operation of the component in question, of another component, of the entire system or of a person.

The FMEA analysis is presented in the form of a table, where the rows correspond to the various components or items, the columns to the failure modes and the causes and the effects of each fault identified.

The FMEA analysis is only qualitative, i.e. it does not give any measure of the criticality of a given failure. An extension of the FMEA analysis is the FMECA analysis, which uses numerical indices to quantify the extent of a given failure. These indices, which range from 1 to 10, represent:

- The severity (S), which estimates how much the effects of the failure affect the system or the user. If the severity equals 1, the effect will be practically negligible, if it equals 10, irreparable damage to the component / system and / or serious consequences for humans can occur.
- The occurrence (O), which estimates how likely the failure is to occur (1 if it is unlikely, 10 if it is very likely).
- Detectability (D), which estimates how likely it is to identify and possibly eliminate the adverse situation before it occurs, affecting the system and the user. Unlike the two previous indices, a low detectability is an indication of a good chance of diagnosing the failure, while it will be almost impossible to do so if this index is high.

The three indices are combined into a product called Risk Priority Number (RPN). The aim is to make this index as small as possible. If the risk is deemed unacceptable, this RPN must be lowered.

$$RPN = S * O * D(RPN = [1 \div 1000])$$

The FMECA analysis applied here is "multidimensional", since the value of S derives from the combination of severity calculated by including the effects on persons and on the device.

The standard suggests criteria for establishing the levels of Severity, Occurrence and Detectability. Nevertheless, since these criteria are not suitable for the medical field, others were adopted through the analysis of various articles in the literature and adapting them to the required application [35], [36], [40]. A detailed description can be found in paragraph B4).

The risk acceptance threshold can be established using several criteria, which are described below.

1) RISK REDUCTION

There are several categories of countermeasures that can be taken to reduce risk, even jointly [16] [18]:

- Changes in the design of the device to make it intrinsically safe.
- Active and passive safety devices.
- Hazard warning devices (warning lamps, alarms, labels…)
- Training personnel on the use of the device, including maintenance and installation personnel.
- Quality Assurance (QA) procedures. This term refers to all activities aimed at ensuring the fulfilment of quality objectives, which can include the organisation of design, components purchasing, installation, sales, after-sales

service and quality control. With regard to CBCT technology CT equipment, reference was made to the guidelines issued in 2017 by various bodies, including the AAPM [29].

- Safety information (operating instructions).

The approach that is generally applied in the risk assessment and control process follows the ALARP principle i.e. the risk must be "As Low as Reasonably Practicable". [30]–[32].

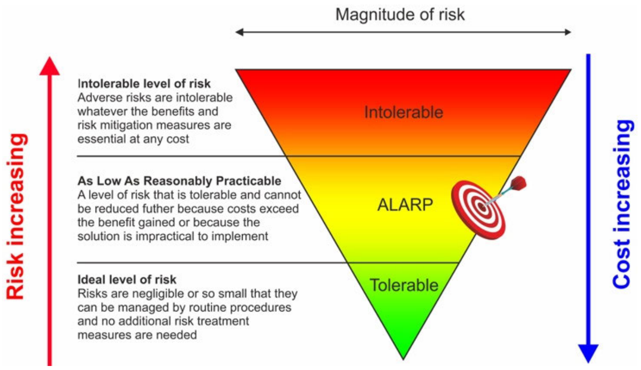
Magnitude of risk
Risk increasing
Cost increasing
Intolerable level of risk
Adverse risks are intolerable whatever the benefits and risk mitigation measures are essential at any cost
Intolerable
As Low As Reasonably Practicable
A level of risk that is tolerable and cannot be reduced futher because costs exceed the benefit gained or because the solution is impractical to implement
ALARP
Ideal level of risk
Risks are negligible or so small that they can be managed by routine procedures and no additional risk treatment measures are needed
Tolerable

FIGURE 3. Risk breakdown based on the concept of tolerability.

As can be seen in Figure 3, the risks that reside in the ALARP zone can be considered tolerable if one of the following situations applies:

- Any further risk reduction is impractical, i.e., there is no other way to reduce the risk.
- The cost, also in the sense of resource expenditure, of further reducing the risk exceeds the achievable improvement.

The 2012 edition of ISO 14971, compared to the previous 2007 edition, highlights that "Manufacturers and Notified Bodies cannot apply the ALARP concept with regard to economic considerations" [23]. This means that manufacturers and notified bodies will only be required to consider risk assessment and reduction measures in product design and in post-production based on technical considerations alone, without considering the cost of that reduction. The sense of being "reasonably practicable" in the ALARP criterion cannot therefore depend on the economic factor, which can only come into play when there is no effective risk mitigation. In addition, the latest edition of the standard stresses that labels and instructions for use alone cannot be considered as risk control measures.

After the mitigation, the presence of residual risks must be assessed, together with the new risks arising from the countermeasures applied. Finally, a risk/benefit analysis is used to determine whether the introduction of countermeasures has really made the device safer. Any residual risk must necessarily be below the acceptability threshold.

2) IDENTIFYING ERROR MODES

The "Design FMECA" or "Product FMECA" focuses on the identification of failure modes during the design and testing stages inside the company. This analysis is used to highlight and correct any design weaknesses that can lead to failures, problems or malfunctions in the use or application of the product. It is therefore a preventive approach that aims to identify those critical components that can lead to risk scenarios deemed unacceptable. Design FMECA can also guide the development of future devices, based on design changes [28]. A "Process FMECA" has also been performed, to analyse all the failure modes related to the use of the equipment. This analysis is not part of this article and will be published separately in the near future.

In our study, to perform the FMECA product analysis the system was divided into subsystems and each subsystem was broken down into components, such as the scanner unit, the base and the patient bed.

The components described in section A2 were grouped in macro-blocks. The resulting structure is shown in Figure 4.

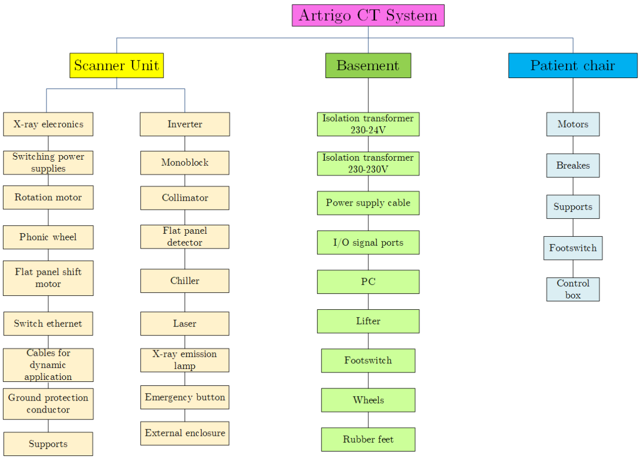

FIGURE 4. Breakdown of the system into subsystems and components for FMECA Design.

To understand how the required function can fail and how the failure can affect the other elements of the system, each component must be studied in its internal structure.

In this type of analysis, the failure mode is understood as a malfunction, a breakdown, damage or unwanted behaviour that may occur during one of the phases of the machine's use. Tests performed at design stage can help identifying failure modes at an early stage. These can therefore be mitigated by modifying the design and by providing appropriate information and training to the operator.

The human factor should not be neglected in the FMECA product analysis, because the cause of several failures lies in the absence of a preventive maintenance procedure and adequate training or adequate procedures, ensuring a proper use of the device.

TABLE 2. Structure of the FMECA design table.

