Metamodel for Safety Risk Management of Medical Devices Based on ISO 14971

***Abstract*—The integration of information technologies into medical systems has led to an increase in digitalization, which results in enormous possibilities, but also challenges in system development. The ever-growing complexity of modern medical devices (MD) requires a system-based development, which must be supported by Model-Based Systems Engineering (MBSE) approaches. Indeed, risk management (RM) and safety analysis must begin in the early development phases to ensure MD's dependability and facilitate the regulatory process. This paper proposes a metamodel that describes the safety and RM concepts related to the medical domain. This metamodel enables safety and quality experts to analyze MD and demonstrate compliance with the recommendations of ISO 14971. We have validated the proposed metamodel using the academic example of a wearable system designed for real-time EEG-based subject monitoring.**

***Index Terms*—Metamodel, risk management, medical devices, ISO 14971**

I. Introduction

The digitization and growing intelligence of modern medical devices (MD) is creating the immense potential for future medicine and presenting challenges for the development of MD [1]. In this context, Model-Based Systems Engineering (MBSE) [2] is a promising approach capable of mastering complexity in the development of modern MD, especially in the early stages. Furthermore, the systematic use of models can be advantageous in identifying and mitigating potential risks [3] [4]. The principle of concern separation is widely used in the field of MBSE to address the aforementioned development challenges. This principle has contributed significantly to the creation of Domain-Specific Modeling Languages (DSML), which offer concepts that are tailored to specific application domains or concerns, such as safety modeling in the medical domain.

The fast-growing MD market is subject to rigorous regulatory controls at the national and international levels. The primary objectives of these regulatory controls are to achieve a high level of protection of health for patients and to ensure smooth functioning of the market for MD products. Risk management (RM), a key activity for the development and certification of MD, plays a vital role in successfully passing the MD regulatory process and in promoting its safety [5]. ISO 14971 [6] describes the main principles of RM for MD. First published in 2000, it establishes a framework for risk analysis, evaluation, control, and review for MD. ISO 14971 is closely related to other safety standards such as ISO 13485 [7], which sets requirements for a specific quality management system for MD, and IEC 62304 [8], which outlines the life cycle processes for MD software. ISO 14971 is also recognized by regulatory bodies (e.g., the US Food and Drug Administration and the European Union's Medical Device Regulation) as a key tool for ensuring the safety and effectiveness of MD. Compliance with ISO 14971 is often a requirement to obtain regulatory approval for MD.

Ensuring MD safety thus represents a further major challenge for quality and safety experts [9]. The question arises as to how RM can be supported in the early stages of MD development within the MBSE to create future products in a safe manner. To be able to analyze the challenges of safety in the medical domain, a modeling language is required that addresses safety-relevant aspects of MD.

Certain efforts show the benefits of MBSE-based approaches for RM in the healthcare context [3] [4] but, in practice, support for MBSE is not well elaborated. Hence, the goal of this paper is to create a basis for the safety-oriented modeling of MD by specifying a language to model and analyze risks according to ISO 14971. The main contributions of the paper are as follows:

- We propose a metamodel that describes concepts for safety modeling in the medical domain based on ISO 14971 to identify and mitigate potential risks in the early stages of MD development.
- We validate the proposed metamodel by modeling the risks of a wearable system for real-time monitoring of brain activity.

The paper is organized as follows. In Section II, we analyze the state of the art in DSML application for safety analysis and RM in the medical domain. In Section III, we introduce our metamodel for ISO14971-based RM. Then we validate the metamodel in Section IV by modeling the risks of an EEG-based MD taken from the literature. In Section V, we discuss the main advantages, limitations, and perspectives of our metamodel and draw conclusions.

II. Problem Statement and Related Works

The International Council on Systems Engineering (INCOSE) has suggested that the near future of system engineering is likely to be based on models. Unlike the traditional document-oriented approach, MBSE enables the integration of several domains in a more consistent and reusable way [2]. A system model can be expressed by combining three key aspects of MBSE: a method, a tool, and a modeling language. To standardize the description of the system model, the Object Management Group (OMG) developed the Unified Modeling Language (UML) [10] and the Systems Modeling Language (SysML) [11] where UML serves as the basis for SysML.

