Clinical risk evaluation of medical device software: an axiomatic design-based methodology

Fernando Rolli*[1], *Fabrizio* Pecoraro[2], *Daniela* Luzi[2], *Fabrizio L.* Ricci[2], *Elaheh* Pourabbas[3], *Chiara* Parretti[1]

[1]Department of Innovation and Information Engineering, Guglielmo Marconi University, Via Plinio 44 - 00193 Rome, Italy
[2]Institute for Research on Population and Social Policies, National Research Council, Via Palestro, 32 - 00185 Rome, Italy
[3]Institute for System Analysis and Computer Science "A. Ruberti", National Research Council, Via dei Taurini, 19 - 00185 Rome, Italy

Abstract. The increasing complexity of medical device (MD) management software requires the adoption of new methodological approaches that pay particular attention to safety issues. The risk analysis is one of the key activities to be carried out by the manufacturer before the development of the software application as it determines the type of documentation to be provided as well as the activities to be performed to place the MD on the market. After the definition of software requirements and their iterative transformation into architectural items and/or units, the manufacturer defines the safety class of each item. The adoption of an axiomatic design approach facilitates this process. This combination of techniques helps to focus the design of medical device software on non-conformities with a clear link to clinical risk. This objective can be achieved by assessing the complexity of the system to be designed, both in terms of its functional size, and as a level of overall clinical risk. In this multi-dimensional perspective, the software effort expressed in function points provides an estimate of the development cost. While the clinical risk analysis allows to quickly identify critical areas, to intervene with the same promptness and to draft a management plan according to the regulations of the various control authorities.

1 Introduction

1.1 Premise

Clinical risk is the probability that the patient will suffer unintentional damage or discomfort, due to health care, that causes an extension of the period of hospitalization, a worsening of health conditions or even death [1-2]. Medical devices are often made up of heterogeneous components that interact with each other. These are hardware, software and mechanical parts designed to perform specific tasks. The analysis of the risks associated with possible malfunctions follows the entire development cycle of the device [3]. This analysis covers all its components. It is even more effective if the various components are functionally decoupled. This means that the attribution of various user requirements can refer uniquely to a single part of the device. In this sense, Axiomatic Design is a design methodology particularly suitable for defining the overall mapping of risks associated with the user of a specific device and for optimizing the patient flow [4]. This allows to easily detecting the specific non-conformity, during the functional decomposition phase, by analyzing the conditions of non-compliance of the functional requirement. In any case, the management of past anomalies for similar procedures provides a significant support at this stage, particularly if the non-conformities have been catalogued and analyzed in Holistic Non-Conformity Reduction mode [5, 6]. Moreover, the axiomatic approach allows to define an interdomain association that keeps specific users together, functional requirements traced back to a specific user requirement [7, 8]. This leads to the definition of a project in which the individual component, at any level, can be traced back to a specific user requirement. This mapping among different domains allows to associate the risk of malfunction occurring with a multi-dimensional perspective. However, at the same time, the mapping makes it possible to decouple the areas of application [9]. Thus, the solution to a precise problem can be sought in a specific area. Each intervention on the system involves a distinct implementation tool or by redefining the functional requirements of the system to be designed. It also involves an overall redefinition of

* Corresponding author: f.rolli@unimarconi.it

the axioms of independence and information. While the axiom of independence allows the identification of a logically coherent design solution, the axiom of information allows the selection of the design solution with a lower information content [10]. This is equal to defining the least complex solution.

1.2 Scope of application

In this paper, we propose to introduce an axiomatic methodology of risk analysis related to the use of software operating on medical devices (MD). The proposed approach is an extension of the Axiomatic Design of Object-Oriented Software Systems (ADO-OSS) methodology [10, 11]. The process of identifying and managing risks takes place throughout the entire life cycle of the software [3]. Axiomatic Design can be used to define the logical design of the system from high user requirements [12]. The application of the axiom of independence remains unchanged. This axiom guides the decomposition of functional requirements until the identification of the detailed design of the system so that the programmers can develop the system. The axiom of information, on the other hand, is applied on a multidimensional perspective. This perspective allows to carry out several evaluations at the same time. By using function point analysis first, we can evaluate the estimate in terms of function points of the software to be estimated [13, 14]. However, we can also estimate the probability that the single component of the system could present a malfunction in the use phase (O). In the same way, we can attribute to the various elementary components of the system the probability that the same non-conformity will be detected (D), as well as provide with an estimate of the impact on patients and health workers (S). This information can be used to feed risk re-composition techniques such as Fault Tree Analysis (FTA) [15] and Health Failure Mode and Effects Analysis (HFMEA) [16, 17]. These techniques are particularly suitable for mapping possible situations of non-compliance of systems, allowing the start of activities to minimize the overall risk [18-21]. In this way, the axiomatic approach not only allows to design a software system that is logically consistent with the functionality to be performed but the system itself will be robust with respect to processing complexity and risk analysis associated with the occurrence of a malfunction. In this paper, we will closely monitor the application of this axiomatic approach, in the specific case, of the implementation of a software for the management of a drug infuser. For this case study, an approach based on axiomatic design is proposed to facilitate the identification of possible malfunctions and consequently contribute to the reduction of clinical risk [18, 22].