ID	Component	Risk type	Potential failure mode	SSRC (#)	Potential cause of failure	Possible effect on the device	Possible effect on person	Initial device state	Sd	Sh	O	D	Smax	RPN	Actions recommended	Sd'	Sh'	O'	D'	Smax'	RPN'
Scanner Unit																					

3) STRUCTURE OF THE FMECA ANALYSIS TABLE

Based on the model in the IEC EN 60812 standard and motivated by examples drawn from the literature, the different failure modes were listed in a table (see Table 2). In the FMECA product analysis, each table row corresponds to a failure mode. Each failure mode is identified by a unique ID code consisting of three elements. The first element indicates the CT system section being considered (the scanner unit, the base or the patient bed). The second element indicates a component that is a part of that section (e.g., power supplies, monobloc, control pedals, etc.), the third gives a number to each failure mode. For example, the failure mode no. 1 for the monobloc, which is a part of the scanner unit, can be referred to as SU.M.F1. This type of classification shows that each component can have several failure modes, leading to different causes and effects. According to the FMECA methodology, each adverse event is considered individually, whenever a different risk scenario occurs, which is understood as a combination of S, O and D [28]. On the other hand, the columns show standard FMECA analysis information, which enables, starting from the failure mode identification, the risk priority index to be set and any countermeasures to be taken if necessary.

These columns are (Table 2):

1) Failure mode ID.
2) Component of the subsystem.
3) Type of risk: The failure mode may cause a hazard that could be mechanical, electrical, radiological, thermal, software-related or that affects usability or the environment.
4) Potential failure mode, i.e. how the component failure occurs.
5) The SSRCs (see Table 1) affecting that specific failure mode.
6) Potential cause of failure: this can be traced back to events that might not be directly dependent on persons (e.g. current or voltage spikes or fluctuations, mechanical wear, electromagnetic interference), or to human error, but, for example, in the design, installation, maintenance or use of the device.
7) Possible effect on the device: how the failure manifests itself in the operation of the device (e.g., it remains unchanged, runs abnormally or the fault causes a malfunction in downstream components).
8) Possible effect on persons: since the failure modes identified can occur at any time the machine is being used, the potential ''victims'' of a failure's occurrence could include the patient, the operator or both. The operator, in this case could be the radiology technician, the radiologist, the biomedical engineer or a technician doing repair or maintenance tasks.
9) Initial status: here the design solutions, procedures and tests already foreseen for the device, as inherited from a previous implementation, are described;
10) Identification of S, O and D, based on the corrective and preventive measures already identified, according to the criteria described in the next section B4.
11) Calculated RPN.
12) Recommended preventive or corrective actions (also in this case design solutions, procedures or tests), for unacceptable risks.
13) Identification of S', O', D', based on the actions taken. Some countermeasures will only mitigate one of the three indices, others more than one.
14) RPN', which must necessarily be below the threshold.

4) CRITERIA FOR ASSIGNING THE S, O, D PARAMETERS

Classification criteria are used in order to consistently attribute the level of severity, occurrence and detectability to each failure mode. These criteria were drawn in part from the literature and others were specifically established for the type of device analysed. Since the risk analysis was carried out during the design stage, it was only possible to estimate the values of S, O and D based on so-called ''predicate devices''. Predicate devices are the legally marketed devices that are substantially equivalent to the considered prototype (e.g., Spiral CT and CBCT scanners from other manufacturers and even other products from the same Company).

a: SEVERITY

Two severity indices have been assigned to each failure mode: the first refers to effects on persons, meaning a patient and/or an operator; the other refers to effects on the device. There are error modes that may be negligible for the device, but hazardous for persons and vice versa.

Severity Related to Persons (Table 3): aside from the physical and tangible effects on persons, such as cuts, bruises,

TABLE 3. Criteria for determining the degree of severity for human.

Severity (for human)	Criteria	Ranking
None	No injury to both patient and operator	1
Very minor	No injury to patient, minor injury to operator	2
Minor	No injury to operator, minor injury to patient	3
Very low	Minor injury to both patient and operator that does not require treatment or impossibility to perform the exam to the patient for few minutes	4
Low	Minor injury to both patient and operator that does not require treatment or impossibility to perform the exam to the patient for few hours	5
Moderate	Moderate injuries requiring treatment or risk of useless exposure to x-rays	6
High	Serious injuries but not permanent or risk of overexposure to x-rays	7
Very high	Very dangerous, long hospitalization with possible chronic outcomes or impossibility to perform the exam to the patient for several days	8
Hazardous with warning	Extremely dangerous, permanent injuries or risk of an incorrect diagnosis	9
Hazardous without warning	Extremely dangerous, possible death	10

TABLE 4. Criteria for determining the degree of severity for the device.

Severity (for device)	Criteria	Ranking
None	No effect on the device	1
Low	Minor effect on device performance	4
Moderate	Moderate effect on device performance	7
Hazardous	Serious effect on device performance	9

fractures, burns, electric shocks, radiological effects were also considered. These include unnecessary exposure to X-rays, which could expose a patient to an excessive dose, and overexposure (setting the tube parameters too high for the district under examination), which could also cause internal harm to the body.

Severity Related to the Device (Table 4): this considers to what extent a failure mode impacts device operation and how quickly the damage can be repaired, which affects the device's availability.

This multidimensional approach generates the identification of one single severity index, considering the calculation for the person and the device and choosing the greater of the two.

b:OCCURRENCE

The probability of occurrence (P), is established with reference to predicate devices: devices produced by the same Company and CT scanners produced by market leaders. Based on the number of failure reports, the likelihood that a specific failure mode will lead to device malfunction and/or harm to the patient or operator can be estimated.

If a certain failure mode was not found in similar devices, a search was made of other types, referring to the so-called Medical Device Reports (MDR), found in the ''Manufacturer and User Facility Device Experience'' (MAUDE) database. These can be consulted directly on the FDA website [33].

The FDA uses MDRs to monitor device performance, detect potential safety issues, and help evaluate the risk/benefit ratio of these products. These reports can be submitted by manufacturers, importers, device users, healthcare professionals (doctors, technicians and nurses), patients and biomedical engineers. The search was restricted to the years 2008-2018, to only the manufacturers Siemens, GE and Philips, identifying the following classes of products as predicate devices:

- X-ray computed tomography systems
- X-ray computed tomography systems for dentistry
- Portable X-ray systems
- X-ray angiography systems
- X-ray mammography systems

The reports have been grouped in categories, according to the fault cause: mechanical, electrical, radiological, environmental, thermal and software. In addition, some problems are related to human factors, due to improper use, faulty procedures and behaviour (unwanted outputs). The percentages of occurrences of each category are illustrated in Figure 5. Problems of an unknown nature were subsequently analysed and, if possible, assigned the proper class.

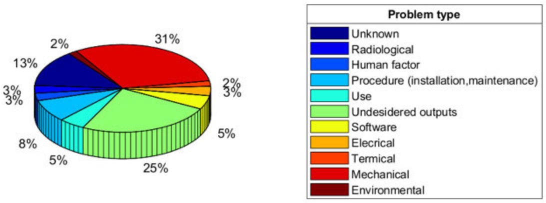

FIGURE 5. Percentages of the occurrence of types of problems.

The probability of occurrence P of a given failure mode was obtained by dividing the number of occurrences found by the number of similar devices currently installed (about 200) or by the total number of Siemens, GE and Philips devices installed in the United States, respectively.

According to the Statista portal [34], in 2017 in the United States about 42 CT scanners per million inhabitants were installed, so there are about 13000 machines in use for a population of 320 million. Sales data from market surveys show that of these 13000 devices, around 4000 were produced by GE, 3000 by Siemens, 2000 by Philips and the remaining 4000 by other manufacturers. As a result, standardisation was implemented on an indicative total of 9000 devices.

TABLE 5. Criteria for determining the degree of occurrence.

Occurrence	Criteria	Ranking
Remote: failure is unlikely	P<0.1%	1
Low: relatively few failures	0.1%≤P<1%	2
	1%≤P<2%	3
Moderate: occasional failure	2%≤P<5%	4
	5%≤P<7%	5
	7%≤P<10%	6
High: repeated failures	10%≤P<15%	7
	15%≤P<20%	8
Very high: failure is almost inevitable	20%≤P<25%	9
	P≥25%	10

The degree of occurrence has been classified with reference to examples from the literature [35] and to the experience of skilled engineers and technicians. The maximum ranking for occurrence was set at a probability of 25% (this means that about a quarter of the devices have found that specific failure). In this case it is reasonable to believe that failure is almost inevitable and should therefore be mitigated. Conversely, a failure occurrence is considered as "remote" when it occurs in less than 0.1% of the devices. (Table 5).

c: DETECTABILITY

The degree of detectability depends on the presence or absence of diagnostic devices, such as sensors, software checks and scheduled maintenance procedures. Also, in this case, the criteria were established based on articles in the literature [35], as shown in Table 6.