A typical modeling language comprises metamodel, concrete syntaxes, and semantics. The former defines the different model elements, their attributes, and their relationships. Since there is a wide range of potential application domains, the development of a modeling language that can cover all existing aspects is not realistic. Therefore, extension mechanisms supported by metamodels are used to add new concepts and/or notations to the existing modeling languages. For example, the Architecture Analysis and Design Language (AADL) [12] is developed by the Society of Automotive Engineers (SAE) to model the software and hardware architecture of embedded real-time systems. It supports analysis of a system architecture in the context of performance-critical properties and also enables defining reliability models of components. Based on UML, SysML and AADL, the Electronics Architecture and Software Technology - Architecture Description Language (EAST- ADL) [14] was created and maintained for the automotive domain by the EAST-ADL Association in cooperation with the European FP7 MAENAD project [13]. EASL-ADL offers facilities to model the architecture and behavior of automotive embedded systems with the aim of safety analysis and fault/error propagation modeling. The OMG UML profile for Modeling and Analysis of Real-Time Embedded Systems (MARTE) provides support for modeling real-time embedded systems [15]. It allows annotating models with the information essential to performing model-based analysis, verification and validation. The aforementioned DSML are largely used to model the architecture of safety-critical embedded systems (e.g. automotive, avionic) and thus serve as a base for safety- and reliability-oriented DSML.

The Risk Analysis and Assessment Modeling Language (RAAML) [16] and Safe Modeling Language (SafeML) [17] define extensions to UML/SysML needed to support functional safety and reliability analysis of critical systems. Besides the method support, linkages to the UML/SysML model are also provided, enabling integration with and traceability to the analyses. In addition, RAAML also has an extension dedicated to ISO 26262 [18] oriented safety analysis for the automotive domain. [19] presents an extension for MARTE that adds dependability analysis and monitoring oriented towards fault-tolerant systems. The CHESS project [20] suggests a complete modeling toolchain for dependable systems: it uses a set of modeling languages and model transforms to assist in the analysis of a system design. The aforementioned DSML are mostly compliant with generic safety and RM standards.

The analysis of the literature shows that such safety-critical domains as avionics and automotive benefit the most from the development and use of dedicated DSML which aim at supporting system-level risk analysis and safety assurance and helping manufacturers better comply with the mandatory safety standards (e.g., ISO 26262). Very few solutions are oriented to the medical application and even fewer support ISO 14971. In the medical domain, while ISO 14971 is well-elaborated in its comprehensiveness and precision, its integration with the development process is an exercise left to individual MD manufacturers. This has led to significant variations in safety outcomes. [3] extends the AADL toolkit for model-based MD hazard analysis. The authors suggest the approach for developing model annotation libraries that instantiate AADL to support ISO 14971-based RM and also report on the model-based safety analysis of the medical patient-controlled analgesic pump device. [4] suggests using SysML activity models to link the steps of ISO 14971 to the technical processes for the development of the system of ISO 15288. [21] describes the RM SysML profile for the IBM Rational Rhapsody software suite that includes interconnected classical safety analysis methods, control measures, and evaluation model elements in compliance with medical standards. However, there is no clear indication of how the classical safety assessment methods implemented in the framework refer to the risk analysis flow (given as the relationship between hazard, sequence of events, hazardous situation, and harm) described in ISO 14971.

The analyzed state of the art shows the lack of a metamodel or DSML that extends generic functional safety concepts to support ISO 14971-oriented safety analysis and RM in the early stages of MD modeling.

III. Risk Management Metamodel

This section introduces the metamodel that we propose for the RM of MD. The metamodel includes a number of key concepts and relationships that exist between them as described in ISO 14971. The UML profile facilities are used to specify the metamodel. The formal structure of a metamodel is obtained by using associations, stereotypes, enumerations, data types and packages.

As shown in Figure 1, the metamodel called *ISO14971RiskManagement* and developed in the context of this paper comprises three packages of the concepts related to the following aspects: 1) system analysis (the *SystemAnalysis* package), 2) RM (the *RiskAnalysis* package), 3) risk control (the *RiskControl* package). The *SystemAnalysis* package contains architectural elements, which are required for the analysis of the MD architecture according to ISO 14971. The basis for deriving these elements is provided by generic modeling languages like SysML or UML. The *RiskAnalysis* package describes the key concepts implied in the analysis of MD risks specified in ISO 14971. These concepts can be split into two groups. The first group includes the core safety and reliability concepts (e.g. hazard, risk) operated by the majority of generic safety standards. Concepts from this group could be derived from other safety or reliability modeling languages such as RAAML or SafeML. The second group, on the other hand, are the concepts specific to ISO 14971 (e.g. foreseeable event); therefore, they are defined and used only in the context of ISO 14971. The *RiskControl* package enables the modeling of risk control measures in the MD architecture that will help reduce risk criticality to acceptable or tolerable levels. The detailed structure of each package will be explained in this section.