2 Axiomatic clinic risk management

2.1 Clinical risk management related to software malfunction

Risk management follows the entire product life cycle [3]. It represents the set of corrective and preventive actions aimed at eliminating and/or mitigating the occurrence of risky events in a system [23, 24]. In the field of medical devices, these events can also have very serious consequences for patients and operators. For this reason, the competent supervisory authorities in Europe and the Food and Drug Administration (FDA), in United States, have issued guidelines on the risk analysis of medical devices. Furthermore, manufacturers are obliged to subject these devices to a conformity assessment to demonstrate that they meet the legal requirements to ensure that they are safe and work as intended. Conformity assessment usually involves an audit of the manufacturer's quality system and a review of the manufacturer's technical documentation on the safety and performance of the device [3]. These security certificates are addressed to the product, but also to its individual components, such as software. [3].

2.2 Introduction to the HFMEA methodology

The HFMEA methodology is particularly suitable to allow the building of a management plan for the clinical risks associated with a specific medical device [23, 24]. HFMEA analysis is usually carried out using brainstorming techniques within multidisciplinary teams. Each team member brings his or her own expertise to a continuous exchange of ideas and design solutions. In its conventional formulation, HFMEA is launched since anomalies historically detected in the system for similar procedures or identified during testing. The following coefficients are determined for each possible anomaly or fault [25]:

- Coefficient of gravity of the selected event (**S**);
- Coefficient associated with the probability of occurrence of the malfunction (**O**);
- Coefficient of detection of the event itself (**D**).

These coefficients are estimated by the members of the multidisciplinary team based on specific tables, which consider the operating context of the software to be implemented. They form the basis for calculating an overall risk coefficient for the malfunction, called RPN (Risk Priority Number). $\boldsymbol{RPN = S * O * D}$ [22]. The HFMEA analysis distinguishes between an "*As is*" phase, which represents the current state of risks associated with the system, and a "To be" phase. This second phase represents the state of the system after the introduction of improvements aimed at minimizing the overall value of the RPN coefficient. In fact, for each failure detected during the "*As is*" phase, one or more actions will be identified to allow its resolution. Each action will be associated with the working group responsible for its execution. Then, the RPN (Risk Priority Number) will be re-determined according to the adoption of the particular action taken. The whole process is cyclical. It is completed when the overall RPN value that is considered adequate to commercialize the

product is achieved, and in any case when all non-conformities of high severity are eliminated or made predictable.

2.3 Methodological approach

2.3.1 Axiomatic Design of Object-Oriented Software Systems

The management of risks associated with the release of a software system in the medical field can be carried out following an axiomatic approach. This approach is particularly well suited to the operating environment. In fact, it could be easy to extend this analysis, also, to the mechanical and hardware components of the medical device. In this way, the causes of malfunction could be verified, depending on the interactions among different components. Moreover, it should be noted that the Axiomatic Design (AD) methodology was created in the manufacturing sector [26]. It was later extended to other sectors, such as the design of information systems. Unlike other engineering sectors, the implementation of software systems is strongly conditioned by the creativity and experience of its designers. In this context, AD provides an approach based on quantitative measurements and comparisons that, if correctly applied, can guide designers to identify optimal implementation solutions. Suh [10, 11] proposed a methodology for developing information systems called Axiomatic Design of Object-Oriented Software Systems (ADOOSS). It combines object-oriented programming techniques (OOP) and AD design. OOP is a programming paradigm, in which a system is conceived as a set of objects that interact with each other. Each object is constituted by a set of attributes and functions, called methods. The set of several objects is defined as class [12, 13]. With this methodology, Suh [10] pointed out that programming techniques can be optimized by preceding the software implementation by a conceptual model of system built based on AD decomposition techniques of the relations functional requirements and data structures. This process was formalized in the so-called model V of Figure 1. It is based on the application of the axioms of independence and information. The independence axiom ensures that the decomposition performed is logically consistent, while the information axiom sets an upper limit to the level of complexity of the system, as a minimization of the information processed by the system.

