IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 15, 2021, accepted September 27, 2021, date of publication October 4, 2021, date of current version October 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3117703

Fuzzy FMECA Process Analysis for Managing the Risks in the Lifecycle of a CBCT Scanner

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

[1]Department of Information Engineering, University of Florence, 50139 Florence, Italy
[2]Epica Imaginalis, 50019 Sesto Fiorentino, Italy

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

ABSTRACT The *Failure Mode, Effects, and Criticality Analysis* (FMECA) is one of the risk analysis techniques proposed by the ISO 14971 Standard. This analysis allows to identify and assess the consequences of faults that affect each component of a complex system. The FMECA is a forward-type technique used for highlighting critical points and classifying them by priority. It also makes it possible to evaluate the extent of failures by means of numerical indices. It can be applied to a product or to a work process. In the latter case we talk about Process-FMECA. The application of the Process-FMECA to bioengineering is of particular interest because this procedure provides an analysis related to risk management during all the different phases of the medical device life cycle. However, practical applications of this method have revealed some shortcomings that can lead to inaccuracies and inconsistencies regarding the risk analysis and consequent risk prioritization. This paper presents an example of application of a Fuzzy Process-FMECA, an improved Process-FMECA based on fuzzy logic, to a small computerized tomography (CT) device prototype designed for studying the extremities of the human body. This prototype is a CT device that uses the *Cone Beam* CT (CBCT) technology. The Fuzzy Process-FMECA analysis has made it possible to produce a table of risks, that are quantified according to the specifications of the method. The analysis has shown that each phase or activity is fundamental to guarantee a correct functioning of the device. The methodology applied to this specific device can be paradigmatic for analyzing the process risks for any other medical device.

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

I. INTRODUCTION

According to the World Health Organization, medical devices are defined as:

> ''any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of:
> - diagnosis, prevention, monitoring, treatment or alleviation of disease,
> - diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
> - [...]
>
> and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means.'' [1]

The design of medical devices must include, according to the main worldwide regulatory frameworks, a risk management process aimed to identify, assess and mitigate the risks associated with their use. The applicable international standard is the ISO 14971:2019 ''Medical devices - Application of risk management to medical devices'' [2]. This standard specifies a procedure that allows manufacturers to identify the hazards associated with medical devices (including *in vitro* diagnostic medical devices), estimate and evaluate the associated risks, control these risks, and finally monitor the effectiveness of controls. The requirements of the standard apply to each phase of the whole medical device life cycle.

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

A specific ''Medical devices — Guidance on the application of ISO 14971'' [3] proposes various risk analysis techniques, which are not mutually exclusive, but can sometimes be applied in a complementary way. Some techniques are more suitable in the prototyping phase while others require a deeper knowledge of the behavior of the device during its life cycle. A list of these techniques, suggested by the standard and most commonly used in the field of medical devices, is reported below:

- Preliminary Hazard Analysis (PHA)
- Fault Tree Analysis (FTA)
- Failure Mode and Effects Analysis (FMEA) / Failure Mode, Effects and Criticality Analysis (FMECA)
- Hazard and Operability Study (HAZOP)
- Hazard Analysis and Critical Control Point (HACCP)

In this work, we present an analysis carried out on a prototype of a Cone Beam Computerized Tomography (CBCT) device, addressing the management of risks occurring during its use. The development of this device is part of a regional project, involving various subjects and companies in Tuscany (Italy), aimed at improving the image quality performance of CBCT technology, to bridge the performance gap with the more common spiral Computed Tomography, while maintaining the typical advantages of the technology, first of all portability. The device will have three possible functions:

- Digital Radiography (DR)
- Fluoroscopy (FL)
- Computed Tomography (CT)

The technological innovation of this project consists in a very small and compact CT unit, provided with wheels allowing easy movements between departments (for layout changes, temporary needs, or fragile patients). Furthermore, the project specifications are aimed at using the CBCT technology to reduce costs and improve simplicity, thus allowing a wide use in different kinds of facilities and health care structures.

The selected methodology is FMECA, as defined in the standard IEC 60812:2018 ''Failure modes and effects analysis (FMEA and FMECA)'' [4]. While FMEA is a qualitative analysis, FMECA involves quantitative values, adding an evaluation path that helps to take coherent operational decisions. Despite the difference, FMEA and FMECA acronyms are often used interchangeably. In this paper we refer exclusively to FMECA. FMECA has many advantages over other methodologies, such as: ease of application, ability to study complex units in detail, suitability for both the design and the management of a system, possibility of updating in case of identification of new fault events. Numerous applications of this technique to innovative industrial technologies can be found in FMECA literature. It has been recently presented as a technique extensively used for the design of protection systems in advanced technologies. For instance, in Selective Production of Exotic Species (an innovative plant for advanced nuclear physic studies), very high vacuum conditions together with appropriate safety systems to storage exhaust gases are required to avoid radiological risk for operators and people [5]. In this case, the Fuzzy FMECA method has been applied to a preliminary design of a high activity gas recovery system to rank with a modified Fuzzy Risk Priority Number the most critical components in terms of failures and human errors. Fuzzy FMECA has also been used to perform a reliability evaluation of continuous emission monitoring system (CEMS), an on-line analyzer system applied in many engineering fields such as natural gas purification plants, thermal power plants and cement plants [6]. Whereas the integrated application of FMECA and HAZOP methodologies has been applied to a safety analysis to determine possible accidental events in the storage system used in the liquefied natural gas regasification plant [7]. Efforts have also been made to automate the FMECA process for complex cyber-physical systems [8]. Composed of numerous interconnected subsystems, each designed to perform specific functions, these systems are employed in critical applications, where identifying the faults and assessing their effects on the overall system becomes mandatory. The FMECA is a safety technique also used in medical applications. A new FMECA method based on fuzzy logic was applied to potential radiological over-exposure of patients during high-dose-rate brachytherapy treatments [9]. Fuzzy FMECA has been used in a variety of fields, including electronics, in particular in semiconductors and in electronic devices and agriculture (for example in paddy fields and edible bird nest), as mentioned in [10].

Although FMECA is a predictive technique, it can be applied retrospectively on a product or work process to determine their critical points and assess their severity. These are respectively referred to as Design-FMECA and Process-FMECA (P-FMECA). Indeed, the object of observation, objectives and technical equipment used in the analysis of fault/failure mode change from one analysis to the other. In P-FMECA the objective is to reduce the risk of defects/errors in a good or service as a result of actions or activities that are poorly performed or not performed at all, during the production/delivery process [11], [12]. The analysis takes proactively into consideration all possible errors of the process execution, thus suggesting the insertion of tests and checks, the development of procedures and countermeasures such as instructions for use and management of complaints. The P-FMECA began to be used in the sixties of the last century in the aerospace industry [13]; it was then adopted in the early 2000s in healthcare, starting from obstetrics-gynecology [14] and emergency departments [15], [16] [17]. It is also worth noting that in recent years, the FMEA/FMECA method has been extensively applied in the field of advanced radiotherapy services. The goal is to improve safety and system control while simultaneously reduce errors that can occur during the steps of different treatments. More precisely, Healthcare Failure Mode and Effect Analysis (HFMEA) has been used to perform a proactive analysis of radiotherapy patient record systems in a large public hospital [18] and it has been reviewed in its application to radiotherapy processes [19]. Another example of application

is the FMEA approach used to assess the potential risks for patients during the delivery of tomotherapy treatments [20]. This technique, when applied to healthcare, makes it possible to identify and treat the potential risks that affect the clinical-care processes [21]. P-FMECA can be listed among the proactive risk management tools, as it involves the analysis of a predefined process and the identification of possible defects or preventable errors (the so-called failure modes) by a multidisciplinary team, in order to attribute priorities for changes that can improve security.

Risk assessment is carried out through:

- standardization of the evaluation process;
- anchoring of the users' (both intermediate and final) points of view;
- use of multidisciplinary groups of experts.

In short, the P-FMECA methodological phases are:

- identification of the object of analysis (product/service, process, or parts or components thereof);
- identification / description of the connected activities;
- identification of failure / error modes;
- analysis and determination of the risk priority index;
- identification of (preventive / improvement / corrective) actions and measures for achieving the expected results.

The analysis that we describe in this paper produced a risk analysis table that considers the different tasks and, for each of these, the possible error modes due to both fully operative use and improper use of the product. The risks thus identified were quantified in accordance with the FMECA method, not lacking in shortcomings such as the failure to assign a value of relative importance to the risk factors, the strong dependency of the Risk Priority Number on the small variation of three parameters, and the difficulty in providing a precise value for these three parameters. These drawbacks were overcome with the fuzzy approach that gives a degree of importance to each factor, a more flexible structure for combining the risk parameters and the ability to handle in a consistent manner both qualitative and quantitative data.

II. METHODS AND TOOLS

A. THE RISK MANAGEMENT PROCESS

As already mentioned, the risk analysis chosen among those proposed in Appendix G of the ISO 14971 standard is the FMEA/FMECA. The reference standard for FMEA/FMECA analysis is IEC EN 60812:2018 [4] which describes and provides examples for approaching the study of failures affecting a complex system. The FMEA analysis is presented in the form of a table, in which the rows correspond to the possible failure modes for each component or item or task, while the columns indicate causes and effects of each identified fault. Its structure is described in Section II-B2. The FMECA analysis, an extension of the FMEA analysis, allows to quantify the entity of a specific fault through numerical indices. These indices, ranging from 1 to 10, represent:

- Severity (S) - it estimates how much the fault affects the system or the user. When the severity equals 1, the effect will be negligible, if it equals 10, irreparable damage to the component / system and / or serious consequences for humans can occur.
- Occurrence (O) - it estimates the probability of occurrence of a failure (1 if it is unlikely, 10 if it is very likely).
- Detectability (D) - it estimates the probability of identifying and possibly eliminating the adverse situation before it occurs, thus affecting the system and the user. Lower values indicate good probability of failure detection, while if this index is high it will be almost impossible to detect the failure.

The *Risk Priority Number* (RPN) is the product of these three indices:

$$RPN = S * O * D \tag{1}$$

It is a meaningful index, that gives a quantitative measure of the relative importance of risks. The aim is to keep it as low as possible for all the failure modes. A variation of the standard FMECA analysis can be applied to consider how failure modes can impact on several subjects; it is multidimensional, meaning that the value of S is assigned separately for the severity related to the effects on people (patient and operator, called *Sh*) and on the device (called *Sd*). The single index for Severity is generated by selecting the greater of these two.

Despite its numerous applications since the 1960s, as mentioned in Section I, FMECA has been criticized for a number of reasons [5], [9], [10], [22]–[27], some specific drawbacks are:

- Presence of gaps in the range of admissible RPN values,
- Relative importance among O, D and S is not taken into consideration,
- Same results of RPN with very different values of severity in failure modes,
- Human errors are not addressed in a manner consistent with human factors.