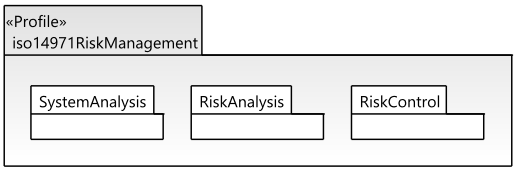


Fig. 1. Package architecture of the ISO 14971 Risk Management metamodel.

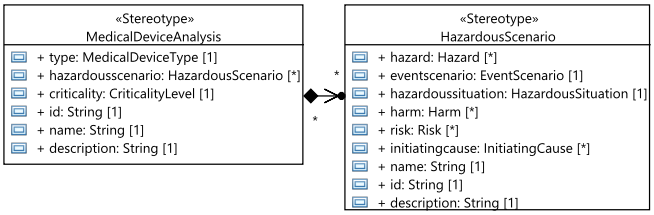


Fig. 2. System Analysis package including the MedicalDeviceAnalysis concept and its relations with other concepts.

A. System Analysis Package

In the MBSE paradigm, various types of analysis (e.g., safety, security, performance) are conducted after modeling the MD architecture at the required level of abstraction (e.g., system, functional, hardware, software). The *SystemAnalysis* package helps extend the description of system architecture components such as *Block* in SysML or *Class* in UML with additional data related to the RM context. The package includes a concept called *MedicalDeviceAnalysis* shown in Figure 2. This concept specifies the type of MD, its assessed criticality level and a list of associated hazardous scenarios. The attribute called *MedicalDeviceType* determines whether a system under analysis is classified as MD or not. The *criticality* attribute sets up a criticality level of the MD component. The type of this attribute (called *CriticalityLevel*) is defined as an enumeration that describes four levels: minor, acceptable, undesirable, and unacceptable. The criticality of an MD component is often estimated to be the highest criticality of all hazardous scenarios related to this component.

B. Risk Analysis Package

Risk analysis is a critical component of the RM process outlined in ISO 14971; it is required for the development, manufacture and post-market surveillance of MD. The *RiskAnalysis* package includes the concepts that allow the modeling and analysis of risks on the MD architecture. The metamodel shown in Figure 3 describes the key concepts of risk analysis process mentioned in ISO 14971: *InitiatingCause*, *Hazard*, *ForeseeableEvent*, *SequenceOfEvents*, *HazardousSituation*, *Harm*, *Risk*. The other two concepts, *EventScenario* and *HazardousScenario*, are introduced to facilitate risk modeling, analysis, and results representation. Furthermore, the metamodel provides knowledge of how the concepts are related to each other (Figure 3) and how they are related to the *SystemAnalysis* package (Figure 2) and the *RiskControl* package (Figure 4).

The concept of a *HazardousSituation* is central to the metamodel. ISO 14971 defines it as a ”circumstance in which people, property or the environment is/are exposed to one or more hazards”. Its attributes, occurrence and severity, help safety experts to estimate the criticality level of the analyzed hazardous situation and then use this value while estimating the criticality of MD components associated with this hazardous situation. The occurrence type is defined as an enumeration called *OccurrenceLevel*; it includes the following levels: improbable, remote, occasional, probable, and frequent. The severity attribute is also specified via enumeration called *SeverityLevel* that suggests five levels: negligible, minor, serious, critical, and catastrophic. The criticality levels of *HazardousSituation* are the same as for *MedicalDeviceAnalysis* and are defined in the *CriticalityLevel* enumeration. *HazardousSituation* has a composition link with three other concepts:

- The *Hazard* that lead to a *HazardousSituation*.
- The *EventScenario* that contains the sequences of foreseeable events, *SequenceOfEvents*, resulting in a *HazardousSituation*.
- The list of *Risks* that appear due to a *HazardousSituation*.

Hazard, in turn, may comprise the list of possible initial causes, *InitialCause*, that led to this hazard and the sequences of foreseeable events, *SequenceOfEvents*, that are initiated by *Hazard* and result in certain hazardous situations.

EventScenario is a supplementary concept not defined in ISO 14971. It is used to model foreseeable events that appear in parallel or to define several sequences of foreseeable events. Therefore, *EventScenario* contains a list of one or several foreseeable events, *ForeseeableEvent*, that lead to a hazardous situation. The occurrence of *EventScenario* is estimated as the highest occurrence level of all sequences of foreseeable events related to it.