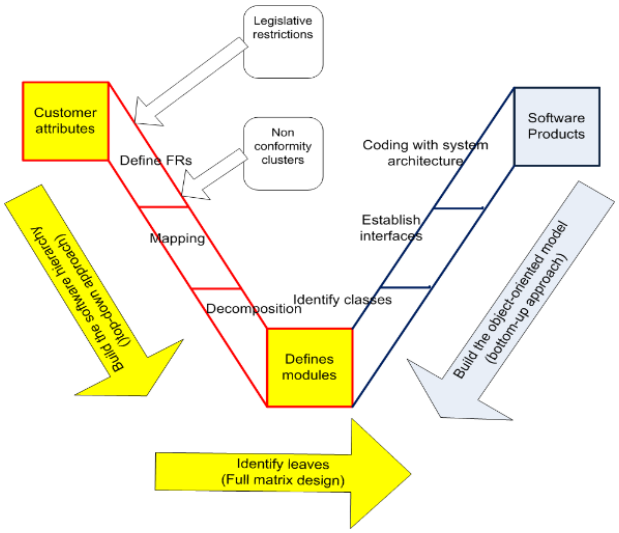

Fig. 1. Application diagram of Axiomatic Design of Object-Oriented Software Systems. Source [10]

2.3.2 Considerations around the information axiom for applications with high safety standards

In order to allow risk management over the entire life cycle of the software, it is necessary to extend the application of the information axiom. Other cases of reformulation of the Information Axiom as a multi-criteria analysis tool are available in literature. The approach proposed by Kulak et al. [25] is very interesting. They propose a combination of AD and fuzzy logic analysis as a tool to support decision-makers in the healthcare field. In this specific case, however, the proposed methodology works mainly in the software design phase. In fact, the proposed reformulation of the Information Axiom allows identifying the parameters required to implement an effective and efficient clinical risk analysis strategy. This extension does not operate on the axiom of independence, whose application remains unchanged. In the software field, the common use of the information axiom is very limited [13]. Often its application can be perceived as a cost in terms of resources used to produce documentation, probably even useless. Especially in the field of agile programming, it is preferable to neglect its applicability. As far as the health-care sector is concerned, overall, the variable cost of the software project has a lower priority than the safety standards that the final product must guarantee. For a non-critical management project, the application may be put into production, starting with a prototype that partially covers the required functions and with a test plan that has not been fully executed. Patients and operators cannot be endangered in the healthcare sector. In Europe and the United States, vigilance authorities oblige MD manufacturers to high levels of safety [3]. This means that the applicability of the axiom of information becomes again not only economically advantageous, but above all necessary.

2.3.3 Re-formulation of the information axiom for compatibility with failure mode and effects analysis

Figure 2 illustrates an example of an extended application of the information axiom. This configuration of the axiomatic model has been designed to be compatible with the ADO-OSS methodology and the HFMEA risk analysis technique. Four system entropy measurement parameters have been introduced. They are the following:

- Function point for estimating the functional size of the software (FP) [27, 28];

- Coefficient of gravity associated with the non-execution of the selected functional requirement (S);

- Coefficient associated to the probability of occurrence of the malfunction of the adopted implementation solution (O);

- Coefficient of detection of the malfunction of the adopted implementation solution (D).

The application of axiomatic decomposition involves a mapping process among three conceptual domains of Figure 2 [9]. In this context, the operational specifications of the device constitute the customer attributes (CA) of the process. Below, we can define MD use cases as high level functional requirements (FR). Design parameters (DP) are created by designers. They correspond to the collaborations (interactions) among various Use Cases. In this way, the first level decomposition describes the network of interactions among Use Cases [9, 12]. This network of interactions is graphically represented by a design matrix. This matrix allows to set the evaluation of the information axiom with respect to a pair of parameters (FP, S). While function points (FPs) can be calculated since functional requirements (FRs) [27, 28], the coefficient of severity associated with the non-execution of the selected functional requirement (S) can be estimated based on a matrix of evaluation of the severity of the clinical risk introduced in 2003 by the Italian Ministry of Health [23, 24]. Finally, we can set the process variables (PV) to coincide with the applications of libraries that implement the functionalities to be implemented. They represent the tools of software implementation. The correlation matrix between Physical domain and Process Domain lays the foundations for a second evaluation of the information axiom with respect to the pair of parameters (O, D). The coefficient of occurrence of the malfunction (O) is related to the reliability of the technical solution to be adopted. Instead, the detection coefficient (D) of the malfunction depends on the possibility that the error is detected before it produces substantial damage to the patient. Both parameters can be estimated since clinical risk assessment matrices introduced in 2003 by the Italian Ministry of Health [23, 24].