TABLE 6. Criteria for determining the degree of detectability.

Detectability	Criteria	Ranking	Probability of detection
Almost certain	Design/operation control will almost certainly detect a potential failure mode	1	91-100%
Very high	Very high probability of detection	2	81-90%
High	High chance of detection	3	71-80%
Moderately high		4	61-70%
Moderate	Moderate chance of detection (e.g. the defect will remain undetected until the device performance is affected)	5	51-60%
Low		6	41-50%
Very low	Remote chance of detection (e.g. the defect will remain undetected until device inspection is carried out).	7	31-40%
Remote		8	21-30%
Very remote	Defect most likely remains undetected (e.g. the design/ operation control cannot detect potential cause, or the operation will be continued to be performed in the presence of the defect)	9	11-20%
Absolute uncertain	Device/component failures are not detected (e.g. there is no design/operation verification, or the operation will be continued certainly to perform in the presence of the defect)	10	0-10%

5) METHODS FOR EXTRACTING THE RISK ACCEPTANCE THRESHOLD

The IEC EN 60812 standard [27] does not describe any method for establishing a threshold between the acceptability and the unacceptability of a risk but refers to the choice of a criterion suitable for the individual application. Several possible approaches have been identified in the literature [[35] - [43]]. Among these, we would like to mention two methods that have been used in this paper.

a: SCREE PLOT

This is a fully graphical method of identifying the RPN threshold, which sorts the failure modes for increasing RPN and then plots a graph that looks like a monotonic increasing curve [42] [43]. Generally, this curve is characterized by two trends: initially, it grows gradually, then there is a so-called "RPN jump" after which there is a sudden increase in the slope of the curve.

There are two ways to identify this slope variation:

1) Qualitatively, by observing the graph trend. This is the most widely used system in literature.
2) Mathematically, through the calculation of the maximum of the second derivative. This is the maximum variation in slope of a curve. The RPN threshold can then be identified as:

$$\mathrm{RPN}_{\mathrm{threshold}} = \max\left[\frac{d^2\mathrm{RPN}}{dx^2}\right]$$

Once the transition between the two trends has been identified, they can be approximated by two lines, the intersection of which represents the RPN threshold value. Therefore, it can be assumed that the point at which the slope of the curve increases abruptly, qualitatively represents the risk acceptability threshold. All failure modes above this limit are to be mitigated [42].

b: PARETO CHART

This type of chart can help determine what factors have the greatest influence on a given phenomenon, and is therefore a useful tool for analysis, decision-making and quality management. Some authors [6], [8] have used this chart for risk analysis, to highlight which error modes have the greatest impact on the safety of the device. This chart consists of a histogram, where failure modes are sorted by decreasing RPN and a line representing the cumulative RPN values, expressed as a percentage, with respect to the total value, i.e. the sum of the RPN. The Pareto criterion represents a statistical methodology, according to which 70-80% of the variability of the process (i.e. the unwanted outputs) derives from 20-30% of the total of the problems (i.e. the failure modes) [44]. Applying this principle, all the failure modes that contribute to 70-80% of the total value can be identified. The choice of the percentage ratio (80-20% or 70-30%) depends on the specific application. Therefore, the RPN threshold is correlated to the failure mode threshold, which corresponds to a cumulative RPN of 70 or 80%: consequently, all the failure modes that are graphically on its left are above the threshold (Figure 6).

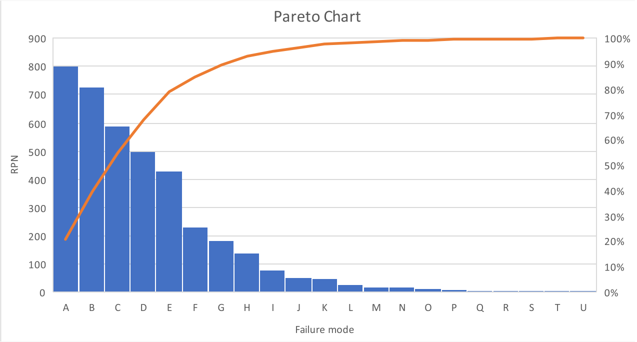

FIGURE 6. **Example of Pareto chart.**

A combined approach was used for the risk analysis covered by this article, using both the ‘‘scree plot’’ and the Pareto chart, based on the 70-30% system. Because these are two different methods, one purely graphic, the other statistical, two thresholds are identified, one for the less conservative method, the other for the more conservative one. Nevertheless, it was decided to maintain both thresholds and to establish a priority for action related to failure modes where the RPN is above both thresholds.

6) RISK CONTROL MEASURES IN THE INITIAL STATE OF THE DEVICE

Some risk control measures were already presend in some components of the prototype. The solutions already in place are listed below.

a: SOFTWARE CONTROLS

The various components are subject to both software and firmware controls, which sometimes act on the security system and sometimes on the coordination system.

- X-ray emission control
- Synchronization between gantry rotation and X-ray emissions.
- Monobloc temperature control.
- Monobloc warm up, which avoids the use of a cold monobloc, a situation that can generate electrical discharges.
- Connection check among the different components before scanning.
- Control of the position of the detector with respect to the collimator.
- Control of the correspondence between the settings of the X-ray tube parameters and those really provided.
- Double-checked verification of patient identity.
- Periodic data mirroring.

b: INTEGRATED SAFETY MEASURES

Aiming at the reduction of the risks associated with the system architecture, components with internal safety and control systems were chosen, for example:

- The power supplies are protected against overload, overvoltage and short circuit.
- The motors are protected against overheating, overvoltage and overcurrent by a control system, that switches off the motor in the event of any of these adverse events.
- The inverter has an insertion circuit that limits the inrush current when the device is switched on, due to the instantaneous charge of the capacitors. This current is limited by a power resistor.
- The monobloc is provided with a safety systems against overheating, as described above.
- The isolation transformer is equipped with primary insulation and an electrostatic shield, manufactured in compliance with IEC 61558-2-4 for over-temperature protection and limited losses on the windings.
- The PC thermal protection is guaranteed by an alarm system detecting overheatings due to continuous use or to heat transmitted by the adjacent insulation transformer.

c: SOLUTIONS FOR ALIGNMENT WITH CURRENT REGULATIONS ON CT SCANNERS

In addition to the testing mentioned in section A4, special design solutions were implemented to comply with standards, especially on radiological equipment.

Mechanically, the patient bed was designed so that the patient can be positioned correctly, without the risk of being trapped inside the gantry. As far as the activation of moving parts is concerned, according to IEC 60601-2- 44 standard [15] only continuous action commands were implemented for the scanner unit and bed pedals, whose release immediately stops any movement. This way, the operator can continuously monitor the patient avoiding possible harms.

Moreover, still in compliance with the standard, two emergency-stop push-buttons, made with high integrity components, located on the side of the gantry, will stop all motorized movements and disconnect power.

From a radiology standpoint, apart from those already discussed in section A4, other means of protection against ionising radiation were considered. To prevent the workstation outside the X-ray room being exposed to radiation, the device is equipped with an interlock, to be connected to the door of the room where the device is actually used. The interlock prevents the start of any emissions unless the door is closed. If the door is opened, accidentally or in an emergency, both the rotation of the gantry and the X-ray emissions are stopped.

Another fundamental aspect is the need to signal X-ray emissions. In compliance with the IEC 60601-2-44 standard, the emission is indicated by a warning lamp located above the scanner unit, an acoustic signal and by the software interface display.

From an electrical standpoint, IEC 60601-1 [12] standard does not recommend the use of multiple sockets or adapters, as they can vary the supply voltage of the load. For this reason, depending on the country where the device is to be used, the manufacturing Company will install the appropriate power plugs (both on the device and on the bed), so no use of adapters will be required. In addition, all metal parts have been connected to the ground terminal of the device using easily recognisable yellow-green wires. At the time of installation, the service will check that the mains voltage at the room power outlet is within the limits set by the standard (230±10% V) using a tester.