B. FUZZY FMECA

Important efforts have been made to overcome these shortcomings and improve the FMECA method. As such, fuzzy logic and consequently fuzzy set theory, proposed by Zadeh in 1965 [28], [29], provide an important tool for working directly with ambiguous or vague information that can be easily translated in linguistic variables during risk analysis: a fuzzy rule-based system. A criticality assessment based on fuzzy logic allows the experts to evaluate the risk associated with specific failure modes in a more natural way, giving a linguistic value to describe a risk factor rather than an exact number. The resulting Fuzzy FMECA has been widely used in the medical field [9], [10], [27], [30]–[32] and its overall rule-based system is shown in figure 1. To further highlight the advantages of a Fuzzy FMECA analysis with respect to the traditional one, a comparison between the two analyses has been made, as shown in table 1.

Before explaining the Fuzzy FMECA rule-based system, it is important to point out that the standard for FMEA/FMECA recommends some criteria for setting the levels of Severity, Occurrence and Detectability. Since these

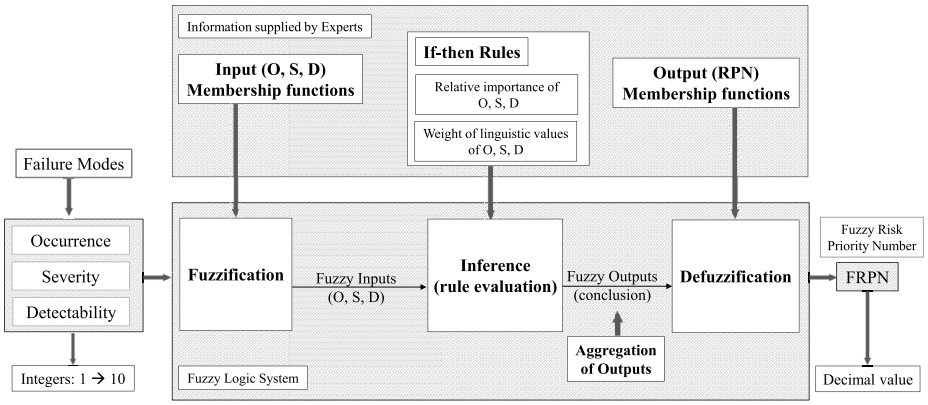


FIGURE 1. Overall procedure for the fuzzy FMECA rule-based system.

TABLE 1. Comparison between traditional FMECA analysis and fuzzy FMECA analysis.

Features of the analysis	FMECA	Fuzzy FMECA
The failure mode analysis yields also the criticality analysis	☒	☒
Addition of a qualitative measure of magnitude of a failure mode effect, the risk priority number	☒	☒
Prioritization possible for the mitigation offailure modes using the risk priority number	☒	☒
Different combination of risk factor values results in a different risk priority number	×	☒
Possibility ofincluding the relative importance of each risk factor	×	☒
Use oflinguistic values to better express risk factors and experience	×	☒
Decimal value for the risk priority number which decreases the presence of gaps in its range of admissible values	×	☒

criteria are not appropriate to the medical field, we adopted specific criteria obtained through an analysis of the literature in this field and adapted them to this application [33], [34] [35]. Section II-B3 describes this selection. Several criteria make it possible to establish the risk acceptance threshold, those applied in this work are described in the Section II-B4.

To apply a fuzzy ruled-based system to this risk assessment, the first step is the fuzzification of the inputs: it can be interpreted as the conversion of a crisp quantity to a fuzzy quantity. For this purpose, linguistic variables have been chosen to describe the levels of Severity, Occurrence and Detectability together with FRPN (Fuzzy RPN) as shown in tables 2 - 6 similarly to what done in a previous study reported in [9].

Since membership in a fuzzy set becomes a matter of degree, a function $\mu(x)$ will associate the degree of membership (a real number between 0 and 1) of a particular level of S (both *Sh* and *Sd*), O or D to the corresponding linguistic data. The most commonly used fuzzy numbers are triangular (a, b, c) or trapezoidal (a, b, c, d) [5], [9], [23], [24]. They are described by the following triangular and trapezoidal membership functions, respectively:

$$\mu(x) = \begin{cases} \dfrac{x-a}{b-a}, & a \le x \le b \\ \dfrac{x-c}{b-c}, & b \le x \le c \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

where $a < b < c$.

$$\mu(x) = \begin{cases} \dfrac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \dfrac{x-d}{c-d}, & c \le x \le d \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

where $a < b < c < d$.

The inputs of the Fuzzy FMECA rule-based system, Severity (both *Sh* and *Sd*), Occurrence and Detectability, together with the output of this system, named FRPN, have been decomposed into different fuzzy sets using these triangular and trapezoidal membership functions for each linguistic variable. Each risk factor function has a $1/2$ overlap, that is to say the height of intersection of each two successive fuzzy sets equals to $1/2$. Triangular membership functions with this kind of overlap have been frequently used in many applications [36]; the same overlap has been deemed appropriate for this particular case, in order to describe the uncertainty in participation of an element to different fuzzy sets. The resulting fuzzy linguistic variables are presented in figure 2.

In this first step, as described in [13], the input values for S, O and D are fuzzified by determining the value of the membership function corresponding to a particular input. This input will not be a single crisp value, instead we allow an interval of values to be given, since it is often difficult for experts to translate their experience into numbers, ranging from 1 to 10, that indicate exactly how the indices S, O and D describe the degree of risk for a particular failure mode. Values near the center of this interval are assumed

TABLE 2. Fuzzy FMECA scale for the severity related to the effects on the device (*Sd*) and their corresponding linguistic terms.

Severity (for device)	Fuzzy Linguistic number (a, b, c, d)	Weight	Criteria	Ranking
None (N)	(0, 0, 2, 3)	1/4 = 0.25	No effect on the device	1
Low (L)	(2, 3, 5, 6)	2/4 = 0.5	Minor effect on device performance	4
Moderate (M)	(5, 6, 8, 9)	3/4 = 0.75	Moderate effect on device performance	7
Hazardous (H)	(8, 9, 10, 10)	4/4 = 1	Serious effect on device performance	9

TABLE 3. Fuzzy FMECA scale for the severity related to the effects on people (*Sh*) and their corresponding linguistic terms.

Severity (for human) Linguistic value	Fuzzy Linguistic number (a, b, c, d) (a, b, c)	Weight	Criteria	Ranking
None (N)	(0, 0, 1, 2)	1/10 = 0.1	No injury to patient	1
Very Minor (VM)	(1, 2, 3)	2/10 = 0.2	No injury to operator	2
Minor (M)	(2, 3, 4)	3/10 = 0.3	Minor injury to operator that does not require treatment or patient or impossibility to perform the exam to the patient for few minutes	3
Very Low (VL)	(3, 4, 5)	4/10 = 0.4	Minor injury to patient that does not require treatment or impossibility to perform the exam to the patient for few hours	4
Low (L)	(4, 5, 6)	5/10 = 0.5	Minor injury to both patient and operator that does not require treatment	5
Moderate (M)	(5, 6, 7)	6/10 = 0.6	Moderate injuries requiring treatment or risk of useless exposure to x-rays	6
High (H)	(6, 7, 8)	7/10 = 0.7	Serious injuries but not permanent or risk of overexposure to x-rays	7
Very High (VH)	(7, 8, 9)	8/10 = 0.8	Very dangerous, long hospitalization with possible chronic outcomes or impossibility to perform the exam to the patient for several days	8
Hazardous with warning (HWW)	(8, 9, 10)	9/10 = 0.9	Extremely dangerous, permanent injuries or risk of an incorrect diagnosis	9
Hazardous without warning (HWOW)	(9, 10, 10)	10/10 = 1	Extremely dangerous, possible death	10

TABLE 4. Fuzzy FMECA scale for the occurrence and their corresponding linguistic terms.

Occurrence Linguistic value	Fuzzy Linguistic number (a, b, c, d)	Weight	Criteria	Ranking
Remote (R): failure is unlikely	(0, 0, 1, 2)	1/5 = 0.2	$P < 0{,}1\%$	1
Low (L): relatively few failures	(1, 2, 3, 4)	2/5 = 0.4	$0{,}1\% \leq P < 1\%$	2
			$1\% \leq P < 2\%$	3
Moderate (M): occasional failure	(3, 4, 6, 7)	3/5 = 0.6	$2\% \leq P < 5\%$	4
			$5\% \leq P < 7\%$	5
			$7\% \leq P < 10\%$	6
High (H): repeated failures	(6, 7, 8, 9)	4/5 = 0.8	$10\% \leq P < 15\%$	7
			$15\% \leq P < \%$	8
Very High (VH): failure is almost inevitable	(8, 9, 10, 10)	5/5 = 1	$20\% \leq P < 25\%$	9
			$P \geq 25\%$	10

TABLE 5. Fuzzy FMECA scale for the detectability and their corresponding linguistic terms.

Detectability	Fuzzy Linguistic number (a, b, c, d) (a, b, c)	Weight	Criteria	Probability of detection	Ranking
Almost certain (AC)	(0, 0, 1, 2)	1/10 = 0.1	Design/operation control will almost certainly detect a potential failure mode	91-100%	1
Very High (VH)	(1, 2, 3)	2/10 = 0.2	Very high probability of detection	81-90%	2
High (H)	(2, 3, 4)	3/10 = 0.3	High chance of detection	71-80%	3
Moderately High (MH)	(3, 4, 5)	4/10 = 0.4		61-70%	4
Moderate (M)	(4, 5, 6)	5/10 = 0.5	Moderate chance of detection (e.g. the defect will remain undetected until the device performance is affected)	51-60%	5
Low (L)	(5, 6, 7)	6/10 = 0.6		41-50%	6
Very Low (L)	(6, 7, 8)	7/10 = 0.7	Remote chance of detection (e.g. the defect will remain undetected until device inspection is carried out).	31-40%	7
Remote (R)	(7, 8, 9)	8/10 = 0.8		21-30%	8
Very Remote (VR)	(8, 9, 10)	9/10 = 0.9	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)	11-20%	9
Absolute Uncertain (AU)	(9, 10, 10)	10/10 = 1	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)	0-10%	10

to be "more certain" than those near the edges, while the width of the interval indicates the amount of uncertainty in the input. A triangular membership function is associated with this interval. As indicated in [9], to build it we assume that the "more certain" value is assigned by experts as the single value *b* (the top of the triangular membership function).

TABLE 6. Fuzzy FMECA scale for the fuzzy risk priority number and their corresponding linguistic terms.