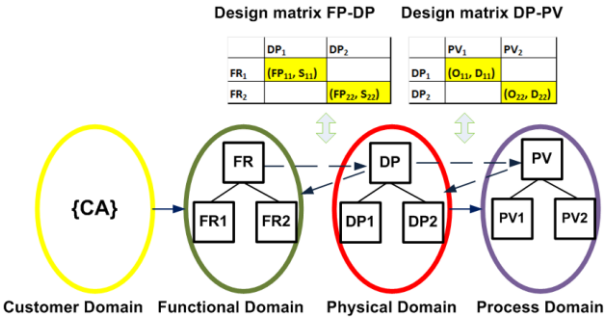

Fig. 2. Multi-criteria evaluation of the information axiom

2.3.4 Axiomatic decomposition

The axiomatic design is a top-down design. It continues with successive decompositions of functionalities up to a level of detail that enables its implementation by developers. In the last stage of decomposition, the decomposed functional requirements (FR) are elementary functions, while the design parameters (DP) are data sets, corresponding to the objects of the upper classes [9-12]. Instead, the project variables (PV) are codes, algorithms, subroutines, machine codes, compilers to accomplish the DPs [10, 11]. The building of mapping matrices is carried out through a multiple zigzagging process among tree domains, as shown in Figure 2. This multiple zigzagging process has the advantage of decoupling the analysis of the different design aspects.

2.3.5 Evaluation of the information axiom as a multi-criteria analysis

The interdomain mapping process involves the evaluation of the information axiom with respect to four different parameters (FP, S, O, D). Table 1 illustrates how to apply the information axiom with respect to the two interdomain mappings in Figure 2. In short, this configuration allows the execution of a multi-criteria analysis. The information axiom becomes the tool not only to minimize the information complexity in function points, but also to design a system with a lower risk level than the HFMEA parameters (S, O, D).

Table 1. Evaluation of the information axiom as a multi-criteria analysis

From	To	Measurement parameter of the information axiom	Scope
Functional Domain	Physical Domain	Function Point	Measure the software size (FP)
Functional Domain	Physical Domain	Risk class	Estimate the risk severity coefficient associated with FMEA (S)
Physical Domain	Process Domain	Probability of malfunction	Estimate the coefficient associated with the probability that the anomaly event will occur for FMEA (O)
Physical Domain	Process Domain	Probability of detecting malfunction before it has consequences during use	Estimate the coefficient associated with the probability of detecting the malfunction before it produces consequences in use for FMEA (D)

2.3.6 General outline of the process

At this point we can present the general scheme of the process that combines these two methodologies. This mixed approach follows a general scheme of type V model (Figure 3). The axiomatic decomposition of functional requirements feeds the HFMEA process of identifying the software failure modes. Instead, the evaluation of the clinical risk is the activity of recomposition of these failure modes, with a reverse process. A team of multidisciplinary experts can provide an estimate of the impact of the elementary failure modes with the final patient. In the same way, the improvement actions aimed at reducing the RPN coefficient follow the same path, from the bottom to the top of Figure 3. The process is overall iterative. It is interrupted when a solution is considered acceptable with respect to the performance and safety standards, required to receive marketing authorization from the competent control authorities (Safety class) [3].

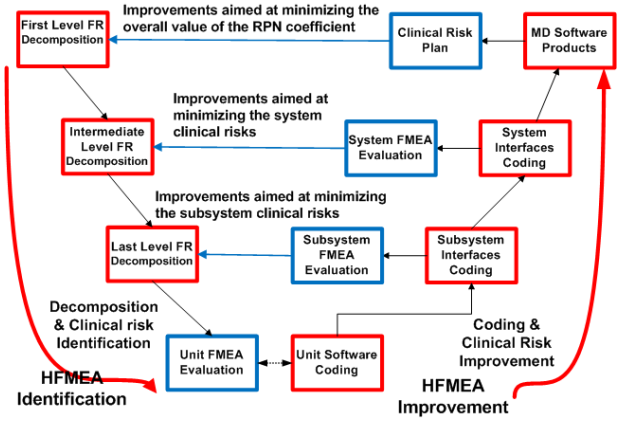

Fig. 3. General clinical risk evaluation process based on a mixed AD/HFMEA approach

3 Case study

3.1 Syringe infusion pumps

Infusion pumps are one of the most widely used medical devices in healthcare facilities [29]. They control the infusion of liquid drugs into the bloodstream or may allow the patient to be fed artificially by means of a probe. For this case study we have taken as reference the general structure of the syringe pumps. This type of infuser is intended for the controlled administration of liquids through a mechanical tool (syringe). The infusion rate is set by the healthcare professional [29]. These pumps can use the syringe piston to calculate the reciprocity between the controlled rectilinear displacement and the infusion rate. A screw under the syringe allows the amount of fluid injected to be precisely adjusted to allow for an almost continuous flow. The mechanism is started by a direct current electric motor. The main difference between this and the other devices lies in the ability of the syringe pumps to infuse very low quantities of fluid simply by replacing the syringe used and thus the capacity of the device. It is measured by the control device in terms of volumes per unit of time. In these pumps the flow control is based on methods of measuring the viscosity of the liquid.