III. RESULTS

From the study of the device's possible overall critical issues, from a design standpoint, 103 failure modes were identified.

A. FMECA PRODUCT ANALYSIS

As indicated in the Materials and Methods section, possible failure modes were analysed for each of the device's individual components, trying to answer the question "What happens if…?" The main fault modes identified, and the resulting critical issues are summarised below, considering one subsystem at a time.

1) SUBSYSTEM 1: SCANNER UNIT

- Gantry enclosure - Two failure modes were identified, concerning the risk of having live metal parts (directly accessible or normally covered by the casing). However, the risk of electric shock is low, due to the tests and countermeasures applied (grounding and plastic guards).
- Switching power supplies - The same possible failure was considered for all five power supplies, i.e. a sudden shutdown causing a power failure to the downstream components. The malfunction of power supplies connected to more than one load (such as the 24 V) or to components required for scanning (such as motors, main board, Ethernet switch, etc.) has a higher RPN than those that supply secondary components, such as lasers.
- Motors - The motors are equipped with internal control systems, therefore there is a very low probability of unwanted behaviour due to drive or encoder malfunctions. Furthermore, the above described safety components ensure that there are no unacceptable risks (breakage of mechanical or electrical parts such as the rotors or stators). Regarding the flat panel shifter motor, the possibility that this could lead to slippage of the detector off its rails was considered: however, this failure mode is prevented by the presence of mechanical limit stops.
- Phonic wheel - The functionality of the phonic wheel may be lost due to the presence of dust/fouling, that prevents the photo-sensor correct functionment, or due to an electrical disconnection from the motor that rotates it. The variation of the trigger signal is detected by the software, thus enabling faster error diagnosis.
- Slewing bearing - It is possible that, due to ageing or poor maintenance, there is greater friction between the fixed and rotating part of the thrust bearing, causing sudden jerks and, in extreme cases, the detachment of the front side of the gantry. However, this failure mode has a low probability, given the limited speed of rotation, and is easy to diagnose because it increases noise output. To avoid unpleasant consequences, thrust bearing lubrication is periodically checked.
- Ethernet Switches - Critical issues have been identified in case of disconnection during acquisition, an eventuality that interrupts signal transmission. This can lead to loss of data and patient exposure to X-rays, because the examination will have to be repeated.
- X-ray Electronics - The correct operation of the components can be compromised by mains voltage instability. Though mains voltage stability is measured during installation, it is not monitored during machine use.
- Inverter - The identified failure modes concern: breakage of the connection circuit (countermeasure described in section B6 of chapter II); input and output voltage fluctuations, which could damage the downstream monobloc; damage to the cables, which could cause an electric shock in the event of contact. Although the voltages are very high (up to 120 kVp AC), these failure modes have a low RPN value, because the inverter is designed to protect the operator from contact with internal parts that could become connected to live voltage as well as the downstream components.
- Monobloc - Failure modes mainly concern the degradation of the tube elements, such as the rotating anode, the cathode and the cooling system consisting of the thermal switch and the oil recirculation pump. Also, in this case, the RPN values obtained are low, because there are several overheating control measures. However, periodic maintenance based on the workload is critical, because performance may deteriorate (e.g. due to darkening of the tube glass), in terms of reduced beam energy, which results in the generation of low-quality images. Another failure mode that could lead to unacceptable risks, such as patient/operator burns, is oil leakage from the monobloc. However, both S and O were considered low because the tank was designed to provide

for the expansion of the oil. Furthermore, it has been verified that if any oil does leak, it would be confined inside the scanner unit, draining along the side walls to the ground, without involving the patient.

- Chiller - Failures are due to inadequate maintenance, installation or use. Therefore, the failure modes identified have a high RPN because the occurrence of these events is high, while the severity is contained because the system can continue to run without major problems. The most frequent failures are glycol leakage, due to an overfilled tank or incorrect installation of the tubes where the liquid flows, and excessive vibration which occurs when the fluid goes below the minimum level. In particular, glycol leakage cannot be considered acceptable, given the toxicity of this substance if inhaled for a long time.
- Collimator - The collimator blades may jam during positioning, causing over or under exposure of the area to be analysed. This failure mode is identifiable because the collimator produces a noise that can be heard even by the operator. The same failure can also occur during the positioning of the filters. In this case, there may be artefacts due to the presence of metal parts, or loss of image quality if the filter does not completely cover the region of interest.
- Detector - Prolonged exposure to X-rays leads to a progressive deterioration of the panel's sensitive elements. This can manifest itself in the appearance of artefacts (especially ring-shaped), a reduction in panel sensitivity and an increase in so-called dark output, which means even non-irradiated pixels have grey levels other than zero, thus generating images with non-uniform background. The risk concerns generating low quality images that are difficult to interpret.
- Another failure mode is related to a misalignment between the collimator and the detector: this problem has been solved by an inspection.
- Laser - Two failure modes have been identified. The first concerns the malfunction of the laser (failure to switch on). The second is misalignment with respect to the patient bed, which may lead to incorrect positioning of the part of the body under examination in the isocentre.
- Dynamic laying cables - This term refers to cables that are not fixed during gantry rotation, but that shift together with the components during their movement. Problems with these components can occur in cases of incorrect wiring.
- Emergency stop - The malfunction of this component can occur in two ways. One is through the inability to turn the device on because of an open circuit or a disconnect failure in the emergency stop button; the other is the inability to lock the machine, due to a button failure. In the first case the software displays an error signal on the device, which can help diagnose the fault. In the second case, since there is an additional emergency button and since the software can also stop rotation, the likelihood of this failure mode occurring is lessened.
- X-ray emission lamp - If the warning lamp above the scanner unit fails, there is the risk that it will not be possible to check if X-rays are being emitted from the source. As already explained in section B6, apart from the lamp there is also an acoustic signal and a warning displayed on the software interface. These reduce the likelihood of a lack of control in the X-ray emission.

2) SUBSYSTEM 2: BASE

- Isolating transformer - The most common failure modes for a transformer are damage to the basic insulation and to the electrostatic shield due to excessive overheating, and damage to the windings due to current exceeding the rated value. The transformer has protections ensuring it can be considered intrinsically safe in case of failure. Another failure mode is related to the vibrations produced during normal operation, which can cause attachment screws to be loosened causing the risk of nearby components being impinged (e.g. the PC).
- Lifter - A crank connected to a hydraulic fluid circuit is used to lift the scanner unit while adjusting the stabilizing feet. Situations worthy of attention occur only in the event of oil leaks.
- Wheels and rubber feet - Since they have to withstand a heavy load, both the wheels and the feet may wear out or come loose, causing the device to become less stable. In addition, the wheels may jam and cause the device to tip over during transport due to the presence of loose cables (such as the power supply cord). In the latter case, mechanical tests have demonstrated that the wheels can overcome an obstacle, thus reducing the probability of the machine tipping over.
- Signal Input/Output ports - Interference signals, such as voltage or current, can enter from the USB and HDMI ports, through which the device can be connected to external devices, such as another PC. This failure mode has a low RPN because immunity to these disturbances was analysed and verified during EMC testing.
- Main power supply - As the power cord is located outside the device, it can often be subject to mechanical stress such as bending, pulling and crushing, which can lead to a change in impedance or an interruption of the power supply to the load. In addition, damage to the insulation may cause electrical shocks due to contact with bare wires. This element was designed to be heavy duty and to withstand the stresses listed above, so the resulting RPN is low. The risk of electric shock from contact with a just-disconnected plug was also low, because of proper component design. The problem of the transmission of a voltage and/or frequency fluctuation from the mains to the load has yet to be addressed.
- Foot switch - This component can encounter two contrasting failure modes: the disconnection of the cable and the failure to control the beam emission because of a

jammed pedal or a short circuit. In the first case, the RPN is low. In fact, if the cable is already disconnected before the acquisition, no unwanted emission can occur. However, if it is disconnected during the acquisition, the X-ray emissions are immediately stopped. If there is a short circuit and the pedal is pressed continuously before the acquisition, the software signals an unwanted activation of the beams. If this fault mode occurs during the scan, the emergency stop button can be used to intervene.