FRPN	Fuzzy Linguistic number (a, b, c, d) (a, b, c)	Weight	Criteria	Ranking
Unnecessary (U)	(0, 0, 25, 75)	1/10 = 0.1	Almost unnecessary to take the follow-up actions.	1 – 50
Minor (M)	(25, 75, 125)	2/10 = 0.2	Minor effect on device performance	50 – 100
Very Low (VL)	(75, 125, 125)	3/10 = 0.3	Very Low priority to take the follow-up actions.	100–150
Low (L)	(125, 200, 300)	4/10 = 0.4	Low priority to take the follow-up actions.	150 – 250
Moderate (M)	(200, 300, 400)	5/10 = 0.5	Moderate priority to take the follow-up actions.	250 – 350
High (H)	(300, 400, 500)	6/10 = 0.6	High priority to take the follow-up actions.	350 – 450
Very High (VH)	(400, 550, 700)	7/10 = 0.7	Very High priority to take the follow-up actions.	450 – 600
Extremely High (EH)	(500, 650, 800)	8/10 = 0.8	Extremely High priority to take the follow-up actions.	600 – 800
Necessary (N)	(700, 800, 900)	9/10 = 0.9	Necessary to take the follow-up actions.	800 – 900
Absolutely Necessary (AN)	(800, 900, 1000 1000)	10/10 = 1	Absolutely Necessary to take the follow-up actions.	900 – 1000

In order to characterize the other two parameters, a and c (lower and upper bounds of the triangular membership function), a procedure based on the Gaussian probability density functions can be chosen, obtaining:

$$a = b - x(2\sigma) \tag{4}$$

$$c = b + x(2\sigma) \tag{5}$$

where σ is the standard deviation and $x(2\sigma) = 13.53\%$ of b [37]. In figure 3 an example of this fuzzification process is shown.

Once the fuzzification is complete, we begin the fuzzy inference, a process of mapping from a given input to an output using fuzzy logic, making use of membership functions, fuzzy logic operators and If-Then rules. A collection of If-Then rules maps from input fuzzy sets to output fuzzy sets, based on fuzzy logic principles [38]; the *If* part of the rule is called the antecedent and the *then* part is the consequent. In this fuzzy rule-based system, If-Then rules are defined by taking into consideration the relative importance of the input variables and the weight of the linguistic value of both the inputs and output. These are calculated by assuming the following linear hypothesis [5]:

$$W_O, W_D, W_{Sh}, W_{Sd}, W_{FRPN} = i/k \text{ with } i = 1, \ldots, k \tag{6}$$

where k is the number of linguistic variables that define O, S, D, and FRPN. The resulting values are presented in tables 2 - 6.

In the medical field, the severity of a failure mode should be more important than its occurrence or detectability. The severity of a consequence could result in an adverse clinical outcome [9]. The authors discussed with the designers and the technical service of the manufacturer, evaluating failures modes and analyzing the experience gained on similar devices already in production. As an outcome of this evaluation, it is possible to confirm that severity should deserve a slightly higher relative importance compared to occurrence and detectability, in accordance to the literature and in particular to what is discussed in [5]. For this reason, the relative importance of the S, O and D indices are respectively set as:

- $R_S = 0.4$, the same value is used for *Sh* and *Sd*
- $R_O = 0.3$
- $R_D = 0.3$

Note that these values are non-negative and sum of 1, they could also be based on the needs of the experts [5].

The linguistic variable of the FRPN output and the corresponding weight W_{FRPN} used within the formulated If-Then rules are identified using the following relationship [9]:

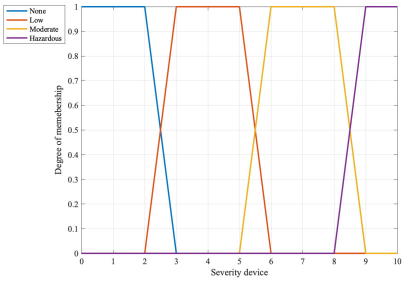
$$W_{FRPN} = R_O W_O + R_D W_D + R_S W_S \tag{7}$$

These W_{FRPN} values allow the identification of the linguistic term of FRPN output. For example, for a specific failure mode we could have the following rule:

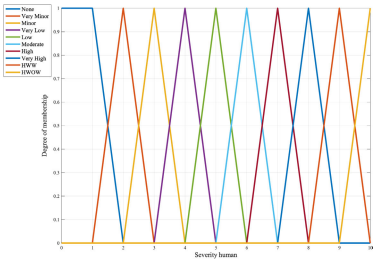
Rule: If the occurrence is **Low** (e.g.: $W_O = 0.4$) **and** the severity is **Moderate** (e.g.: $W_{Sd} = 0.75$, assuming Sd>Sh) **and** the detectability is **Very Low** (e.g.: $W_D = 0.7$), **then** the **risk** is **High** (e.g.: $W_{FRPN} = 0.3{*}0.4{+}0.4{*}0.75{+}0.3{*}0.7 = 0.63$). This value of W_{FRPN} is placed between 0.6 (High risk) and 0.7 (Very High risk). Being closer to risk **High**, the risk has been identified with this linguistic value.

The gathering of fuzzy rules is a known challenge when implementing Fuzzy FMECA, since a fuzzy rule can result incomplete, not monotone or inconsistent. These issues have been overcome by considering, for the gathering of rules, each combination of linguistic variables describing each risk factor once the "more certain" value is assigned by the experts. The resulting base rule describes the riskiness of the system for every combination of Severity, Occurrence and Detectability. These rules then need to be combined in a single fuzzy set. The min-max interference [38], [39] is frequently used in the literature to do this rule evaluation. It consists of determining the minimum rule antecedent, which is taken to be the truth value of the rule, then applying this truth value to all consequences of the rule. Essentially, this inference method starts with the selection of the minimum membership function value in *If* parts of each rule. Then, the fuzzy output is set to the maximum truth value of all the rules that include it as a consequent, which means that the final membership function value of the output is the aggregation (union) of the fuzzy sets assigned to that output. The aggregation of fuzzy output is completed with weight of W_{FRPN}.

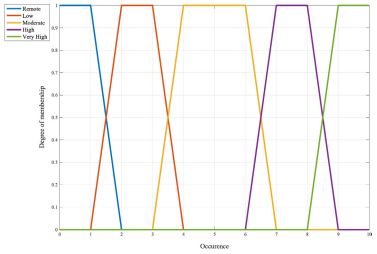
Note that for the operation on fuzzy sets, it has been suggested the minimum operator for the intersection and the maximum operator for the union of two fuzzy sets [29]. The fuzzy union and intersection of three fuzzy sets A, B, C on



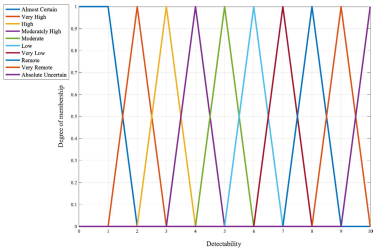
(a)



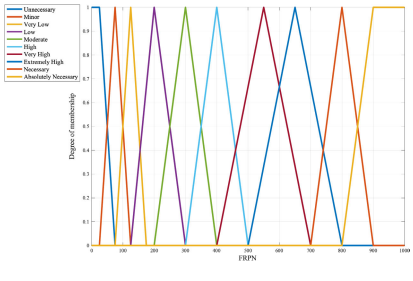
(b)



(c)



(d)



(e)

FIGURE 2. **(a) Fuzzy linguistic variables for the Severity related to the effects on the device - *Sd*. (b) Fuzzy linguistic variables for the Severity related to the effects on people - *Sh*. (c) Fuzzy linguistic variables for the Occurrence - O. (d) Fuzzy linguistic variables for the Detectability - D. (e) Fuzzy linguistic variables for the Fuzzy Risk Priority Number - FRPN.**

the universe X, for a given element x of the universe, are as follows [40]:

$$\textit{Union} \quad \mu_{A \bigcup B}(x) = \mu_A(x) \vee \mu_B(x) \tag{8}$$

$$\textit{Intersection} \quad \mu_{A \bigcap B}(x) = \mu_A(x) \wedge \mu_B(x) \tag{9}$$

where the symbol $\vee$ is the maximum operator and $\wedge$ is the minimum operator.

The final step in a fuzzy rule-based system is the defuzzification. It is the conversion of a fuzzy quantity to a crisp quantity, mapping the output from the fuzzy domain back into the crisp domain [9], [40]. In this last step the FRPN crisp value is obtained with the Weighted Mean of Maximum method which is often the most commonly adopted and one of the more computationally efficient methods [13], [22], [41]–[43]. It is given by the algebraic expression:

$$Z = \frac{\sum_{i=1}^{n} \mu_i(\bar{x})\bar{x}}{\sum_{i=1}^{n} \mu_i(\bar{x})} \tag{10}$$

where n is the number of output fuzzy sets and $\bar{x}$ is the crisp value at which the i-th membership function $\mu_i(\bar{x})$ reaches its maximum value.

An example of the proposed If-Then rules and use of the min-max inference is shown in figure 3 (this representation is based on that of [13]): let us take for example the inputs occurrence *Low*, severity (Sd) *Moderate* and detectability *Low* in **rule R1**. They yield the conclusion risk **High** with a membership function value of $\mu_{FRPN} = \min(\mu_O = 1,\ \mu_{Sd} = 1,\ \mu_D = 0.4872)$* $W_{FRPN} = 0.4872$*$0.63 = 0.29$ with weight factor of $W_{FRPN} = 0.60$ (computed with equation 7). By same reasoning, in **rule R2** the inputs yield the conclusion risk **High** with a membership function value of $\mu_{FRPN} = 0.63$ and weight factor of $W_{FRPN} = 0.63$. Using the min-max inference method, the conclusion risk **High** will have these last values of membership function and weight factor. The aggregation of fuzzy outputs with weight is shown as a gray area in figure 3. The FRPN crisp value, evaluated using equation 10, is 450.69. For this example the overall min-max inference method with aggregation of outputs and defuzzification for evaluation of riskiness is summarized in table

1) RISK REDUCTION

Some countermeasures can be adopted even jointly in order to reduce the risk [44], [45]:

- Use of active and passive safety devices;
- Adoption of hazard warning devices (lamps, alarms, labels, etc.);
- Training courses on the use of the device for the maintenance and installation staff;
- Adoption of Quality Assurance (QA) procedures. This term refers to all activities aimed to ensure the fulfillment of quality objectives, which can include installation, sales, after-sales service and quality control. The guidelines issued in 2017 by various bodies, including

the AAPM [46], was considered for this CBCT technology equipment.
- Inclusion of operating instructions.

The ALARP principle is the approach generally applied in the risk assessment and control process. This principle states that the risk must be ''As Low as Reasonably Practicable'' [47]–[49]. An ALARP zone is defined in such a way [50], that all the risks allocated in this zone are considered tolerable if one of the following situations occurs:

- a further reduction of the risk is impracticable;
- the achievable improvement does not justify the cost and the expenditure of employed resources.

Once the mitigation has been carried out, it is necessary to assess the presence of residual risks and of the new risks arising from the applied countermeasures. The residual risk necessarily has to be below the acceptability threshold.