3.1.1 Syringe infuser components

A syringe infuser consists essentially of two fundamental components: the pump and a syringe (Figure 4) [29, 30]. The two components are connected to each other by a special cannula, called outflow. The pump is a hardware device with a control software system. The syringe is, on the other hand, a mechanical instrument.

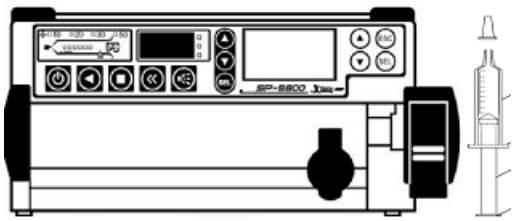

Fig. 4. Syringe infuser pump 35205 (GIMA) [15]

3.1.2 Fault alerts

Standard EN 60601-2-24 states that in the event of an anomaly being detected, the infusion pumps must activate a visual and acoustic alarm signal [31]. The visual signal must be continuous, while the acoustic signal may be intermittent with a duration of not less than two minutes. Healthcare professionals cannot intervene to disable these signals. For syringe pumps, the main detectable anomalies are the following: incorrect syringe insertion; occlusion; pressure level; pressure drop; end of infusion; end of stroke; prolonged pause;

insufficient battery charge; pump malfunction [30, 31]. Therefore, the device management software must also process signals relating to mechanical and electrical components.

3.2 Infusion management process

3.2.1 Use cases associated with the infuser management process in pediatric oncology

In the diagram shown in Figure 5, the main use cases of the general scenario relating to the home administration of drug infusion are highlighted. The operational context concerns pediatric oncology. Furthermore, the actors of the process are identified. They are the device operator and service center. The device operator can be a healthcare professional or a child's parent. The following use cases reported represent the high-level functioning of a generic syringe infuser in this specific operating context:

1) Initialization of the administration parameters (FR1)

2) Drug administration (FR2)

3) Purge (FR3)

4) Bolus (FR4)

5) Alert management / reporting (FR5)

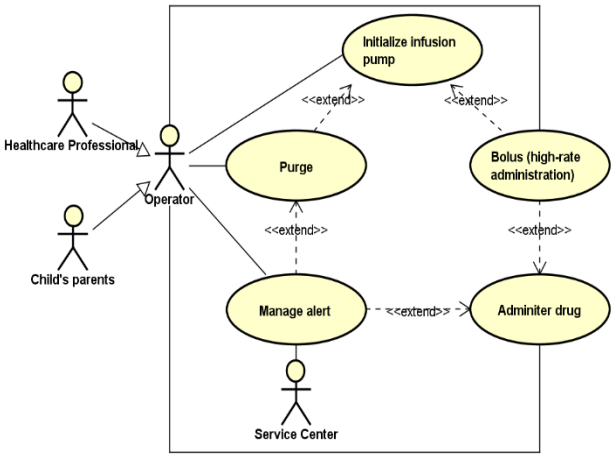

Fig. 5. General process scenario in home administration of drug infusion in pediatric oncology with syringe infuser pump

3.2.2 Axiomatic decomposition of use cases

Axiomatic design allows to proceed to a decomposition of the functional requirements in terms of cases of use of the system. This decomposition can be extended to define the logical design of the system. This level allows programmers to initiate the software implementation process. For the sake of brevity, we will not proceed with further decompositions. For the same reason, we will neglect the estimation of the size of the software in terms of function points. The use cases of the previous paragraph (3.2.1) can be represented by the design matrix of Table 2. This matrix is built by placing the use cases along the lines of a square matrix. The corresponding columns show the reciprocal collaborations or interactions [9, 12]. At this point, we assume the following condition: a collaboration is only possible if the case of use indicated in the column of the matrix activates any event, which changes the status of the case of use indicated in the corresponding row. The cells that show a collaboration between use cases show the symbols S_{ij}. These symbols measure the risk class of the specific processing or interaction between use cases. For example, S_{11} is the risk class associated with initialization of the infusion process (FR1). However, S_{31} represents the risk class of the event generated by the use case FR1 that triggers processing in the use case related to purging operations (FR3).

Table 2. Design matrix of use cases related to general scenario of Figure 5 in home pediatric oncology

	DP1 Collaboration Start	DP2 Collaboration Administer drug	DP3 Collaboration Purge	DP4 Collaboration Bolus	DP5 Collaboration Manage alert
FR1 Start	S_{11}				
FR2 Administer drug		S_{22}			
FR3 Purge	S_{31}		S_{33}		
FR4 Bolus	S_{41}	S_{42}		S_{44}	
FR5 Manage alert	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}

3.2.3 Application of independence and information axioms for the project matrix of use cases

First functional level corresponds to FR0. It is the management of the infusion process for a syringe pump. For the sake of simplicity, we do not consider the mode of functional decomposition in the use cases shown in Figure 5. We refer this in-depth to the existing literature on the subject [9, 12]. Therefore, let us start again from the evidence that the applied functional decomposition led us to the matrix in Table 2. This matrix is triangular. Therefore, the axiom of independence is respected. With regard to the axiom of information, we must provide an estimate of the parameters of severity of the clinical risk (S_{ij}) associated with a possible malfunction of the device. Taking as reference what is prescribed by the Decree of the Italian Ministry of Health of March 5, 2003 [23, 24], we can attribute to S_{ij} whole values ranging from 1 to 5. The rules for assessing the level of severity of clinical risk are defined by the ministerial Table 3.