- PC - The first failure mode identified is the PC overheating, due to both prolonged use and the heat transmitted by adjacent components such as the transformer. The risk is that excessive heat can damage internal components (such as boards, memories, etc.), resulting in data loss. The PC has been located so that it will dissipate heat towards the outside. Moreover, once a certain operating temperature has been exceeded, it goes into thermal alarm. Nevertheless, the operator cannot monitor PC status. Another risk identified is the failure of one of the hard drives, due to the shocks and vibrations that the device suffers for example during transport. In this case, the RPN value decreases due to the implementation of mirroring, as seen in section B6.

3) SUBSYSTEM 3: PATIENT SUPPORT BED

- Motors - The probability of a malfunction of one of the four motors is very low. If there is a failure, the risk for the patient is limited. This is because the low height of the bed makes it easy to descend from it and because the patient can be manually withdrawn from the inside of the gantry. If the bed drops suddenly, the descent of the leg support is considered less serious than that of the backrest.
- Brakes - The bed braking system can only be activated manually. Therefore, it is possible that during normal use one or more wheels might not be braked either because the operator forgot it or because the brake was disengaged involuntarily. With regard to this latter case, the position of the front brakes, which are longitudinal to the seat, has been deemed hazardous since a patient could trip over or step on them while sitting down or getting up from the bed. This could have negative consequences for the user and/or the machine.
- Support bed (cushion) - An initial failure mode involves exceeding the bed's maximum load (200 kg), beyond which the bed could deform and flex excessively. Another failure mode is the presence of accessible metal parts, such as the armrest attachment bars. Regardless, this risk was considered low, since the manufacturer has declared that this electromedical equipment conforms to Class I after carrying out the tests required by the standard. Finally, how the presence of the support bed might affect the acquisition of images was evaluated in terms of beam attenuation. The risk lies in having to increase the emission parameters to compensate for the decreased energy of the beam, adding to the dose delivered to the patient.
- Foot switch: - As with the scanner unit foot switch, the possibility that one of the buttons gets stuck or is held down unintentionally has been considered. This could cause an uncontrolled movement of the bed. The risk is of entrapment or general injury to the patient, who might strike the scanner unit or fall to the floor. This failure mode was considered very critical, due to the absence of an emergency stop button for the bed.
- Control box - A failure mode reported by the supplier concerns the sudden shutdown of the control unit for the motors when used in the presence of other equipment, either electromedical or not.

B. IDENTIFICATION OF THE RISK ACCEPTANCE THRESHOLD

The RPN values obtained for each failure mode were used to identify the risk acceptance threshold, using the Scree Plot technique and the Pareto Diagram (Section B5).

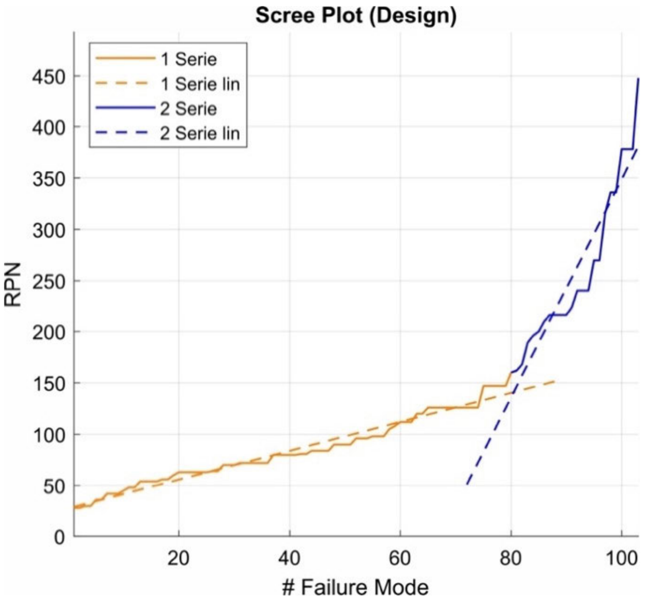

FIGURE 7. Scree plot of the FMECA Design. The intersection of the two lines corresponds to an RPN = 141.

The chart in Figure 7 was obtained by sorting the RPN values in ascending order. It was decided to qualitatively identify the point at which the slope variation occurs because the method would have been too conservative through the calculation of the maximum of the second derivative. The point of intersection of the two lines that approximate the two trends corresponds to an RPN of 141.

Instead, by using the 70-30% system Pareto Diagram, the RPN threshold value that delimits the failure modes that contribute 70% of the total RPN was 105 (Figure 8).

As can be seen, the Pareto Diagram provided a lower RPN value, thus being less conservative than the Scree Plot.

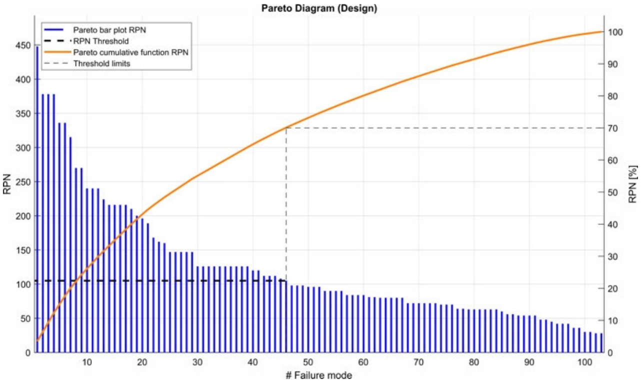

FIGURE 8. **Pareto Diagram of the FMECA Design. The threshold was identified as RPN = 105.**

As mentioned above, it was decided to maintain both thresholds by establishing a higher failure mode intervention priority to the failure modes trespassing both thresholds. Beyond the intervention priority, risk acceptability and therefore the need to implement an appropriate countermeasure is established by the lowest threshold identified by the two methods.

In the FMECA Design, 46 out of 103 failure modes were found unacceptable (29 with high priority and 17 with low priority). This means that nearly 50% of the failure modes require some sort of corrective action.

In light of these results, the following aspects were found to be a part of the failure modes considered unacceptable:

- Sensitivity to voltage fluctuations from the power grid.
- Sensitivity to disturbances introduced by external equipment, especially operating in the RF range.
- Progressive deterioration of the components.
- Hazards arising from the introduction of the new patient support bed in the machine design, related to its management, its handling and its positioning with respect to the scanner unit.

The highest RPN values were obtained from mechanical and usability risks, including activities related to the use and maintenance of the device. These results were in line with reports found on the FDA website and in articles from the literature [34], [35], [37], where special attention was given to the risks arising from proper patient centring.

More electrical and electronic hazards were identified in this analysis compared to the literature in the MAUDE history and database. This was probably due to external factors, such as the environmental conditions of transport and storage, rather than to poor design or low quality of the components.

C. RISK MITIGATION

To lower the risk priority index for those failure modes above the threshold, countermeasures were proposed. Some countermeasures were applied and their validity tested. The producing Company undertakes to implement the others in future developments of the device.

Several types of risk mitigation actions were identified as summarised below:

- Design changes, consisting of an improvement in the quality and performance of existing components or the introduction of new ones.
- Introduction of monitoring tools, such as sensors and transducers, to improve fault diagnostics.
- Changes to the software, enabling to easier user interface with the machine thus avoiding errors linked to its use.
- Quality Assurance (QA) procedures, to be implemented when the device is installed.

It is possible that some countermeasures could generate new risks not considered in the previous assessment. Their risk indices were calculated as well and assessed to be acceptable, to confirm that the introduced safety measures brought benefits.

Below is a list of the failure modes identified in the FMECA Design and their corrective actions. The first step was to describe the failure modes belonging to the category with RPN over both thresholds (RPN $\geq$ 141), being those that require a more urgent mitigation. A distinction was made between the countermeasures proposed and those actually applied.