Each *ForeseeableEvent* includes the list of possible effects and causes. These attributes are defined via the *Effect* and *Cause* concepts. The occurrence attribute of *ForeseeableEvent* is defined via the *OccurrenceLevel* enumeration.

Several *Risks* may be caused by *HazardousSituation*. Each *Risk* may be characterized by three attributes: *isResidual*, *isAcceptable*, *isBenefitOutweighed*. The *isResidual* attribute defines whether *Risk* is residual, i.e. portion of risk remains after risk control measures have been applied, or not. The *Risk* can be acceptable or not (see the *isAcceptable* attribute) based on the value of the risk *occurrence* attribute. The ISO 14971 standard requires that the risk-benefit analysis for individual residual risks as well as for the overall residual risk be conducted. This analysis helps a manufacturer establish if the benefits of an MD outweigh its risks. Therefore, the *isBenefitOutweighted* attribute shows if benefits balance the risk considered. The severity, occurrence and criticality attributes of *Risk* are defined by the *SeverityLevel*, *OccurrenceLevel* and *CriticalityLevel* enumerations respectively. The criticality level of *Risk* is evaluated through the risk matrix, as explained in ISO 14971. The *Risk* can also contain a list of corresponding harms, *Harm*, caused by the *Risk*.

ISO 14971 defines *Harm* as ”physical injury or damage to the health of people, or damage to property or the environment”. However, the *Harm* concept in ISO 14971 encloses a nature of an ”event” because the standard operates with the

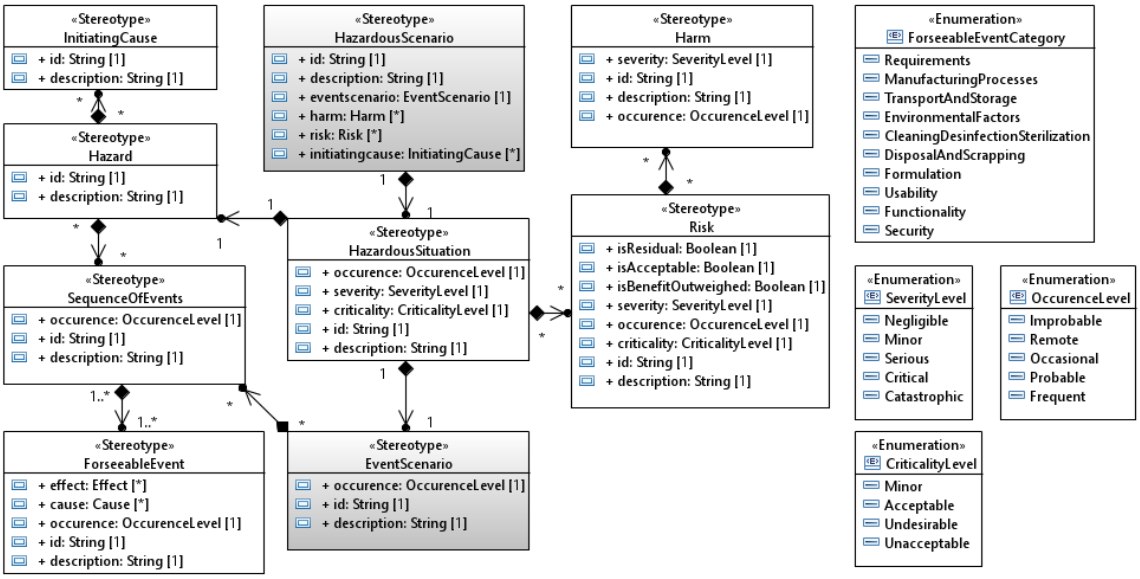


Fig. 3. Risk Analysis package. Concepts highlighted in white are defined in ISO 14971; concepts in grey color are not defined in ISO 14971.

occurrence as one of the properties of *Harm* in addition to the *Harm* severity.

Although the *HazardousScenario* concept is not defined in ISO 14971, it is widely used in other safety standards such as ISO 26262 or IEC 61508. A hazardous scenario is a sequence of conditions that can lead to a hazardous situation. In the proposed metamodel, the *HazardousScenario* concept includes such attributes as *EventScenario*, a list of *Risks*, *Harms* and *InitiatingCauses* related to the considered hazardous situation. On the other side, the *HazardousScenario* concept is used in the *SystemAnalysis* package because several *HazardousScenarios* can be defined for a system component under analysis (*MedicalDeviceAnalysis*) as shown in Figure 2.