Table 3. Matrix for assessing the severity of a malfunction of a device or equipment in the health sector [24]

Severity		
Score	**Description**	**Assessment**
1	**No damage**	Matrix for assessing the severity of a malfunction of a device or for monitoring the patient.
2	**Mild damage**	The event has caused temporary damage to the patient and has required additional interventions or treatments or an extension of the stay above the average value for specific pathology.
3	**Average damage**	The event caused temporary damage to the patient (temporary disability) and made it necessary to start or extend the stay.
4	**Severe damage**	The event caused permanent damage to the patient (permanent disability) or generated an event close to death
5	**Death**	Patient's death

3.2.4 Functional decoupling

The functional decomposition of paragraph 3.2.3 can also be reversed as a mapping between the Physical domain and the Process domain. Following the diagram in Figure 2, we can construct the matrix of application interventions in Table 4. This matrix shows the interactions of the design matrix in Table 2 along the rows. Not necessarily or not only through software applications, it is possible to execute the use cases that have been defined in advance. If we consider the specific case of a syringe infuser, the administration of the drug can also be very accurately regulated with a mechanical instrument. Often this type of infusion is combined with special syringes that use a manual regulation of the flow by means of a screw. In other cases, sets of syringes are supplied that are calibrated to allow the administration of specific drugs with specific speeds. The matrix in Table 4 shows as an exclusively mechanical solution the execution of the case of use related to the administration of the drug (Administer drug Tool). In other situations, the implementation interventions concern the development of software procedures (App). This is possible because the axiomatic methodology allows the decoupling between the functional side, represented by the design matrix of the use cases (Table 2) and the implementation side of Table 4 [9]. The matrix of implementation actions shows the solutions to be adopted, regardless of whether it is a software procedure, an electronic device or a manually adjustable mechanical mechanism. Of course, the whole design process is iterative. Therefore, the adoption of a specific solution can change the configuration of the functional requirements [9].

Table 4. Project matrix of implementation interventions

	PV1 Start App	PV2 Administer drug Tool	PV3 Purge App	PV4 Bolus App	PV5 Manage alert App
DP1 Collaboration Start	(O_{11}, D_{11})				
DP2 Collaboration Administer drug		(O_{22}, D_{22})			
DP3 Collaboration Purge	(O_{31}, D_{31})		(O_{33}, D_{33})		
DP4 Collaboration Bolus	(O_{41}, D_{41})	(O_{42}, D_{42})		(O_{44}, D_{44})	
DP5 Collaboration Manage alert	(O_{51}, D_{51})	(O_{52}, D_{52})	(O_{53}, D_{53})	(O_{54}, D_{54})	(O_{55}, D_{55})

3.2.5 Axioms of independence and information application to the project matrix of implementation measures

As for paragraph 3.2.3 we restart from the evidence that the matrix is triangular in Table 4. Therefore, the axiom of independence is respected. As far as the information axiom is concerned, the entropy of the system can be evaluated with respect to a pair of values (O_{ij}, D_{ij}). O_{ij} represents the probability that the single implementation intervention can be a cause of malfunction. D_{ij} is the level of detection of the same malfunction. Both parameters of the pair (O_{ij}, D_{ij}) can assume integer values varying from 1 to 5. Table 5 and Table 6 illustrate the rules for assigning evaluation scores for both parameters. Both tables transpose the requirements of DM 5 March 2003 on clinical risk management [23, 24].

Table 5. Matrix for evaluating the occurrence of a malfunction for a device or apparatus in the health sector [24]

Occurence		
Score	**Description**	**Assessment**
1	**Remote** (no known events)	1 in 10,000 cases may occur
2	**Low** (possible but no known data available)	1 out of 5,000 cases may occur
3	**Moderate** (documented but rare)	1 out of 200 cases may occur
4	**High** (documented and frequent)	1 out of 100 cases may occur
5	**Very high** (documented and almost certain)	1 out of 20 cases may occur

Table 6. Matrix for evaluation of the detection of a malfunction for a device or equipment in the health sector [24]

Detection		
Score	**Description**	**Assessment**
1	**Very high** (error always detected)	9 times out of 10 the event occurs
2	**High** (error probably detected)	7 times out of 10 the event occurs
3	**Average** (moderate probability of error detection)	5 times out of 10 the event occurs
4	**Low** (low probability of error detection)	2 times out of 10 the event occurs
5	**Remote** (virtually impossible to detect)	0 times out of 10 the event occurs