- Power supply failure (RPN = 147) - These components will be replaced with medical switching power supplies, which provide a higher degree of isolation. In addition, as concerns protection against electromagnetic interference, there must be compliance with the latest edition of IEC 60601-1-2 [13]
- Intermittent operation of the rotation motor (RPN = 240) - Any uneven rotation of the motor can be diagnosed by the frequency change of the trigger signal used to control the X-ray emissions. To avoid uncontrolled emissions, which could cause patient overexposure, a peak counter could be implemented. If this counter detects an acceleration of gantry rotation during a scan, it will send a feedback signal to the motor to stop its operation.
- Interruption of the signal transmission during a scan (RPN = 240) - The idea is to implement a digital timestamp to record any delay between two successive samples. If the response from a certain component does not arrive before a pre-set time interval, it may indicate a malfunction of that component, so the acquisition will be interrupted.
- Fluctuations in mains voltage and frequency (RPN = 448) and failure of X-ray electronics boards (RPN = 378) - These two fault modes are grouped together because the main cause of the malfunction of these boards has been identified in possible mains voltage fluctuations. To avoid the risk of malfunction in the radiological image chain, it has been suggested to insert two components upstream of the load: a voltage stabilizer, to eliminate fluctuations, and a booster, a sort of transformer, to guarantee the required mains voltage.

- Cathode degradation (RPN = 196) - The degradation of the cathode filament can be controlled by monitoring the load state of the monobloc using a pulse counter. When this count exceeds a certain threshold, the operator must be alerted so that the component can be serviced.
- Glycol leakage from the chiller (RPN = 240) - Coolant level can be kept under control using a flowmeter to monitor the flow rate of the fluid entering and leaving the tank, diagnosing any leakage. In addition to this, the procedures should provide that the tank level be checked periodically.
- Failure of the collimator blades (RPN = 224) - It has been suggested to periodically perform a a test to verify the correct positioning of the blades (e.g. every week). This test consists in verifying that each of the four blades is perfectly aligned with the sides of a square figure of various sizes, which can be set in the software.
- Degradation of the flat panel sensors (RPN = 162) - The increase of the so-called "dark current", already described in the results, and the appearance of "dead pixels" in the image, can only be countered by appropriate QA procedures, which require, depending on the workload, a periodical replacement of the sensor.
- Emergency stop button not disengaged (RPN = 315) - It should be provided that after use the Emergency stop button must be reset to its initial state, to avoid making the machine unusable in case of emergency. This mitigation intervention is only possible through operator training.
- Emission Warning Lamp Failure (RPN = 216) - A daily self-test procedure could be provided for to verify that the lamp is working.
- PC Overheating (RPN = 270) - To keep the PC temperature under control and to avoid data loss, a warning can be shown on the screen, a few degrees before the PC triggers a thermal alarm.
- Bed foot switch failure (RPN = 216) - Because it should be possible to block any motorised movement of the bed, the need to provide an emergency stop button for the patient bed has been assessed. To prevent the bed emergency stop button from being confused with those for the scanner unit and create a new risk, mode of activation should be differentiated. Since the scanner unit emergency stop buttons are positioned at the top and can therefore be operated by hand, the new button should be positioned on the bed base, so that it can be activated easily with the operator's foot.

So far, a series of proposed corrective actions have been listed; their effectiveness lies in the fact that they would bring the RPN value below the acceptability threshold.

Below, the countermeasures actually applied are described:

- Oil leakage from the hydraulic lifting circuit (RPN = 336) - The previous lifting system has been replaced by simple, pedal-operated mechanical levers. This system may introduce a new risk, i.e., that the scanner unit might tip over when pressure is applied to the lever. It was possible to ascertain the stability of the device through testing, which also assessed that this risk remains below the threshold of acceptability.
- Malfunction of the control unit (RPN = 336) - The bed supplier has equipped its control unit with a filter against external electromagnetic interference, resolving problems from malfunctions or uncontrolled motor movements.
- Unintentional release of the bed brakes (RPN = 200) - To prevent the brake pedals from being stepped on by the patient while sitting down or getting up from the bed, the supplier was asked to change their orientation from longitudinal to lateral.

Some of the corrective actions described above also affect the mitigation of some failure modes with RPN between the thresholds ($105 \leq \text{RPN} < 141$), since they concern the same component. Those failure modes still requiring mitigation but that have not yet been considered are as follows:

- Incorrect positioning of the aluminium filters (RPN = 126) - Even here a timestamp can be implemented to monitor filter position over time.
- Laser misalignment (RPN = 126) - Laser alignment must be inspected visually each time the device is switched on. If the two laser beams are not orthogonal to each other, maintenance must be carried out by facility technicians.
- Excessive vibration of the isolation transformer (RPN = 126) - The insertion of shock absorbing support brackets, which will reduce the noise emitted and the risk of loosening the screws, has been foreseen.
- Loosening of the scanner unit wheels (RPN = 112) - The risk of the loss of stability due to the loosening of one of the four wheels can be avoided by verifying that they are correctly attached when the device arrives at the facility.

Considering the proposed mitigations, new S', O' and D' values were assigned and consequently the new RPN' product was calculated. As can be seen from Figure 9, all RPN' values (shown in green) lie below both the most conservative and the least conservative acceptability thresholds.

Even the Pareto diagram shows that previously unacceptable RPNs are now below both thresholds. In particular, the yellow curve represents the cumulative RPN' value, normalised with respect to the sum of the pre-mitigation RPNs: clearly, the total of the RPNs' is more than halved compared to the total RPNs (Figure 10).

IV. DISCUSSION OF THE RESULTS

Once the FMECA Design analysis has been completed on the device prototype, it was found that the most critical issue concerned the electrical part. This especially includes current spikes and fluctuations around the nominal values. If these variations are not properly managed, they could compromise the proper functionment of the heart of the device, i.e., the radiological image chain.

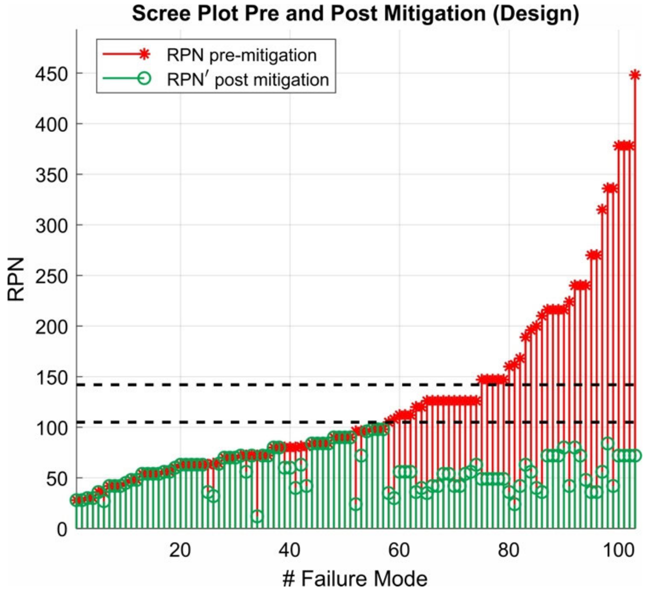

FIGURE 9. Pre-mitigation (red) and post-mitigation (green) Scree plots. All post-mitigation failure modes were lower than both acceptability thresholds.

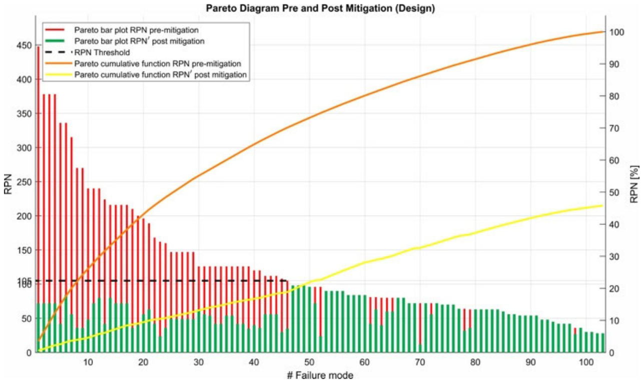

FIGURE 10. Pre- and post-mitigation Pareto Diagrams. The yellow curve shows the weight of the cumulative RPN′ value on the previously calculated value.