2) STRUCTURE OF THE FUZZY PROCESS-FMECA TABLE

The various failure modes have been included in a table, that is based on the model provided by the IEC EN 60812 standard and inspired by examples from the literature. In the Fuzzy Process-FMECA analysis, each row of the table is assigned to a failure mode, identified by a unique ID code. The ID code is made up of two elements: the former indicates the task under consideration (outdoor transport, indoor transport, storage, installation, maintenance, etc.), the latter the failure mode with increasing numbering. For example, T.F1 refers to the fault mode n° 1 and is related to ''Transport'' task. This type of classification highlights that multiple failure modes can correspond to each task, and in turn each failure mode can have multiple causes and multiple effects. As the FMECA methodology imposes, each adverse event has been considered individually, whenever a different risk scenario occurs, that is intended as a combination of S, O and D [51]. The typical information of the FMECA analysis is entered in the table columns. This information, starting from the identification of the failure mode, enables to assess the risk priority index and possibly the countermeasures to be adopted (with reference to Table 7):

1) Failure mode ID.
2) Type of risk: the failure mode can cause a mechanical, electrical, radiological, thermal hazard, or a risk that is related to software, or a risk that affects usability and environment.
3) Potential failure mode, i.e. how the failure occurs.
4) The System Safety Related Characteristics (SSRC) of the Device in study (see Table 10) affecting the specific failure mode.
5) Potential cause of failure: this can be blamed both to events not directly dependent on persons (e.g.: peaks or fluctuations of current / voltage, mechanical wear, electromagnetic interference), or to human errors (e.g.: installation, maintenance and use).
6) Possible effect on the device: how the fault occurs in the device operation (e.g.: it remains unchanged or behaves abnormally or causes malfunction in downstream components).
7) Possible effect on the person: since the identified failure modes can occur at any stage of the use of the device, the potential ''victims'' of a failure can be the patient or an operator, who in turn can be: the radiology technician, the radiologist, the biomedical engineer, the technician who carries out repair or maintenance.
8) Initial state: the design solutions, procedures and tests already provided for the device are described.
9) Evaluation of S, O and D, based on the corrective and preventive identified measures (according to criteria reported in the next subsection).
10) Obtained value of the FRPN.
11) Based on the acceptability threshold, set according to what reported in the ''Results'' section, recommended preventive or corrective actions have been suggested, with the aim of making the risk acceptable.
12) Evaluation of new S', O' and D' values based on the proposed control measures.
13) Obtained value of FRPN', which must necessarily be below the threshold.

3) CRITERIA FOR ASSIGNING S, O AND D PARAMETERS

The determination of severity, occurrence and detectability values was carried out using classification criteria obtained from the literature and others established specifically for the type of device analyzed. We considered estimated values of S, O and D. These estimates are based on so-called ''predicate devices''. These are legally marketed devices that are substantially equivalent to the considered prototype (e.g.: scanners from the same company and products from market leaders).

An in-depth discussion of the detailed range and criteria for attributing the different values to S, O, and D parameters is reported in Section II.B4 (tables 3-6) of a previous article from the authors [50] (please note: ''occurrence'' is defined there as ''probability of occurrence P'').

4) EXTRACTION OF THE RISK ACCEPTANCE THRESHOLD

The IEC EN 60812:2018 standard [4] does not indicate any methods for choosing a threshold for assessing the risk acceptability, but it just refers to a criterion suitable for the specific application. This freedom of choice has entailed that various approaches can be found in the literature [33]–[35], [52]–[57]. This paper focuses on two of these. The first method is fully graphical and is called ''Scree Plot''. Initially, it sorts the failure modes by increasing RPN, then plots the determined values on a graph so as an increasing monotone curve is obtained [56], [57], the monotone propriety of the RPN scores is important in FMECA and it has been observed in this particular analysis. The slope of this curve generally grows slowly at the beginning and more rapidly as values away from the ordinate axis are considered. The point where this variation occurs is called the ''RPN jump''. The RPN jump can be identified in two ways: by observing the trend of the graph or by evaluating the second

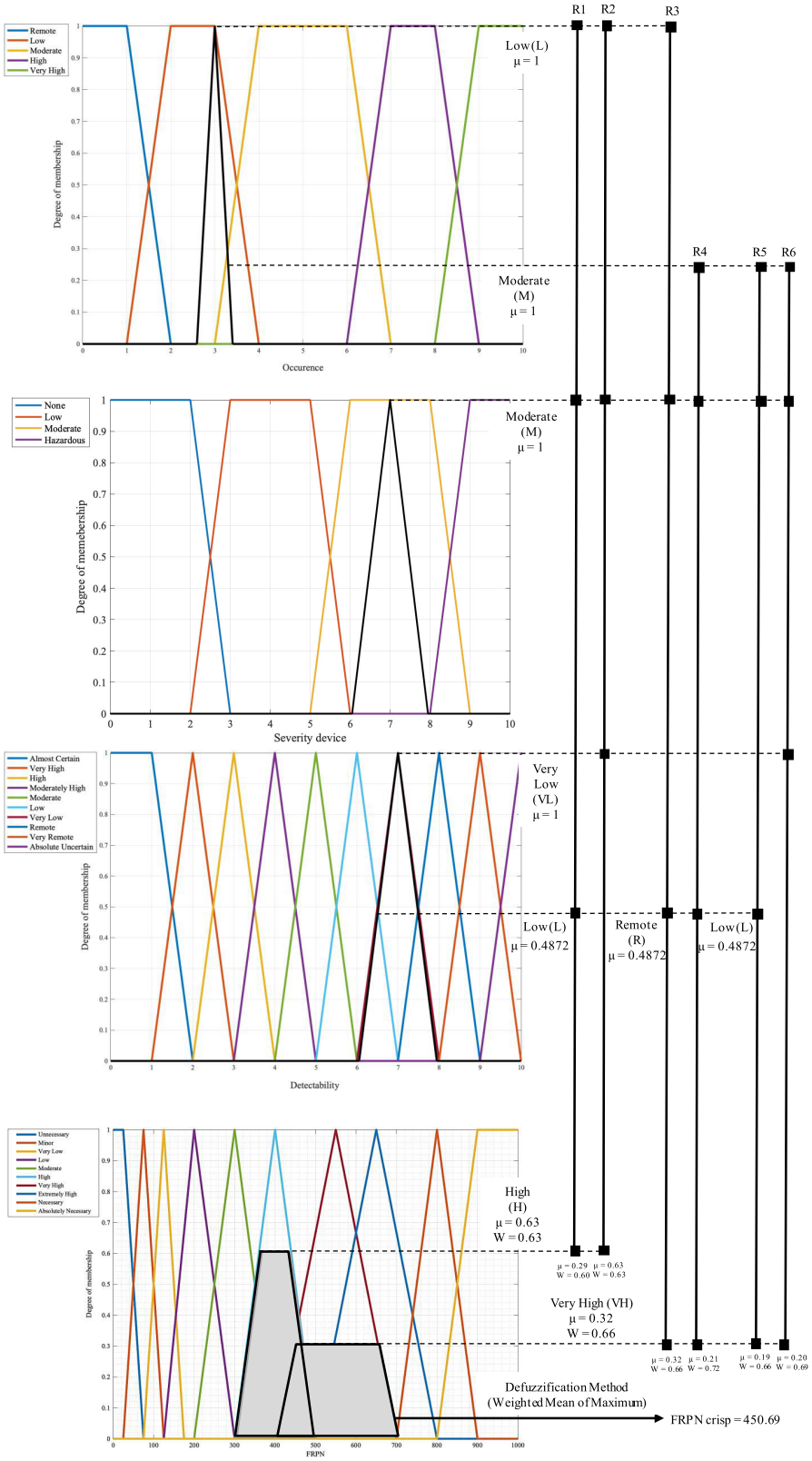


FIGURE 3. The rule evaluation process.

derivative of the curve. In fact, the maximum of the second derivative gives information on the maximum variation in slope of the curve. The point where the slope of the curve suddenly changes, qualitatively represents the risk acceptability threshold. When a failure mode exceeds this limit, it must be mitigated [57]. The second method is the Pareto

TABLE 7. Structure of the fuzzy process-FMECA table.

ID	Risk type	SRC (#)	Potential failure mode	Potential cause of failure	Possible effect on the device	Possible effect on person	Initial process state	Sd	Sh	O	D	Smax	FRPN	Action recommended	Sd'	Sh'	O'	D'	S'max	FRPN'
T.F1																				

criterion, a statistical methodology that has been used by some authors [58], [59] in their risk analyzes in order to determine the failure modes that compromise the security of a device. It is a graphical method that considers a histogram, where the failure modes are sorted by decreasing RPN, and a curve which points coincide with the cumulative RPN values, expressed as a percentage, with respect to the total value (that is the sum) of the determined RPNs. This is the Pareto chart. According to this criterion, 70-80% of the process variability (i.e. unwanted outputs) is caused by 20-30% of the total failure modes [60]. Applying this principle, it is therefore possible to identify the 20-30% of the failure modes that contribute to 70-80% of the RPN cumulative value. The RPN threshold is set equal to the RPN value that corresponds to a cumulative RPN (read on the previously mentioned curve) of 70 or 80%. All the failure modes above the threshold are graphically located on the left of the threshold [50], [60]. The methods described above, the Scree plot and the Pareto criterion, have been used in combination to carry out the fuzzy logic risk analysis presented in this article. The Pareto chart is based on 70-30% system, it means that was considered the RPN threshold (in our case, the FRPN threshold, Fuzzy Risk Priority Number), to the left of which there is 30% of the failure modes. The sum of the corresponding FRPN values gives rise to a cumulative FRPN that equals 70%. The two methods are different and produced two different thresholds. It was decided to maintain both thresholds and to set a priority of action for failure modes with FRPN above both thresholds.

III. RESULTS AND DISCUSSION

The prototype of a CBCT device, on which the life cycle risk management analysis was carried out, is thoroughly described in a previous article [50], describing the risk analysis performed during the design phase of the device (Design-FMECA). We recall its essential characteristics hereafter and introduce some information useful for the process risk management analysis.

A. FEATURES OF THE CBCT PROTOTYPE

The scanner unit is the basic unit of the device and is made up of two main sub-units: a gantry and a base. The gantry is the rotating element that hosts both the source and the sensors for obtaining radiological images. The base supports the gantry and makes it possible to move the scanner: the unit has a small size and is fitted with stabilizing feet and wheels, making it possible to move it quickly in the healthcare facility from one department to another. Upon installation, the wheels are raised, and the feet lowered by means of a hydraulic lifting system. A PC and an isolation transformer are positioned inside the base sub-unit.

The patient lays down on a bed suitable for use and separate from the scanner unit. The bed is motorized and controlled by pedals, allowing the operator to shape it to different configurations. The bed is equipped with swivel wheels and pedal brakes, operated during the manual positioning of the patient under the scanner unit. The parts that support the body regions of clinical interest are radiolucent. The arm support is anchored to the bed by means of a special clamp, that allows the operator to move the patient's arm to the needed height.