3.3 Clinical risk assessment

The axiomatic decomposition of use cases enables a robust infuser design to be defined. This design includes both the electronic components, the management software and the mechanical parts. Each of these specific components is, down to the most basic level of detail, linked to a specific functional requirement. This overall mapping allows us to identify possible operational criticalities and to reconfigure the project itself, in order to minimize its occurrence. The overall process is iterative. It is based on the application of the axioms of independence and information. In particular, the information axiom allows to associate the complexity of the system to the Risk Priority Number (RPN). Therefore, the designer's objective is to minimize the value of RPN. This iterative process stops, when the pre-set clinical risk mitigation goals are achieved. These goals must guarantee, at least, the safety standards set by the control authorities to obtain authorization for the marketing of the medical device in its entirety. However, the manufacturer can set a higher product quality level than the service levels set by the guidelines of the authorities. In this case, we have that: Clinical risk mitigation goals = FR satisfied / resources spent [32]

3.3.1 Construction of the HFMEA matrix

The construction of the FMEA matrix is the final act for the definition of the clinical risk management plan. Table 7 illustrates how to analyze the malfunction associated with the occlusion of the outflow. This problem is associated with the case of use related to the administration of the drug (FR2). The effects are related to discontinuation of treatment. The indicators of severity (S), detectability (D) and probability of occurrence (O) should be estimated based on the specific treatment for which the device is intended [3]. The corrective actions to be taken concern the use of a sensor that controls the flow of the drug. In the event of an occlusion, the management software must activate visual and acoustic alarms that cannot be deactivated by healthcare professionals. Only the resolution of the problem can disable the alarm [31]. FMEA also identifies the person responsible for the problem resolution intervention. In this case, this is a situation that must be managed by the healthcare professionals who are treating the patient using the infuser.

Table 7. HFMEA matrix scheme

Use case	Failure mode	Effects	Severity (1-10)	Occurrence (1-10)	Detection (1-10)	RPN	Actions	Responsability
FR2 Administer drug	Occlusion of the outflow	Interruption of drug administration	S_{22}	O_{22}	D_{22}	$S_{22}*O_{22}*D_{22}$	Visual acoustic signaling of the device	Healthcare worker

4 Conclusions

In this context, Axiomatic Design is the most appropriate tool to allow the integrated design of a device consisting of non-homogeneous components. This is possible because the axiomatic methodology allows the decoupling between the functional side, represented by the design matrix of the use cases (Table 2) and the implementation side of Table 4. The implementation matrix shows the solutions to be adopted, whether it is a software procedure, an electronic device or a manually adjustable mechanical mechanism. Of course, the whole design process is iterative. So, the adoption of a particular solution can change the configuration of the functional requirements. This same process makes it possible to build a clinical risk management plan based on the information axiom. This axiom allows the complexity of the system to be assessed since the Risk Priority Number (RPN). This assumption allows us to simultaneously implement an infuser control software application and build a clinical risk management plan.

References

1. L. Kohn, J. Corrigan, M. Donaldson, *To err is human: building a safer health system*, National Academy Press, Washington, D.C. (1999)
2. Decreto Ministeriale 5 Marzo 2003, Ministero della Salute https://www.gazzettaufficiale.it/eli/id/2003/07/03/03A07239/sg
3. F. Pecoraro, D. Luzi, *The Integration of the Risk Management Process with the Lifecycle of Medical Device Software*, Methods Inf Med (2014)
4. Arcidiacono G, Matt DT, Rauch E, 2017, "Axiomatic Design of a Framework for the Comprehensive Optimization of Patient Flows in Hospitals", Journal of Healthcare Engineering, Vol. 2017, Article ID 2309265
5. C. Cavallini, A. Giorgetti, P. Citti, A. Meneghin. *Sviluppo di un approccio olistico per l'analisi e la risoluzione delle non conformità*, AISS, 3, 1 (2012)
6. F. Rolli, A. Giorgetti, P. Citti, *Integration of Holistic Non-Conformities Management and Axiomatic Design: a case study in Italian Income*

Tax Returns Management, Proc. CIRP **34**, 256-262 (2015)