It should be pointed out that the risk assessment of two devices to be assembled, such as the CT scanner and patient bed, is much longer and more demanding than an integrated design risk assessment. At the conclusion of the analysis, countermeasures were proposed to lower the risk priority index for those failure modes that were found to be above the threshold.

Following the introduction of some of these mitigations, all the RPN' values, calculated with the new S', O' and D' values, were below both previously determined acceptability thresholds. It became necessary to assess the residual risk resulting from these countermeasures. Part of the residual risks were so low that they did not need to be mitigated, while others, greater in magnitude, could still be considered acceptable because of the associated benefits and because their reduction was not practical. In conclusion, no risk has remained unacceptable and the introduced mitigations have not generated new hazardous situations.

Among the residual risks that could not be completely eliminated there were the consequences of being exposed to X-ray emissions. The most infamous risk is the formation of tumours as a result of genetic mutations potentially induced by the ionising power of X-rays. In accord with the ALARP principle, the presence of ionising radiation in the human body is considered acceptable because of the benefits of using X-rays for biomedical imaging. Therefore, operator training is fundamental. This will enable them to avoid repeated and prolonged exposure, which could reduce the advantages of using this diagnostic technique.

V. CONCLUSION

This paper illustrates how a complete risk management system ought to be implemented when designing a new medical device. This management system must be in compliance with the existing legislative framework. When the device is marketed, all risks, including those of failure or harm to patient and caregiver, must have been identified, evaluated and minimized through careful evaluation work, using appropriate instruments and methods. Analysis using the FMECA method has proved to be a valid technique for the achievement of this purpose. Because of its modular structure, both the most critical components of a CT scanner using CBCT technology and the activities that can lead to a greater number of errors during the device life cycle, can be highlighted.

A methodologically well-conducted analysis leads to consistent results. These results, in accordance with the principle of device life cycle management, can also be used to verify the safety and effectiveness of devices already on the market and to draw inspiration for the design of new devices.

A weak point of the FMECA approach is its inability to analyse the interrelations between failure modes. This can be addressed by performing some complementary analysis with more techniques.

This research work has also provided useful indications for the achievement of the essential safety requirements demanded by the European Medical Devices Regulation 2017/745/EU, needed to obtain the CE mark, and by the United States regulations for FDA approval 510(k). The analysis performed, and the results obtained have been included in the Risk Management File (RMF). This is the document where the activities, documentation and records relating to risk management are tracked. The RMF is attached to the device's technical file once it can be marketed.

The work has proved that ''Design FMECA'' is a valid tool to assess the risks of complex medical devices, at design stage, in order to achieve the highest levels of safety and security required by the current standards and regulations. Further works will apply a similar method (Process FMECA) to investigate the risks related to the whole process of using the device.

REFERENCES

[1] C. Richmond, ''Sir godfrey hounsfield,'' *Brit. Med. J.*, vol. 329, p. 687, 2004, doi: 10.1136/bmj.329.7467.687.

[2] RadiologyInfo.org. *Radiation Dose in X-Ray and CT Exams*. Accessed: Jul. 2019. [Online]. Available: https://www.radiologyinfo.org/en/pdf/safety-xray.pdf

[3] W. A. Kalender, *Computed Tomography: Fundamentals, System Technology, Image Quality, Applications*, 3rd ed. New York, NY, USA: Wiley, 2011.

[4] W. A. Kalender, A. Polacin, and C. Süss, ''A comparison of conventional and spiral CT: An experimental study on the detection of spherical lesions,'' *J Comput. Assist. Tomogr.*, vol. 18, no. 2, pp. 167–176, Mar./Apr. 1994.

[5] L. Lechuga and G. A. Weidlich, ''Cone beam CT vs. Fan beam CT: A comparison of image quality and dose delivered between two differing CT imaging modalities,'' *Cureus*, vol. 8, no. 9, 2016.

[6] J. A. Carrino, ''Dedicated cone-beam CT system for extremity imaging,'' *Radiology*, vol. 270, no. 3, pp. 816–824, 2014.

[7] A. M. Luke, K. P. Shetty, S. V. Satish, and K. Kilaru, ''Comparison of spiral computed tomography and cone-beam computed tomography,'' *J. Indian Acad. Oral Med. Radiol.*, vol. 25, no. 3, pp. 173–177, Jul./Sep. 2013.

[8] European Commission. *The new Regulations on Medical Devices: Regulation (EU) 2017/745*. Accessed: May 2019. [Online]. Available: https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en

[9] *US Food & Drug Administration Website*. Accessed: May 2019. [Online]. Available: https://www.fda.gov/

[10] U. Food and D. Administration. *Federal Food, Drug, and Cosmetic Act (FD&C Act)*. Accessed: May 2019. [Online]. Available: https://www.fda.gov/regulatoryinformation/lawsenforcedbyfda/federalfooddrugandcosmeticactfdcact/default.htm

[11] U. S. Governement. *Code of Federal Regulations*. Accessed: May 2019. [Online]. Available: https://www.govinfo.gov/help/cfr

[12] *Medical Electrical Equipment—Part 1: General Requirements for Basic Safety and Essential Performance*, Standard IEC 60601-1, 2007.

[13] *Medical Electrical Equipment—Part 1–2: General Requirements for Basic Safety and Essential Performance—Collateral Standard: Electromagnetic Disturbances—Requirements and Tests*, Standard IEC 60601-1-2, 2018.

[14] *Medical Electrical Equipment—Part 1–3: General Requirements for Basic Safety and Essential Performance—Collateral Standard: Radiation Protection in Diagnostic X-Ray Equipment*, Standard IEC 60601-1-3, 2009.

[15] *Medical Electrical Equipment—Part 2-44: Particular Requirements for the Basic Safety and Essential Performance of X-Ray Equipment for Computed Tomography*, Standard IEC 60601-2-44, 2011.

[16] *Medical Electrical Equipment—Part 2–54: Particular Requirements for the Basic Safety and Essential Performance of X-Ray Equipment for Radiography and Radioscopy*, Standard IEC 60601-2-54, 2011.

[17] *Evaluation and Routine Testing in Medical Imaging Departments—Part 3–5: Acceptance Tests—Imaging Performance of Computed Tomography X-Ray Equipment*, Standard IEC 61223-3-5, 2006.

[18] *Medical Devices—Part 1: Application of Usability Engineering to Medical Devices*, Standard IEC 62366-1, 2016.

[19] *Radiographic Equipment*, document FDA 21 CFR 1020.31, 2018.

[20] *Computed Tomography (CT) Equipment*, document FDA 21 CFR, 1020.33, 2011.

[21] *Fluoroscopic Equipment*, document FDA 21 CFR,1020.32, 2011.

[22] *Diagnostic X-Ray Systems and Their Major Components*, document 1020.30 2011, FDA 21 CFR, 2018.

[23] *Medical Devices—Application of Risk Management to Medical Devices*, (in Italian), document UNI CEI EN ISO 14971:2012, 2013.

[24] S. Sklet, ''Comparison of some selected methods for accident investigation,'' *J. Hazardous Mater.*, vol. 111, n. 1-3, pp. 29–37, 2004, doi: 10.1016/j.jhazmat.2004.02.005.

[25] R. C. Fries, *Reliable Design of Medical Devices*. Boca Raton, FL, USA: CRC Press, 2017.

[26] Smart & Start Italia. *Homepage*. [Online]. Available: http://www.smartstart.invitalia.it/site/smart/home/eng.html

[27] *Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA)*, Standard IEC EN 60812, 2006.

[28] B. S. Dhillon, *Design Reliability-Fundamentals and Applications*. Boca Raton, FL, USA: CRC Press, 1999.