The environmental technical specifications of the device are described in Table 8, where the International Protection (IP) degree in the first row refers to the scanner unit. The indicated temperature limits, especially the lower ones, are very restrictive, even if the components have been designed and tested to work at even lower temperatures. Indeed, the table reports the range within which a correct functioning of the device is guaranteed.

Table 9 shows electrical specifications. It can be noticed that oscillations of 10% of the alternating supply voltage are allowed: within the corresponding extremes the elements of the radiological chain can work correctly. Wiring conforms to the safety UL/CSA agency standards for the US and Canadian marketplaces.

The system is very complex and sophisticated, being made up of numerous components. A set of short-circuit and over-current protections and components makes the system safe in case of failure. The safety function can be activated manually by means of an emergency button, that cuts off the power, or automatically by means of relays, called safety relays.

B. CLASSIFICATION OF THE RISKS

According to ISO 14971 [2]: ''risk'' is the combination of the probability of the occurrence of harm and the severity of that harm. ''Harm'' means physical injury or damage to the health of people, or damage to property or the environment. ''Hazards'' are the potential sources of harm. Annex A of the above mentioned guidance ISO 24971 [3] proposes a list of questions that makes it possible to determine the characteristics of the medical device that might affect safety. This procedure helps in identifying the risks associated with the

TABLE 8. Technical environmental specifications.

IP Protection Degree	Scanner Unit: IP20
Operating Environmental Conditions	Temperature: between 10°C (50°F) and 40°C (104°F) Relative Humidity: between 30% and 75% RH (no capacitor) Atmospheric Pressure: between 700 hPa and 1060 hPa
Transport Environmental Conditions	Temperature: between 10°C (50°F) and 50°C (122°F) Relative Humidity: between 20% and 85% RH (no capacitor) Atmospheric Pressure: between 700 hPa and 1060 hPa
Storage Environmental Conditions	Temperature: between 10°C (50°F) and 50°C (122°F) Relative Humidity: between 20% and 85% RH (no capacitor) Atmospheric Pressure: between 700 hPa and 1060 hPa

TABLE 9. Electrical specifications.

Protection against electrical shock	I-B Class (see Section A4 [50])
Power Supply	$(230 \pm 10\%)V_{AC}$, 50/60 Hz
Wiring	Compliant with UL/CSA Certification
Maximum absorption	5000 VA

use of the considered device. The questions concern its manufacture, intended use, final users, any reasonably foreseeable misuse and the final disposal of the medical device itself. This methodology gives a comprehensive view of where the potential hazards are located. The characteristics for the device under examination are collected in the System Safety Related Characteristics (SSRC), reported in Table 10 [50]. These characteristics and the requirements found in the reference standards enable the classification of risks as mechanical, thermal, electromagnetic and radiological.

C. IDENTIFYING ERROR MODES

After a deep study of the conditions of use applied to the device, we identified some tasks and the possible failure modes or errors for each of them. The identified tasks are:

- Transport of the device from the manufacturer / distributor to the healthcare facility: the packaging must protect the device as much as possible from any form of weather and environmental conditions, since the device can be shipped in many very different environments. This packaging consists of an external wooden crate and an internal barrier bag made of aluminum and shock-absorbing material. The device is vacuum-sealed in order to protect it from humidity.
- Transport within the structure's premises: the device is mobile, therefore it can be manually moved within the hospital structure, thus increasing its versatility of use.
- Storage: the device is kept in special warehouses, if it is not immediately installed.
- Installation: the installation phase is critical when the device is moved to a new environment. The service technicians of the manufacturer or distributor, those inside the structure and other professional figures, such as engineers and health physicists, are responsible for the correct installation.
- Preparation of the patient for the examination: this phase is composed of different steps, namely: patient identification, patient positioning (first on the table and then inside the gantry), setting the scan parameters, checking the patient positioning.
- Device handling: this task refers to the maneuvers that are carried out to move both the scanner unit and the patient support inside the radiological room, in order to correctly perform the scan.
- Execution of the CBCT scan: when the patient has been correctly placed, the operator can start the acquisition. Although the scan time is quite short (the typical value is 27 seconds), this stage can lead to various risks for the patient, primarily radiological ones.
- Interpretation of the results: this phase mainly involves devices' software, which has to provide the radiologist with images that are as free of artifacts as possible.
- Maintenance: it is important to take into account certain errors that may occur during both scheduled maintenance (SM) and corrective maintenance (CM) while evaluating the use of the system. SM refers to those scheduled periodic activities (daily, monthly, annual) that monitor the status of the device. CM is required in case of failures and is made up of activities such as device or components repairing or replacement. These activities can be carried out by the manufacturing company's service or by the distributor's service.
- Labeling and user manuals: when a device is marketed, it must be accompanied by the manufacturer's instructions for use, which informs the operator about the correct use of the device. Furthermore, it must be provided with labels, which signal hazards or explain the function of a specific component.

Various users, according to their different knowledge and training, can perform some of the above tasks, namely: manufacturer's or distributor's service technicians, clinical engineers, healthcare structure managers, radiology technicians and radiologists. One key task is to identify the persons responsible for each phase of device use and to provide solutions, both technological, software, and procedural, in order to limit the improper use of the device.

D. THE FUZZY PROCESS-FMECA

During the study of the possible critical issues for each task listed above, possible error modes, arising from both normal use and reasonably foreseeable misuse, were identified: 51 error modes were recognized. In some cases, failure

TABLE 10. System Safety Related Characteristics (SSRC) for the device in study [2].

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, precision of measurement results*)
4	Device interpretative (*algorithms used, confidence limits, unintended application of algorithms*)
5	Unwanted output energy (*noise, vibration, heat, radiation, leakage currents, electric and magnetic fields*)
6	Unwanted output substances (*substances used in manufacturing, discharge of chemicals, waste products, body fluids*)
7	Device susceptible to environmental influences (*operational, transport and storage environments, electromagnetic interference, 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 subject to mechanical forces (*forces under the control of user or controlled by interaction with other persons*
12	Factors which determine the device lifetime (*aging, battery depletion*)
13	Installation or use requiring special training (*a-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, color 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*)
21	Device holding 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*)

modes that were previously identified during the Design-FMECA ([50]) have been included in this Fuzzy Process-FMECA as well, showing new grades of severity and possible adverse events.

1) DEVICE TRANSPORT FROM THE MANUFACTURER/ DISTRIBUTOR TO THE HEALTHCARE FACILITY

The critical factors during transport are environmental conditions, such as temperature, pressure, humidity, and vibrations. The device is also able to travel under temperature and humidity conditions beyond the ranges under which correct operation is guaranteed (Table 7). However, damage to electrical and electronic components, which are the weakest, may still occur. In addition, when the device is switched on, any condensations might generate electrical discharges, which could cause considerable damage to the device or harm to persons. Excessive vibrations, on the other hand, can lead to mechanical damage and disconnection of electrical components. Although a special packaging procedure is provided, the calculated *Fuzzy Risk Priority Numbers* (FRPNs, for definition see Section II-A) are high, since circumvention would require step-by-step monitoring of the transport process.

2) TRANSPORT INSIDE THE FACILITY PREMISES

When moving scanner unit and patient bed from one room to another, they might overturn or impact persons and/or other objects. During mechanical trials, the device was found to be stable even in case of improper handling by the operator or

obstacles [50]. For this reason, this risk index was deemed to be low.

3) STORAGE

The consequences of prolonged storage should be assessed, especially when in environments other than where the device will be used, e.g. outdoor warehouses. The risk is that internal parts, especially electrical and electronic components, may deteriorate, compromising the device performance and putting human health at risk.

4) INSTALLATION

Several failure modes have been identified, including various aspects of the installation procedure. The first one is the incorrect arrangement of external cables, such as power cord and foot-switch cables, which could obstruct the patient or operator passage. Since the power cord is connected to the back of the base and therefore away from the work area, the probability of this happening is considered low. Instead, the cables connecting the main unit with the operator workstation are routed through a conduit. Other plausible errors may arise from possible installer (technician or engineer) negligence when performing required procedures prior to device commissioning. These procedures include:

- Checking the interlock connection, linked to the room door, which will not permit the start of emissions until the door is closed;
- Geometric calibration;
- Warming up the monobloc, which is the integrated system containing the X-ray tube and the high voltage generator that powers the tube. Warm up prevents the monobloc from being used when still cold, in which case it can generate electrical discharges.

These failure modes have a low FRPN, being easily diagnosed by the system software. Since the device is supplied with a power plug suitable for the required electrical standard, there are no risks from using adapters for connection to the mains outlet. Indeed, the power cord may be too short, making the use of an extension cord inevitable; this, as already mentioned, could alter the device electrical performance. Finally, the radiology room may not be adequately shielded.

5) PREPARING THE PATIENT FOR EXAMINATION

Errors related to patient identification are easily diagnosed because of the one-to-one correspondence between the patient's ID and biographical data, making the risk of improper examination very low. More critical is the positioning of the patient into the gantry. Since patient-bed alignment in its different configurations is completely manual, there is the risk of not being able to properly center the area of interest or hindering the gantry rotation. Another error mode is linked to positioning the limb at the isocenter. Because this device presents an innovative configuration in diagnostic imaging, if the operator has not been properly trained, there is a risk of movement artifacts. For example, this happens if the limb is not in a comfortable position for the patient, or if there is beam hardening because the region of interest is obscured by very dense tissue (such as bone). Finally, the chance has been considered that the operator might set an inappropriate combination of parameters for the investigated area. As already explained, the upper limit is linked to the maximum power that can be delivered by the tube, while there are no constraints on the lower limit.

6) MACHINE HANDLING

An assessment was made of what might happen if the scanner unit wheel brakes are not locked. Since the gantry rotation speed is very low, the probability of the whole unit moving during operation is minimal. Nevertheless, should the room's floor have a slight slope, collisions with patient, operator or other people/assets could not be excluded. For the bed, the probability of unintentionally pressing the footswitch pedals that drive bed's movements, was considered high. This could occur if the operator was distracted or if the bed's wheels were to roll over the pedals. Furthermore, the lack of means to ergonomically move the device (e.g.: a handle), especially when the patient is lying in the bed, was considered critical.

7) PERFORMING THE RADIOLOGY EXAMINATION

Several error modes have been identified that could cause a patient to be exposed to unneeded or, in a worst-case scenario, excessive ionizing radiation. During a scan, acquisition could be interrupted suddenly, for example due to a power failure or external electromagnetic disturbances. In the first case, since there are no internal power sources, if there is no connection to an uninterruptible power supply (UPS), the device will simply shut down and lose any newly acquired data. In the second case, tests showed that other devices operating in the radio frequency range may cause sudden shutdowns or intermittent operation of some components, such as motors or power supplies. Another error mode concerns the unintentional activation of the X-ray command. As mentioned above, X-ray emission can only be enabled with a dual command making the probability of error very low. The influences of the environmental and ergonomic conditions under which the operator works were also considered. By blocking the visibility of the light from the emission lamp, an obstacle, an object, or a very intense light, could prevent the operator from continuously monitoring machine operation and intervening in case of emergency.