C. Risk Control Package

The last part of the overall metamodel covers the risk control measures mechanism specified in ISO 14971. According to the standard's definition, risk control is "the process of implementing risk reduction measures or risk acceptance decisions". The *RiskControl* package aims at supporting safety experts during risk control activities. Figure 4 shows the *RiskControlMeasure* concept and its relation with MD risks. The *RiskControlMeasure* is characterized by the *category* and *status* attributes. The former attribute is typed with the *RiskControlMeasureCategory* enumeration that includes the following elements (as defined in ISO 14971): safe design, protective measures, and information for safety. The latter attribute has also an enumeration type, *RiskControlMeasureStatus*, that contains the following elements: accepted, new, implemented, and rejected. The *RiskControlMeasure* concept is used in the *RiskAnalysis* package because the set of the *RiskControlMeasures* must be defined and applied to the *Risk* under analysis in order to decrease its criticality level.

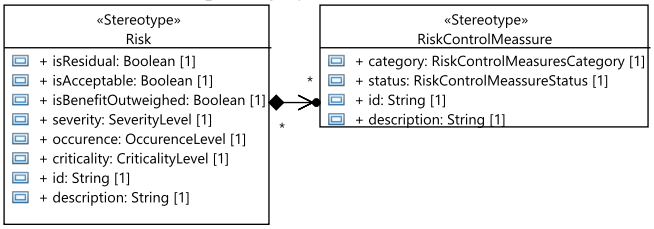
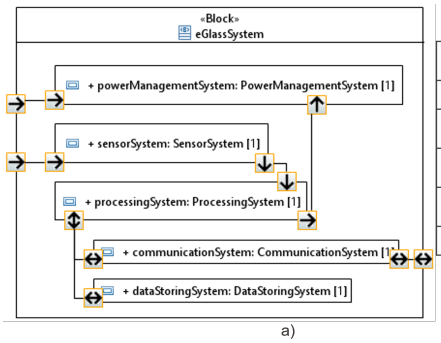


Fig. 4. Risk Control package including the RiskControlMeassure concept and its relations with other concepts.

IV. Validation

The validation of the proposed metamodel is done by analyzing the example of a wearable system for the real-time monitoring of brain activity called *e-Glass* [22]. The device would acquire and process EEG continuously, providing information to the user in real-time via Bluetooth to a user application.



Subsystem	Hardware Component
Processing System	STM32L476
Power Management System	STBC03
Sensor System	ADS1299, MIS2DH
Communication System	BlueNRG-MS
Data Storing System	MX25R6435

b)

Fig. 5. e-Glass top-level system architecture described in IDD.

A. e-Glass System Analysis

The *e-Glass* system is modeled in SysML as it has a good foundation for capturing system requirements, architecture and constraints. Figure 5a presents the *e-Glass* system architecture modeled with the internal block diagram (IBD) showing interconnections between the main blocks of the system. The SysML blocks represent *e-Glass* components while ports

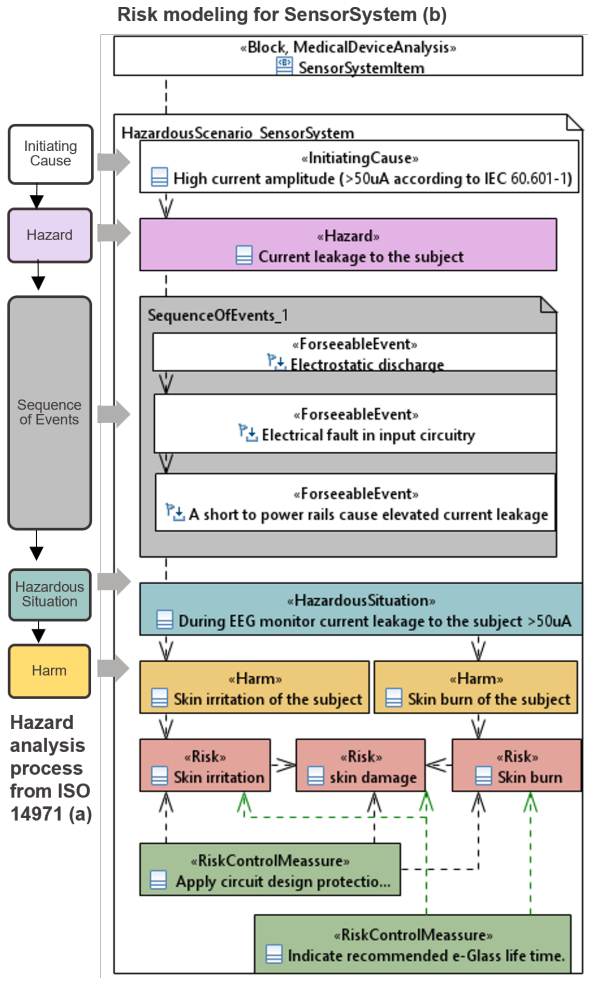


Fig. 6. Validation example. The hazardous scenario is modeled for the Sensor System of e-Glass (b) where each element is mapped to the appropriate step of risk analysis from ISO 14971 (a).