[29] H. de las Heras Gala, A. Torresin, A. Dasu, O. Rampado, H. Delis, I. H. Girón, C. Theodorakou, J. Andersson, J. Holroyd, M. Nilsson, S. Edyvean, V. Gershan, L. Hadid-Beurrier, C. Hoog, G. Delpon, I. S. Kolster, P. Peterlin, J. G. Roca, P. Caprile, and C. Zervides, ''Quality control in cone-beam computed tomography (CBCT) EFOMP-ESTRO-IAEA protocol (summary report),'' *Physica Medica*, vol. 39, pp. 67–72, 2017, doi: 10.1016/j.ejmp.2017.05.069.

[30] R. Bell and D. Reinert, ''Risk and system integrity concepts for safety-related control systems,'' *Microprocessors Microsyst.*, vol. 17, no. 1, pp. 3–15, 1993, doi: 10.1016/0141-9331(93)90088-O.

[31] R. E. Melchers, ''On the ALARP approach to risk management,'' *Rel. Eng. Syst. Saf.*, vol. 71, no. 2, pp. 201–208, 2001, doi: 10.1016/S0951-8320(00)00096-X.

[32] M. Jones-Lee and T. Aven, ''ALARP-What does it really mean,'' *Rel. Eng. Syst. Saf.*, vol. 96, no. 8, pp. 877–882, Aug. 2011, doi: 10.1016/j.ress.2011.02.006.

[33] US Food & Drug Administration. *MAUDE—Manufacturer and User Facility Device Experience*. Accessed: Dec. 17, 2019. [Online]. Available: https://www.fda.gov/medical-devices/mandatory-reporting-requirements-manufacturers-importers-and-device-user-facilities/manufacturer-and-user-facility-device-experience-database-maude

[34] Statista. *Number of Computer Tomography (Ct) Scanners in Selected Countries as of 2017 (Per Million Population)*. Accessed: Dec. 17, 2019. [Online]. Available: https://www.statista.com/statistics/283085/computer-tomography-examinations-in-selected-countries/

[35] A. Pandey, M. Singh, A. U. Sonawane, and P. S. Rawat, ''FMEA based risk assessment of component failure modes in industrial radiography,'' *Int. J. Eng. Trends Technol.*, vol. 39, no. 4, pp. 216–225, 2016, doi: 10.1155/2013/763186.

[36] A. Petrillo, R. Fusco, V. Granata, S. Filice, N. Raiano, D. M. Amato, M. Zirpoli, A. di Finizio, M. Sansone, A. Russo, E. M. Covelli, T. Pedicini, and M. Triassi, ''Risk management in magnetic resonance: Failure mode, effects, and criticality analysis,'' *Biomed Res. Int.*, vol. 2013, Sep. 2013, Art. no. 763186, doi: 10.1155/2013/763186.

[37] S. Broggi, M. C. Cantone, A. Chiara, N. Di Muzio, B. Longobardi, P. Mangili, and I. Veronese, ''Application of failure mode and effects analysis (FMEA) to pretreatment phases in tomotherapy,'' *J. Appl. Clin. Med. Phys.*, vol. 14, no. 5, pp. 265–277, 2013, doi: 10.1120/jacmp.v14i5.4329.

[38] M. C. Cantone, M. Ciocca, F. Dionisi, P. Fossati, S. Lorentini, M. Krengli, S. Molinelli, R. Orecchia, M. Schwarz, I. Veronese, and V. Vitolo, ''Application of failure mode and effects analysis to treatment planning in scanned proton beam radiotherapy,'' *Radiat. Oncol.*, vol. 8, no. 1, 2013, doi: 10.1186/1748-717X-8-127.

[39] J. Kim, B. Miller, M. S. Siddiqui, B. Movsas, and C. Glide-Hurst, ''FMEA of MR-only treatment planning in the pelvis,'' *Adv. Radiat. Oncol.*, vol. 4, no. 1, pp. 168–176, 2019, doi: 10.1016/j.adro.2018.08.024.

[40] E. Thornton, O. R. Brook, M. Mendiratta-Lala, D. T. Hallett, and J. B. Kruskal, ''Application of failure mode and effect analysis in a radiology department,'' *Radiographics*, vol. 31, no. 1, pp. 281–293, 2011, doi: 10.1148/rg.311105018.

[41] M. Casamirra, F. Castiglia, M. Giardina, and E. Tomarchio, ''FMECA Analyses of radiological over-exposure accident to patients in brachytherapy,'' presented at the 13th Int. Congr. Int. Radiat. Protection Assoc., Glasgow, Scotland, 2012.

[42] Z. Bluvband, P. Grabov, and O. Nakar, ''Expanded FMEA (EFMEA),'' in *Proc. Annu. Symp. Rel. Maintainability (RAMS)*, 2004 pp. 31–36, doi: 10.1109/RAMS.2004.1285419.

[43] N. Sellappan, D. Nagarajan, and K. Palanikumar, ''Evaluation of risk priority number (RPN) in design failure modes and effects analysis (DFMEA) using factor analysis,'' *Int. J. Appl. Eng. Res.*, vol. 10, no. 14, pp. 34194–34198, 2015.

[44] F. Lopez, C. Di Bartolo, T. Piazza, A. Passannanti, J. C. Gerlach, B. Gridelli, and F. Triolo, ''A quality risk management model approach for cell therapy manufacturing,'' *Risk Anal.*, vol. 30, no. 12, pp. 1857–1871, 2010.

ERNESTO IADANZA (SM'07) received the B.M.E., C.E., M.Sc., and Ph.D. degrees. He is currently an Adjunct Professor in clinical engineering with the Department of Information Engineering, University of Florence. He is also a member of the IFMBE Administrative Council, the Chairman of the International Federation for Medical and Biological Engineering/Health Technology Assessment Division Board (IFMBE/HTAD), the Immediate Past Chairman of the Clinical Engineering Division Board (IFMBE/CED), and the Immediate Past Chairman of the International Union for Physical and Engineering Sciences in Medicine / Education and Training Committee (IUPESM). He is a Supervisor of more than 160 graduation theses. He is author of more than 145 publications on international books, scientific journals, volumes, and conference proceedings. He is an IEEE-EMBS Senior Member and received the IBM Faculty Award, in 2013. He is a member of the scientific committee, and a Track Chair and a Session Chairman of national and international scientific conferences in biomedical engineering. He is an Associate Editor of *Health and Technology* and *Future Internet*, a Section Editor of the *International Journal of Clinical Engineering and Healthcare Technology Assessment* (CEHTA), and a member of the Editorial Board of *China Medical Devices Journal* and *Journal of Healthcare Engineering*. He is a Guest Editor for the journal *Health and Technology* (Special issue: Global issues in Clinical Engineering). He has been an Organizer of postgraduate and postmaster courses in clinical engineering, healthcare engineering, and HTA at the University of Florence, since 2007.

DILETTA PENNATI received the M.S. degree in biomedical engineering from the University of Florence, in 2019, where she is currently pursuing the degree in biomedical engineering. She is a coauthor of a book chapter edited by Springer, in 2017.

LEONARDO MANETTI received the M.Sc. degree in biomedical engineering from the University of Florence, Italy, in 2008. He is currently the Research and Development Director of a biomedical imaging company.

LEONARDO BOCCHI received the M.S. degree in electronic engineering from the University of Florence, Italy, in 1993, and the Ph.D. degree in biomedical engineering from the University of Bologna, in 1997. He is currently an Associate Professor in biomedical engineering with the University of Florence. He is author of more than 100 publications in biomedical engineering. He is a member of the IEEE TC on Cardiovascular Systems, a Project Evaluator, and a reviewer for the EU and national projects. He acts as referee for several international journals (among others, IEEE TMI, IEEE TBME, *Pattern Recognition*, *Signal Processing*, and *Biomedical Signal Processing and Control*) and participated, under different roles, to the organization of various conferences (EuroGP and EvoWorkshops, ACIVS, MAVEBA, and Interspeech).

MONICA GHERARDELLI received the M.S. degree in electronic engineering from the University of Florence, Italy, in 1981, and the Ph.D. degree in information engineering from Padua University, Italy, in 1987. She is currently a Professor with the University of Florence and scientific responsible of agreements between the Information Engineering Department of the University of Florence and University Hospitals in Tuscany, Italy. She is author of articles in the biomedical engineering field.