8) INTERPRETATION OF THE EXAM RESULTS

Acquired images may be affected by artifacts. The presence of such artifacts is considered a failure mode only when they can be prevented. Artifacts may originate from the patient (motion artifacts or metal objects), from panel sensitivity degradation (such as ring artifacts) or from poor positioning of the limb to be scanned (beam hardening caused by dense tissue that should not be within the Standard Field Of View, or FOV). Other artifacts produced by physical causes, such as beam hardening caused by tissues actually in the

FOV, partial volume artifacts or photon starvation, cannot be checked before scanning, but can be compensated through image enhancement techniques. Another error mode concerns the presence of scatter radiation. This is a phenomenon that should not be overlooked whether because the regions of interest are large (e.g. the head) or because the dose absorbed by the patient must be reduced as far as possible to only the dose needed for imaging. Finally, the possibility of incorrect data transfer was considered. This error mode was found to have low risk, since the data transfer relies on the DICOM standard, which contains all the information (resolution, scanning parameters, region of interest (ROI), patient data, etc.) required to ensure that the images are equally visible and interpretable on any suitable workstation [61].

9) MAINTENANCE

a: PREVENTIVE MAINTENANCE

- Failure to daily warming up the monobloc and failure to periodically calibrate it are among the most frequent maintenance errors. These two failure modes can lead to changes in the accuracy and repeatability of the emission parameters. These changes include loss of image quality, in terms of uniformity, linearity, geometric accuracy, spatial resolution and noise as well as in terms of emission levels, which can lead to an increase in the Computed Tomography Dose Index (CTDI). This index expresses the dose actually delivered to the patient [62]. If these procedures are not periodically repeated, the device's performance may be compromised, with the risk of obtaining images that do not represent reality.

b: CORRECTIVE MAINTENANCE

- There are essentially two errors that can occur for this type of maintenance. One is the lack of immediately available spare parts. The other is failure in tracking and monitoring the corrective actions performed during the whole device lifecycle. In the first case, the severity and likelihood of not having spares on hand depend on whether or not there is a spare-parts warehouse where the most critical components, such as those of the radiological chain, can be stored. In the second case, if maintenance is done directly by the manufacturer's service department, a record of all repairs, related to all devices, will be available. Should the supplier's service department not adopt this procedure, there might be a risk of improper device behavior: reviewing the record of past critical issues will facilitate fault diagnoses and fast return to service.

10) LABELING AND USE INSTRUCTIONS

It is possible that the machine labels or instructions for use might be incomplete or misunderstood. To avoid this, two standards have been applied to the former and to the latter, respectively EN ISO 15223-1 ''Medical devices - Symbols to be used with medical device labels, labelling and information to be supplied - Part 1: General requirements'' [63] and EN 1041 ''Information supplied by the manufacturer of the medical devices'' [64]. This way, symbols, nomenclature and device information are drafted according to precise standards valid for all medical devices. For this reason, these risks can be considered to have a low FRPN.

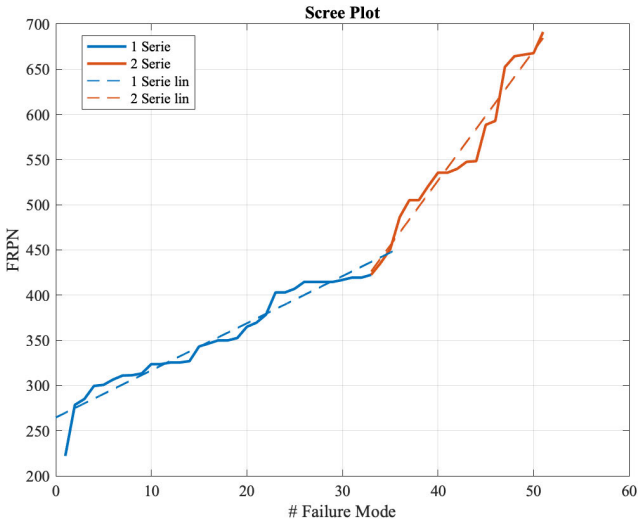


FIGURE 4. Scree plot obtained from fuzzy Process-FMECA. Intersection of the lines is FRPN = 442.62.

E. IDENTIFICATION OF THE RISK ACCEPTANCE THRESHOLD

The FRPN values obtained for each failure mode were used to identify the risk acceptance threshold, using two methods: Scree Plot and Pareto Diagram, as illustrated in Section II-B4. The graph in Figure 4 was obtained by sorting the FRPN values in ascending order. It was decided to qualitatively identify the point where the slope variation occurs, avoiding the calculation of the maximum of the second derivative, deemed too conservative. The point of intersection of the two lines approximating the two trends corresponds to an FRPN of 442.62.

Instead, using a Pareto diagram with the 70%-30% system, the FRPN values are sorted in descending order and the FRPN threshold value is found as the value, in the cumulative curve, corresponding to the 70% ot the total. This threshold is FRPN = 378.40 (Figure 5).

As can be seen, the Pareto Diagram provided a lower FRPN value, less conservative than the Scree Plot. As already discussed, it was established that both thresholds would be kept, with a fault mode intervention priority set above the highest threshold. In the FMECA Process table, described in Section II-B2, the fault modes with FRPN exceeding both thresholds are indicated in red, those with FRPN between the two thresholds in yellow and those with a lower FRPN in green. The lowest of the two thresholds is taken as the limit of acceptability. All the failure modes with higher FRPNs will need appropriate risk control countermeasures. In the Fuzzy FMECA Process, 29 out of 51 failure modes were unacceptable (17 on high priority and 12 on low priority). This means that more than 50% of the failure modes need some corrective actions.

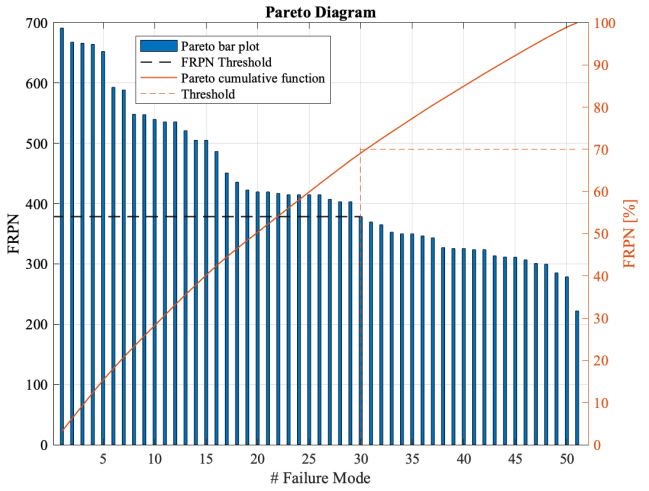


FIGURE 5. Pareto diagram of the fuzzy Process-FMECA. The threshold was identified as FRPN = 378.40.

F. RISK MITIGATION

For those failure modes above the threshold, some countermeasures were proposed to lower their fuzzy risk priority indexes. Some countermeasures were applied to test their validity. According to ISO 14971, it is possible that some of these countermeasures might lead to the appearance of new risks. These risks are highlighted in the Fuzzy Process-FMECA table, together with their risk indexes (FRPN). These indexes have to be acceptable to prove that the introduced protection measures brought benefits. The failure modes identified in the Fuzzy Process-FMECA and their corrective actions are listed below. First of all, the risks in the red band (FRPN $\geq$ 442.62) which therefore require more urgent mitigation, are described. Then, the countermeasures proposed and those actually applied are identified.

- Transport outside the foreseen environmental ranges (FRPN = 691.15, FRPN = 539.72): in order to monitor the environmental conditions during the whole duration of transport, the packaging (the external wooden crate) can be equipped with a *data logger*. This instrument can be rented from the shipping company in charge of transporting the machinery. The data logger records crucial parameters such as temperature and humidity, as well as possible overturning and impacts.
- Storage outside of the provided environmental ranges (FRPN = 666.09): if there is an expectation that the device will be stored for an extended period before being installed in the hospital or clinic, the device should be kept in its original packaging, therefore mitigating the likelihood of damage to mechanical or electrical components. Good practice would call for the continued monitoring of environmental parameters on the data logger during storage.
- Incorrect positioning of the region of interest (FRPN = 548.23, FRPN = 422.51): two countermeasures are applicable to avoid the patient lying in an uncomfortable position and artifacts that might be generated in the image. The first is adequate operator training (in this case the radiology technician or the doctor). The second is, depending on the district to be analyzed, a screen preview provided by the software that suggests the ideal position for patient placement.
- Unintentional pressing of bed footswitch pedals (FRPN = 664.31, FRPN = 535.53): to prevent this error mode at its root, a metal or plastic guard could be installed to prevent the pedals from being accidentally pressed by the operator or by the wheels on the bed.
- Performing an incorrect examination on the patient (FRPN = 667.74): this error mode at the moment can only be mitigated by appropriate training of the operator, who, before starting the scan, must collect as much information as possible from the patient, through questions and visual evaluation. Further risk reduction can be achieved by connecting the device to a *Picture Archiving and Communication System* (PACS) for examination request management.
- Moving the scanner unit during rotation (FRPN = 486.43): to avoid starting to scan while the scanner unit is not properly braked, an assessment of the possibility of installing photo-sensors, connected to the main board of the device, linked to the wheel brake locks was made. The software will display a screen message to the operator if any one of the four brake locks is not activated.
- Presence of non-intrinsic artifacts (FRPN = 547.54, FRPN = 520.99): in addition to applying correct positioning procedures, radiotransparent supports or cushions may be provided to reduce movement artifacts. Clinical protocols suggest the use of anti-scatter septa to reduce scatter radiation for large volumes only (including the head) and not for scanning the extremities [65]. For this reason, it has been suggested that removable septa be used for head scans only.
- Failure to check the device history (FRPN = 505.10): it is necessary to provide for an agreement between manufacturer and distributor so that all maintenance activities are recorded.

The countermeasures listed below have actually been implemented:

- Non-ergonomic handling of the bed (FRPN = 535.53): to ease bed handling, four handles were installed, two on each side of the bed. It has been shown that these handles do not significantly increase the width of the bed, thus responding to the risk that the gantry will impact a person during its rotation.
- Disturbances from external equipment (FRPN = 652.40): to deal with the malfunctions that emerged during testing, ferrites and copper tape were installed on the components that were shown to be problematic (motors and 24-V power supply) to shield them from disturbances at critical frequencies.