and connectors provide interactions between blocks. During the risk analysis, the block specification is extended with the information on the risks associated with each block by using the *MedicalDeviceAnalysis* concept from the *SystemAnalysis* package. The system architecture model of *e-Glass* comprises the following subsystems: SensorSystem, PowerManagementSystem, ProcessingSystem, DataStoringSystem, CommunicationSystem.

The hardware is embedded in glasses' temples to mimic an everyday wearable device and it is battery-powered. Figure 5b shows an allocation of main subsystems to the appropriate hardware components. The *e-Glass* system is designed using off-the-shelf components to target medical applications: 1) an STM32L476 ARM Cortex-M4 microcontroller; 2) the ADS1299 EEG Front-End, a complete EEG System-on-Chip; 3) a BlueNRG-MS, Bluetooth Low Energy network processor. Finally, it also includes an external Flash memory and an ultra-low power triaxial accelerometer to allow for data logging and user activity monitoring.

B. e-Glass Risk Analysis

The risk modeling of *e-Glass* is illustrated by using the concepts from the *RiskAnalysis* package. Figure 6b shows an example of a *HazardousScenario* specified for the Sensor system of *e-Glass*. The *InitiatingCause* of the "Current leakage to the subject" *Hazard* is "High current amplitude (more than 50uA according to IEC 60.601-1)". This hazard leads to the *HazardousSituation* formulated as "During EEG monitor current leakage to the subject more than 50uA" after appearing the following sequence of the *ForeseeableEvents*: "Electrostatic discharge", "Electrical fault in input circuitry" and then "A short to power rails cause elevated current leakage".

To specify the sequence of foreseeable events, we use SysML state machine diagrams (although SysML sequence or activity diagrams can also be explored) as shown in Figure 7: each *ForeseeableEvent* defined earlier is introduced as a trigger to switch from one state of *e-Glass* to another.

The given *HazardousSituation* leads to two *Harms*: "Skin irritation of the subject" and "Skin burn of the subject". These harms are associated with the corresponding *Risks*: "Skin irritation" and "Skin burn". One residual *Risk*, "Skin damage", caused by these risks is defined.

The validation example shows how to display hazardous scenarios (Figure 6b), along with other results (Figure 7) of the safety and risk analysis, in a graphical form. Furthermore, one can model and visualize hazardous scenarios the way that is described in ISO 14971. Indeed, Figure 6a shows the excerpt from ISO 14971 which explains the recommended hazard analysis flow and the relationship between *Hazard*, sequence of *ForeseeableEvents*, *HazardousSituation*, and *Harm*. This flow is mapped to the *HazardousScenario* modeled in Figure 6b. The graphical presentation of the hazardous scenarios (i) highlights unacceptable hazardous scenarios and associated risks for their further review and analysis, and (ii) provides traceability links between RM artifacts and MD architecture.

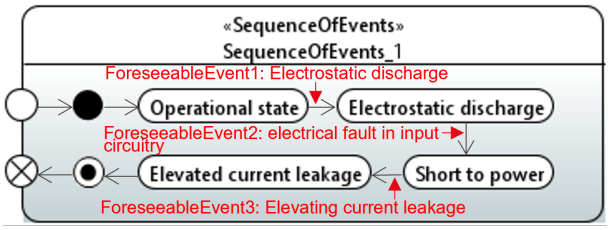


Fig. 7. Modeling sequences of foreseeable events with State Machine Diagrams: each event triggers the change from one state to another.

C. e-Glass Risk Control

The modeling of the control measures related to the risks associated with *e-Glass* is done by using the *RiskControl* package. Figure 6b shows two *RiskControlMeasures* that are recommended to reduce the criticality level of the identified risks: "Apply circuit design protection: ESD diodes, add resistors and capacitors between electrode and front-end " and "Indicate recommended e-Glass lifetime". Once analyzed and approved, risk control measures serve as input for the definition of safety requirements at the system level.

V. Discussion

In this section, we discuss the major benefits, limitations and perspectives of the RM metamodel for ISO 14971 that has been described and validated in previous sections.