7. B. Pacifici, C. Parretti, A. Girgenti, A.,P. Citti, *Axiomatic Design for an Efficient Development of Optimized RPM Systems*, MATEC Web of Conferences the 12th International Conference on Axiomatic Design (ICAD 2018)
8. B. Pacifici, C. Parretti, G. Arcidiacono, A. Giorgetti, A. Girgenti, *Conceptual framework for user based RPM*. In Proc. International Conference on Industrial Engineering and Operations Management (2017)
9. C. Parretti, F. Rolli, E. Pourabbas, P. Citti, *Axiomatic Selection of Health and Social Care Web Services on the Basis of Use Cases*, the 12th International Conference on Axiomatic Design (ICAD 2018)
10. N.P. Suh, *Axiomatic Design - Advances and Applications*, (Oxford University Press, 2001)
11. S.H. Do, N.P. Suh, *Object-oriented software design with axiomatic design*, Proc. CIRP 49, 278-84 (2000)
12. P. Pimentel, C. Stadzisz, *A Use Case based Object-Oriented Software Design Approach using The Axiomatic Design Theory*. Proceedings of ICAD2006 Fourth International Conference on Axiomatic Design, 4:1-8 (2006)
13. F. Rolli, A. Giorgetti, P. Citti, M. Rinaldi, *Information content evaluation to obtain robustness of the management in Italian fiscal process (Part 2): optimization of Italian income certification process of the year 2016*, Proc. CIRP 53, 63-69 (2016)
14. F. Rolli, A. Giorgetti, P. Citti, M. Rinaldi, *Improvement of the compilation process of the Italian income certifications: a methodology based on the evaluation of the information content (Part 1)*, Proc. CIRP 53, 56-62 (2016)
15. G. Arcidiacono, *Development of a FTA versus Parts Count Method Model: Comparative FTA*, Quality and Reliability Engineering International Journal, Vol. 19: pp. 411-424 (2003)
16. M. Pallaver, S. Do, *Failure mode analysis as an implementation of axiom 2 in the axiomatic design functional decomposition process*, (Proceedings of ICAD 2013)
17. G. Arcidiacono, G. Campatelli, *Reliability Improvement of a Diesel Engine Using the FMETA Approach*, Quality and Reliability Engineering 20 (2):143 - 154 (2004)
18. G. Arcidiacono, A. Pieroni, *The Revolution Lean Six Sigma 4.0,* International Journal on Advanced Science, Engineering and Information Technology, Vol. 8, Issue 1 (2018)
19. G. Arcidiacono, A. Giorgetti, A. Ciappi, *An axiomatic design framework for reliability improvement*, ACM International Conference Proceeding Series proceeding ICSCA 2017, pp. 214–217
20. A. Giorgetti, G. Arcidiacono, A. Ciappi, R. Barbieri, P. Citti, *HNCR model following robust approach. Quality and Reliability Engineering International*. 34, 1271–1288 (2018)
21. A. Giorgetti, A. Girgenti, P. Citti, M. Delogu, *A novel approach for axiomatic-based design for the environment in Axiomatic Design in Large Systems: Complex Products, Buildings and Manufacturing Systems* (Springer International Publishing, 2016), pp. 131–148
22. B. Goo, J. Lee, S. Seo, D. Chang, H. Chung, *Design of reliability critical system using axiomatic design with FMECA*, International Journal of Naval Architecture and Ocean Engineering (2019)
23. Commissione tecnica sul rischio clinico, *Risk Management in Sanità*. Ministero della Salute (2004) http://www.salute.gov.it/imgs/C_17_pubblicazioni_583_allegato.pdf
24. F. Camilli, *La Gestione del rischio clinico attraverso la FMEA*, Azienda Sanitaria Locale Rieti (2014)
25. O. Kulak, HG. Goren, AA Supciller, *A new multi criteria decision making approach for medical imagingsystems considering risk factors*. Applied Soft Computing, Volume 35, Pages 931-941 (2015)
26. Arcidiacono G, Brown C, Bucciarelli L, Melosi F, 2016, "Axiomatic Design of Production Systems for Performance Improvement: A Project Identification and Prioritization Model", *Axiomatic Design in Large Systems*, Springer, pp. 251-272
27. A. J. Albrecht, *Measuring Application Development Productivity*, (Proceedings SHARE/GUIDE IBM Applications Development Symposium, 1979)
28. IFPUG - *Function Point Counting Practices Manual*, Release 4.1 - Westerville - Ohio, 1999
29. G. Calcagnini, F. Censi, M. Floris, M. Triventi, M. D'Alessandro, P. Cianfanelli, G. Scavino, P. Bartolini, *Valutazione delle interferenze elettromagnetiche indotte dai telefoni cellulari GSM su pompe di infusion*e, (Istituto superiore di sanità, Rapporti ISTISAN 05/15, 2005)
30. GIMA Professionals Medical Products, *Manuale d'uso e manutenzione Pompa a Siringa 35205*, https://www.gimaitaly.com/DocumentiGIMA/Manuali/IT/M35205IT.pdf
31. IEC, *Medical electrical equipment – Part 2-24: Particular requirements for the safety of infusion pumps and controllers* (1998) https://www.sis.se/api/document/preview/124600/.
32. E. Benavides, *Advanced Engineering Design*, Woodhead Publishing in Mechanical Engineering (2011)