Other error modes to be mitigated, in the yellow band (378.40 $\leq$ FRPN $<$ 442.62), are listed below:

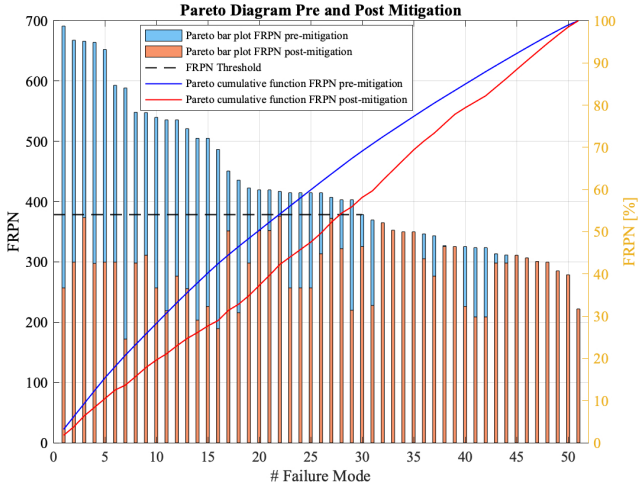


FIGURE 6. Pre-mitigation (blue) and post-mitigation (orange) Pareto diagrams. The red curve shows the weight of the cumulative FRPN' on the previously calculated value.

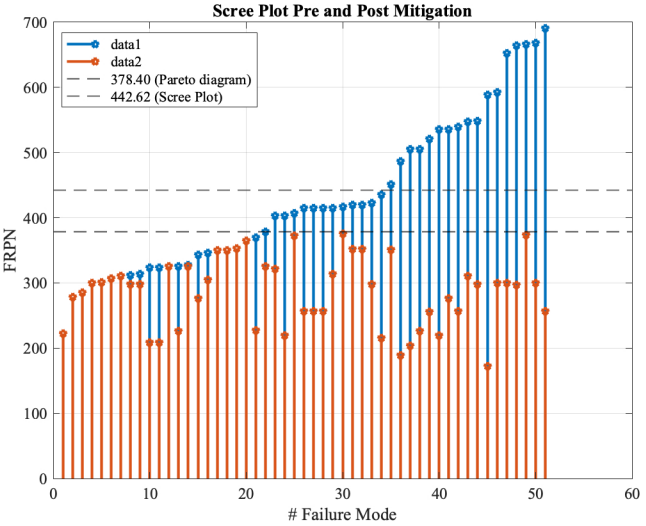


FIGURE 7. Pre-mitigation (blue) and post-mitigation (orange) scree plots. All post-mitigation failure modes were lower than both acceptability thresholds.

- Use of extension cords with the power cord (FRPN = 435.68): to avoid the use of extension cords, power cords with different lengths can be supplied, so that a cord with an appropriate length can be chosen during installation. Since the length of the cord affects its impedance, there is the risk that it will not supply the load correctly. For this reason, during electrical testing, the operation of the device must be verified with each cable supplied.
- Incorrect alignment of the support with respect to the gantry (FRPN = 416.85): to avoid that the bed, especially when it is in an elongated configuration, obstructs gantry rotation, guides drawn on the floor or lasers could be used for alignment. The possibility of inserting a hook system to the scanner unit base was also assessed. However, this countermeasure would introduce an additional trapping risk, particularly in case of emergency, when it could be more difficult extracting the patient from the gantry.
- Loss of calibration (FRPN = 414.65): the Quality Assurance (QA) procedures provide for several types of calibration [46]. Each of these should be repeated at a different frequency, which must be indicated by the manufacturer in the user manual. The manufacturer will provide the necessary instrumentation (dummies and dosimeters) for on-site maintenance by specialized hospital/clinic personnel. Specifically, to counteract the loss of image quality, monthly inspections are to be made to verify:
  - no loss of accuracy of the radiological parameters (in terms of tolerances required by the standard [66])
  - repeatability of the radiation emissions (in terms of coefficient of variation)
  - no deterioration in uniformity and spatial resolution.

  Less frequently (generally each year) it is necessary to check that the CTDIs declared at the beginning have not changed, e.g., due to a reduction in the effectiveness of the intrinsic and supplementary shielding. Instead, every day at start up, a quick geometric calibration test is performed.

In light of the proposed control measures, new S', O' and D' values were assigned and a new product FRPN' was calculated accordingly. As shown in Figure 7, all error modes were reduced to an acceptable level. The Pareto diagram in Figure 6 shows a significant reduction of the overall risk index value, which is less than 50% of the total pre-mitigation FRPN. The complete Fuzzy P-FMECA analysis report is provided as supplementary material.

IV. CONCLUSION

This paper illustrates how a risk analysis should be conducted when managing an electromedical device. In this work the risk analysis was applied to a prototype of a CBCT device. The Fuzzy Process FMECA was chosen among the existing risk analyses because, due to its modular structure, it makes it possible to highlight the activities that can lead to a great number of errors during the life cycle of a device, obtaining an improved risk analysis capable of overcoming the shortcomings of traditional FMECA. The proactive nature of this method implies that there will be evidence of improvements obtained from Fuzzy FMECA once field data will be available, as further explained in Section IV. When the analysis was completed, countermeasures were proposed in order to lower the risk priority index for those failure modes that resulted above the threshold. After the adoption of these mitigations, all RPN' values obtained using the new S', O' and D' parameters, were below both previously determined acceptability thresholds. Therefore, it was necessary to assess the residual risk consequent to these countermeasures. For this purpose we distinguished between residual risks not requiring mitigation, and residual risks with higher entity, but

which can still be considered acceptable due to the associated benefits and the impracticability of reducing them. The result of the adopted procedure was that no risk was unacceptable and that the introduced mitigations did not cause new hazardous situations. The applied risk analysis has shown that each phase or activity is fundamental to guarantee a correct life cycle of the device. It is to note that the correct execution of the transport, installation, use and maintenance procedures is of great importance. Adequate training of the operators (radiology technicians, radiologists, technicians in charge of maintaining Quality Assurance) is essential.

FUTURE WORKS

In future developments of this work, relative importance of S, O and D parameters can be reassessed and tuned on the basis of field data, not available to date. Being this device not yet in production, but currently existing as a prototype, there are no feedback data yet from the field. The comparison with existing experience from similar devices is in line with the expectations from this Fuzzy FMECA proactive analysis, about the reduction of the overall risk. Risk management is an iterative process, therefore when real data from actually installed devices will start flowing in, it will be possible reassessing the whole process, both reviewing the relative importance of S, O, and D (therefore applying the so-called *"Evidence Theory"*, as discussed in [5]), and the real effectiveness of applied countermeasures, updating or confirming the proactive results obtained through the mitigated FRPN calculation.

REFERENCES

[1] (Mar. 2018). *World Health Organization: Medical Device Full Definition*. Accessed: Jan. 7, 2021. [Online]. Available: https://www.who.int/medical_devices/full_deffinition/en/

[2] *Medical Devices Application of Risk Management to Medical Devices*, Standard ISO 14971:2019, ISO, 2019.

[3] *Medical Devices Guidance on the Application of ISO 14971*, Standard ISO 24971:2020, ISO, 2020.

[4] *Failure Modes and Effects Analysis (FMEA and FMECA)*, Standard CEI IEC EN 60812, IEC, 2018.

[5] P. Buffa, M. Giardina, G. Prete, and L. De Ruvo, "Fuzzy FMECA analysis of radioactive gas recovery system in the SPES experimental facility," *Nucl. Eng. Technol.*, vol. 53, no. 5, pp. 1464–1478, May 2021.

[6] Y.-J. Yang, Y.-L. Xiong, X.-Y. Zhang, G.-H. Wang, and B. Zou, "Reliability analysis of continuous emission monitoring system with common cause failure based on fuzzy FMECA and Bayesian networks," *Ann. Oper. Res.*, pp. 1–17, Apr. 2019. [Online]. Available: https://link.springer.com/article/10.1007/s10479-019-03234-x#citeas

[7] M. Giardina and M. Morale, "Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology," *J. Loss Prev. Process Ind.*, vol. 35, pp. 35–45, May 2015.

[8] D. Piumatti, J. Sini, S. Borlo, M. Sonza Reorda, R. Bojoi, and M. Violante, "Multilevel simulation methodology for FMECA study applied to a complex cyber-physical system," *Electronics*, vol. 9, no. 10, p. 1736, Oct. 2020.

[9] M. Giardina, F. Castiglia, and E. Tomarchio, "Risk assessment of component failure modes and human errors using a new FMECA approach: Application in the safety analysis of HDR brachytherapy," *J. Radiol. Protein*, vol. 34, no. 4, pp. 891–914, Dec. 2014.

[10] N. Chanamool and T. Naenna, "Fuzzy FMEA application to improve decision-making process in an emergency department," *Appl. Soft Comput.*, vol. 43, pp. 441–453, Jun. 2016.

[11] G. Bernardini, F. Paganelli, M. Manetti, A. Fantechi, and E. Iadanza, "SYRMA: A tool for a system approach to risk management in mission critical systems," *Int. J. Bus. Inf. Syst.*, vol. 13, no. 1, pp. 21–44, 2013.

[12] F. Bambi, I. Spitaleri, G. Verdolini, S. Gianassi, A. Perri, F. Dori, and E. Iadanza, "Analysis and management of the risks related to the collection, processing and distribution of peripheral blood haematopoietic stem cells," *Blood Transfusion*, vol. 7, no. 1, p. 3, 2009.

[13] J. B. Bowles and C. E. Peláez, "Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis," *Rel. Eng. Syst. Saf.*, vol. 50, no. 2, pp. 203–213, Jan. 1995.

[14] V. Basini, R. Cinotti, P. Di Denia, N. Caranci, F. Novaco, and R. Tartaglia, "FMEA–FMECA. Analisi dei modi di errore/guasto e dei loro effetti nelle organizzazioni sanitarie. Sussidi per la gestione del rischio 1. Dossier N. 75/2002," Agenzia sanitaria e sociale regionale, Regione Emilia-Romagna, Bologna, Italy, Tech. Rep. 75/2002, 2002.

[15] E. Hergon, P. Rouger, and P. Garnerin, "La prévention Des.défaillancesdu processus transfusionnel," *Transfusion Clinique et Biologique*, vol. 1, no. 6, pp. 455–465, Jan. 1994.

[16] A. Marey, B. Coupez, L. Gruca, V. Vannier, P. Renom, B. Wibaut, L. Rugeri, C. Cossement, and A. Cosson, "Impact d'une démarche qualité en sécurité transfusionnelle sur la prescription, l'optimisation Des.circuits, la traçabilité," *Transfusion Clinique et Biologique*, vol. 4, no. 5, pp. 469–484, Oct. 1997.

[17] M. R. Cohen, J. Senders, and N. M. Davis, "Failure mode and effects analysis," *Nursing*, vol. 24, pp. 40–42, Feb. 1994.