A. Integration with Other Modeling Languages

Despite the practical effectiveness of the principle of separation of concerns in addressing system complexity, it also poses heterogeneity and integration problems. In other words, after the definition of different concerns, they have to be reintegrated into the global system, while considering the semantic relationships that may exist between several DSML. In this regard, it was decided to reuse as many concepts from the SysML/UML language and existing safety DSML (e.g. RAAML) as possible and only add concepts that are missing (mainly, they are specific to ISO 14971) to address safety and RM aspects of MD. This approach avoids duplication between a few languages and leads to a relatively small metamodel based on SysML / UML and generic DSML safety that covers ISO 14971-related concepts. Table I shows how the proposed metamodel can be mapped to SysML/UML concepts as well as to RAAML concepts providing a common base for the method- and domain-specific safety modeling. In addition, all kinds of safety-specific relationships defined in RAAML (e.g. Causality, ControllingAction) are compatible with our metamodel.

TABLE I
MAPPING OF THE METAMODEL CONCEPTS TO RAAML, UML, SYSML.

Metamodel Concept	RAAML	SysML/UML
Risk	Risk	Block/Class
Hazard	Hazard	Block/Class
InitiatingCause	Cause	Block/Class
Harm	Effect	Block/Class
HazardousSituation	Situation	Block/Class
SequenceOfEvents	Situation	Block/Class
ForeseeableEvent	AbstractEvent	Event
EventScenario	Scenario	Block/Class
HazardousScenario	Scenario	Block/Class
RiskControlMeassure	Situation	Block/Class
MedicalDeviceAnalysis	Situation	Block/Class

B. Metamodel Application and Benefits

The application of the proposed metamodel brings several advantages for safety analysis and RM in the medical field:

Improved Risk Analysis. The ISO 14971-based metamodel enables safety and quality experts to perform an accurate and comprehensive risk analysis in the healthcare context. The metamodel enables a structured approach for identifying and analyzing potential risks associated with MD and minimizing their impact.

Standardized Risk Management Process. The metamodel supports a standardized RM process that can be applied by different MD manufacturers. It ensures consistency in RM processes, making it easier for safety professionals to compare and evaluate risks across different MD.

Regulatory Compliance. Compliance with regulatory requirements is essential for MD manufacturers. The metamodel provides a base for building a framework compliant with ISO 14971, which helps in ensuring that MD meets regulatory requirements and is safe to use.

Increased Patient Safety. One of the primary benefits of using the proposed metamodel is that it helps in improving patient safety. By identifying and mitigating potential hazards, safety and quality experts can ensure that MD is safe to use and does not pose a risk to patients.

C. Metamodel Limitations

Although the proposed metamodel has been shown to offer several advantages, it has also certain limitations. The harmonization and compliance with different safety standards is a non-trivial task, and thus the proposed metamodel alone cannot comprehensively address all of its potential issues. In this context, the metamodel includes a relatively small set of ISO 14971-associated concepts that are based on SysML/UML and general safety knowledge implemented in safety DSML. Furthermore, some aspects are inherently difficult to fully address due to their nature (for example, the human factor in safety-related decision making).

D. Open Issues

To facilitate the use of our metamodel by different categories of stakeholders, tool support and user interaction should be provided. However, the non-trivial task would be to choose a trade-off between the various automation features enabled by MBSE techniques and the degree of automation while generating safety models. RM automation is possible to a certain extent, it requires a deep understanding of the domain-specific context and requirements and involves complex algorithms to generate accurate safety and reliability models. Therefore, a combination of automated and manual approaches should be used to ensure the completeness and consistency of safety and risk analysis.

E. Future Work

In future work, we plan to address the open issues discussed above and to continue working on the harmonization with generic safety DSML such as RAAML. The technical aspects might include activities on completing the metamodel with concrete syntaxes and semantics to develop a profile able to semi-automate risk analysis, assessment and evaluation in the medical field. The proposed metamodel also needs to be further evaluated and validated using industrial use cases.

VI. CONCLUSION

In this paper, we have described a metamodel designed for modeling the safety-related concerns of medical devices (MD). The metamodel describes the main safety concepts from the medical safety standard ISO 14971 and aims at the facilitation of risk identification and mitigation in the early MD development stages. It can serve as a methodological base for creating Domain-Specific Modeling Languages and tools that support ISO 14971 and are harmonized with the generic functional safety domain. For this reason, we have shown in this work how the safety concepts from the proposed metamodel can be integrated with RAAML, SysML and UML. Furthermore, we have demonstrated that the metamodel is capable of modeling the risks as recommended in ISO 14971 through the example of a wearable system designed for real-time EEG-based subject monitoring.

REFERENCES

[1] Smania, G.S., Mendes, G.H.d.S., Lizarelli, F.L. and Favoretto, C. (2022), "Service innovation in medical device manufacturers: does the digitalization matter?," Journal of Business and Industrial Marketing, Vol. 37 No. 3, pp. 578-593.

[2] Walden, D.D., Roedler, G.J., Forsberg, K., Hamelin, R.D. and Shortell, T.M. (Eds.) (2015), Systems engineering handbook: A guide for system life cycle processes and activities, INCOSE-TP-2003-002-04, 4. edition, Wiley, Hoboken, NJ.

[3] H. Thiagarajan et al., "Model-Based Risk Analysis for an Open-Source PCA Pump Using AADL Error Modeling," en, in Model-Based Safety and Assessment, M. Zeller and K. Hofig, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2020, pp. 34–50.

[4] R. J. Malins et al., "SysML Activity Models for Applying ISO 14971 Medical Device Risk and Safety Management Across the System Lifecycle," en, INCOSE International Symposium, vol. 25, no. 1, pp. 489–507, 2015.

[5] European Commission, Medical Device Regulation (MDR). Regulation (EU) 2017/745 on medical devices. 2017. [Online].

[6] ISO/TC 210, ISO 14971 Medical devices — Application of risk management to medical devices, 2019.

[7] ISO 13485: Medical devices — Quality management systems — Requirements for regulatory purposes, 2016. [Online]. Available: https://www.iso.org/standard/59752.html

[8] IEC 62304: Medical device software — Software life cycle processes. 2006. [Online]. Available: https://www.iso.org/standard/38421.html

[9] H. Thimbleby, "Improving Safety in Medical Devices and Systems," 2013 IEEE International Conference on Healthcare Informatics, Philadelphia, PA, USA, 2013, pp. 1-13.

[10] James Rumbaugh, Ivar Jacobson, and Grady Booch. 2004. Unified Modeling Language Reference Manual, The (2nd Edition). Pearson Higher Education.

[11] Friedenthal, S., Moore, A., Steiner, R.: A Practical Guide to SysML: The Systems Modeling Language. Morgan Kaufmann (2009).

[12] Feiler, P.H., Gluch, D.P., Hudak, J.J.: The Architecture Analysis and Design Language (AADL): An Introduction. Tech. rep., Software Engineering Institute, Carnegie-Mellon University, Pittsburgh (2006).

[13] Model-based Analysis and Engineering of Novel Architectures for Dependable Electric Vehicles [Online]. Available: http://www.maenad.eu/

[14] P. Cuenot, P. Frey, R. Johansson, H. Lonn, Y. Papadopoulos, M.-O. Reiser, et al., "The EAST-ADL architecture description language for automotive embedded software," in Proc. of the 2007 International Dagstuhl conference on Model-based engineering of embedded real-time systems, Dagstuhl Castle, Germany, 2010, pp. 297-307.

[15] OMG UML Profile for MARTE: Modeling and Analysis of Real-time Embedded Systems (2011). URL http://www.omg.org/spec/MARTE/1.1/

[16] Risk Analysis and Assessment Modeling Language, 2022.[Online]. Available: https://www.omg.org/spec/RAAML.

[17] Biggs, G., Sakamoto, T., Kotoku, T. (2016). A profile and tool for modelling safety information with design information in SysML. Software and Systems Modeling, 15(1), 147-178. doi:10.1007/s10270-014-0400-x

[18] ISO/TC 22/SC 32, ISO 26262: Road vehicles - Functional safety, 2011. [Online]. Available: https://www.iso.org/standard/43464.html

[19] Bernardi, S., Merseguer, J., Petriu, D.: A dependability profile within MARTE. Software and Systems Modeling 10, 313–336 (2011). DOI 10.1007/s10270-009-0128-1.

[20] Montecchi, L., Lollini, P., Bondavalli, A.: Dependability concerns in model-driven engineering. In: Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2011 14th IEEE International Symposium on, pp. 254 –263 (2011). DOI 10.1109/ISORCW.2011.32

[21] Y. Uludag et al., "Integration of systems design and risk management through model-based systems development," en, System Engineering, vol. 26, no. 1.

[22] D. Sopic et al., "E-Glass: A Wearable System for Real-Time Detection of Epileptic Seizures," in Proc. - IEEE Int. Symp.on Circuits and Systems, ISSN: 02714310, vol. 2018-May,Institute of Electrical and Electronics Engineers Inc., 2018.