[18] L. Chadwick and E. F. Fallon, "Evaluation and critique of healthcare failure mode and effect analysis applied in a radiotherapy case study," *Hum. Factors Ergonom. Manuf. Service Industries*, vol. 23, no. 2, pp. 116–127, Mar. 2013.

[19] M. Giardina, M. C. Cantone, E. Tomarchio, and I. Veronese, "A review of healthcare failure mode and effects analysis (HFMEA) in radiotherapy," *Health Phys.*, vol. 111, no. 4, pp. 317–326, 2016.

[20] S. Broggi, M. C. Cantone, A. Chiara, N. Di Muzio, B. Longobardi, P. Mangili, and I. Veronese, "Application of failure mode and effect analysis to tomotherapy treatment delivery," *Radioprotection*, vol. 50, no. 3, pp. 171–175, Jul. 2015.

[21] R. E. McDermott, R. J. Mikulak, and M. R. Beauregard, *The Basics FMEA*, 2nd ed. New York, NY, USA: CRC Press, 2008.

[22] E. Akyuz, I. Akgun, and M. Celik, "A fuzzy failure mode and effects approach to analyse concentrated inspection campaigns on board ships," *Maritime Policy Manage.*, vol. 43, no. 7, pp. 887–908, Oct. 2016.

[23] A. Mariajayaprakash, T. Senthilvelan, and R. Gnanadass, "Optimization of process parameters through fuzzy logic and genetic algorithm—A case study in a process industry," *Appl. Soft Comput.*, vol. 30, pp. 94–103, May 2015.

[24] H.-C. Liu, J.-X. You, M.-M. Shan, and Q. Su, "Systematic failure mode and effect analysis using a hybrid multiple criteria decision-making approach," *Total Qual. Manage. Bus. Excellence*, vol. 30, nos. 5–6, pp. 537–564, 2019.

[25] G. Gupta and R. P. Mishra, "Comparative analysis of traditional and fuzzy FMECA approach for criticality analysis of conventional lathe machine," *Int. J. Syst. Assurance Eng. Manage.*, vol. 11, no. S2, pp. 379–386, Jul. 2020.

[26] X.-Y. Li, Y. Xiong, C.-Y. Duan, and H.-C. Liu, "Failure mode and effect analysis using interval type-2 fuzzy sets and fuzzy Petri nets," *J. Intell. Fuzzy Syst.*, vol. 37, no. 1, pp. 1–17, 2019.

[27] M. S. Kirkire, S. B. Rane, and J. R. Jadhav, "Risk management in medical product development process using traditional FMEA and fuzzy linguistic approach: A case study," *J. Ind. Eng. Int.*, vol. 11, no. 4, pp. 595–611, Dec. 2015.

[28] L. A. Zadeh, "Fuzzy sets," *Inf. Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965.

[29] L. A. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning-I," *Inf. Sci.*, vol. 8, no. 3, pp. 199–249, 1975.

[30] M. Kumru and P. Y. Kumru, "Fuzzy FMEA application to improve purchasing process in a public hospital," *Appl. Soft Comput.*, vol. 13, no. 1, pp. 721–733, Jan. 2013.

[31] A. Jamshidi, S. A. Rahimi, D. Ait-kadi, and A. Ruiz, "A comprehensive fuzzy risk-based maintenance framework for prioritization of medical devices," *Appl. Soft Comput.*, vol. 32, pp. 322–334, Jul. 2015.

[32] Q.-L. Lin, D.-J. Wang, W.-G. Lin, and H.-C. Liu, "Human reliability assessment for medical devices based on failure mode and effects analysis and fuzzy linguistic theory," *Saf. Sci.*, vol. 62, pp. 248–256, Feb. 2014.

[33] 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, pp. 1–5, Sep. 2013.

[34] 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, Sep. 2016.

[35] 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, Jan. 2011.

[36] W. Pedrycz, "Why triangular membership functions?" *Fuzzy Sets Syst.*, vol. 64, no. 1, pp. 21–30, 1994.

[37] B. De Finetti, *Teoria Della Probabilità*. Turin, Italy: Einaudi Editore Torino, 1970.

[38] H. Thiele, "Investigation of IF-THEN rule bases by methods of mathematical logic," in *Proc. IEEE Int. Conf. Fuzzy Syst.*, vol. 3, 1995, pp. 1391–1396, doi: 10.1109/FUZZY.1995.409862.

[39] E. H. Mamdani, "Application of fuzzy algorithms for control of simple dynamic plant," *Proc. Inst. Elect. Eng.*, vol. 121, no. 12, pp. 1585–1588, Dec. 1974.

[40] T. J. Ross, *Fuzzy Logic With Engineering Applications*, vol. 2. Hoboken, NJ, USA: Wiley, 2004.

[41] C. E. Pelaez and J. B. Bowles, "Using fuzzy logic for system criticality analysis," in *Proc. Annu. Rel. Maintainability Symp. (RAMS)*, Jan. 1994, pp. 449–455.

[42] M. Braglia, M. Frosolini, and R. Montanari, "Fuzzy criticality assessment model for failure modes and effects analysis," *Int. J. Qual. Rel. Manage.*, vol. 20, no. 4, pp. 503–524, Jun. 2003.

[43] T. R. Moss and J. Woodhouse, "Criticality analysis revisited," *Qual. Rel. Eng. Int.*, vol. 15, no. 2, pp. 117–121, Mar. 1999.

[44] *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, IEC, 2011.

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

[46] 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. Garayoa Roca, P. Caprile, and C. Zervides, "Quality control in cone-beam computed tomography (CBCT) EFOMP-ESTRO-IAEA protocol (summary report)," *Phys. Medica*, vol. 39, pp. 67–72, Jul. 2017.

[47] R. Bell and D. Reinert, "Risk and system integrity concepts for safety-related control systems," *Microprocessors Microsyst.*, vol. 17, no. 1, pp. 3–15, Jan. 1993.

[48] R. E. Melchers, "On the ALARP approach to risk management," *Rel. Eng. Syst. Saf.*, vol. 71, no. 2, pp. 201–208, Feb. 2001.

[49] 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.

[50] E. Iadanza, D. Pennati, L. Manetti, L. Bocchi, and M. Gherardelli, "FMECA design analysis: Risk management for the manufacture of a CBCT scanner," *IEEE Access*, vol. 7, pp. 181546–181564, 2019.

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

[52] S. Broggi, M. C. Cantone, A. Chiara, N. D. 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, Sep. 2013.

[53] M. 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, p. 127, 2013.

[54] 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, Jan. 2019.

[55] M. Casamirra, F. Castiglia, M. Giardina, and E. Tomarchio, "FMECA Analyses of radiological over-exposure accident to patients in brachytherapy," in *Proc. 13th Int. Congr. Intarnational Radiat. Protection Assoc.*, Glasgow, Scotland, 2012, pp. 1–10.

[56] Z. Bluvband, P. Grabov, and O. Nakar, "Expanded FMEA (EFMEA)," in *Proc. Annu. Symp. Rel. Maintainability (RAMS)*, Jan. 2004, pp. 31–36.

[57] 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.

[58] J. A. Carrino, A. Al Muhit, W. Zbijewski, G. K. Thawait, J. W. Stayman, N. Packard, R. Senn, D. Yang, D. H. Foos, J. Yorkston, and J. H. Siewerdsen, "Dedicated cone-beam CT system for extremity imaging," *Radiology*, vol. 270, no. 3, pp. 816–824, Mar. 2014.

[59] European Commission. (2017). *The New Regulations on Medical Devices: Regulation (EU) 2017/745*. Accessed: Feb. 2, 2020. [Online]. Available: https://ec.europa.eu/growth/sectors/medical-devices_en

[60] F. Lopez, C. D. 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, Dec. 2010.

[61] Medical Imaging & Technology Alliance. (2020). *The DICOM Standard*. Accessed: Feb. 2, 2020. [Online]. Available: https://www.dicomstandard.org/current/

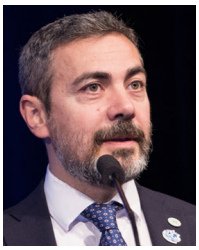
[62] *Number of Computer Tomography (CT) Scanners in Selected Countries as of 2017 (Per Million Popultion)*, Statista, Hamburg, Germany, 2020.

[63] *Medical Devices—Symbols to be Used With Medical Device Labels, Labelling and Information to be Supplied—Part 1: General Requirements*, Standard EN ISO 15223-1, 2016.

[64] *Information Supplied by the Manufacturer of the Medical Devices*, Standard UNI CEI EN 1041, 2013.

[65] World Health Organization (WHO). *Basics of Radiation Protection. How to Achieve ALARA: Basic Tips and Guidelines*. Accessed: Feb. 2, 2020. [Online]. Available: https://apps.who.int/medicinedocs/documents/s15961e/s15961e.pdf

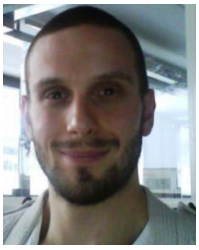
[66] *Evaluation and Routine Testing in Medical Imaging Departments—Part 3-5: Acceptance Tests Imaging Performance of Computed Tomography X-Ray Equipment*, Standard IEC 61223-3-5, 2006.



ERNESTO IADANZA (Senior Member, IEEE) 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, nationally qualified as an Associate Professor in bioengineering. He is a supervisor of more than 190 graduation theses. He has authored more than 160 publications on international books, scientific journals, volumes, and conference proceedings. He is a member of the IFMBE Administrative Council and the Chairman of the International Federation for Medical and Biological Engineering/Health Technology Assessment Division Board (IFMBE/HTAD). He received the IBM Faculty Award, in 2013, and the IFMBE/CED Teamwork Award, in 2019. He is the Editor-in-Chief of the *Clinical Engineering Handbook* (Academic Press, Second Edition, 2020). He is an associate editor of many BME journals.

MARGHERITA ZACCHIA is currently pursuing the bachelor's degree in electronics engineering with the School of Engineering, University of Florence.

DILETTA PENNATI received the M.S. degree in biomedical engineering from the University of Florence, in 2019, where she is currently pursuing the Ph.D. degree in biomedical engineering. She has coauthored 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 Biomedical Imaging Company.

LEONARDO BOCCHI (Member, IEEE) 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 of biomedical engineering at the University of Florence. He has authored more than 100 publications in biomedical engineering. He is also a member of the IEEE TC on Cardiovascular Systems, a Project Evaluator, and a reviewer of the EU and national projects. He acts as a referee of several international journals (among others, IEEE TRANSACTIONS ON MEDICAL IMAGING (TMI), IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING (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 the University of Padua, Italy, in 1987. She is currently a Professor with the University of Florence, and scientific responsible of agreements between the Department of Information Engineering, University of Florence, and University Hospitals in Tuscany, Italy. She has authored articles in the field of biomedical engineering.