Proceedings of the 2019 Design of Medical Devices Conference
DMD2019
April 15, 16-18, 2019, Minneapolis, MN, USA

DMD2019-3210

MODEL-BASED SYSTEM, SAFETY AND SECURITY CO-ENGINEERING METHOD AND TOOLCHAIN FOR MEDICAL DEVICES DESIGN

Marc Sango[1], Jean Godot[1]
ALL4TEC
Massy, France

Antonio Gonzales[2], Ricardo Ruiz Nolasco[2]
RGB Medical Devices
Madrid, Spain

ABSTRACT

The increasing complexity of the medical regulatory environment and the inherent complexity of medical devices, especially due to the increased use of connected devices and embedded control software, impose adoption of new methods and tools for the system design, safety and security analyses. In this paper, we propose a method and an associated toolchain to couple model-based system engineering and safety/security analyses at the design phase of medical devices. The method is compliant with ANSI/AAMI/ISO TIR57 safety and security guidance, and compatible with INCOSE Biomedical-Healthcare Model-Based Systems Engineering works. The toolchain is based on a system architecture modelling tool and supports medical device domain specific reference architecture, as well as tools for safety and security risk analyses. The proposed method and toolchain are illustrated by considering a RGB's TOF-CUFF monitor device analyzed in the scope of the AQUAS project as a medical device use case.

Keywords: Medical Devices, Architecture Model, Safety and Security Analyses.

INTRODUCTION

The increased use of connected medical devices in healthcare applications has created a new source of risks for their safe operation. While the need to protect patient data from cyber-attack is now well understood, there is no framework for security risk management for medical devices [1]. The Association for the Advancement of Medical Instrumentation (AAMI) has recently published medical devices guidance that mirrors the most detailed approach in development for control systems, to bridge safety and security risk management (Figure 1).

This safety/security guidance follows the structure of the standard ANSI/AAMI/ISO 14971:2007 [2], which is an integral part of the safety risk management process required by many regulatory authorities. Although differences exist between cybersecurity analysis and safety analysis, there are many similarities in system thinking, analysis techniques, and documentation methods required for each [3]. Regarding system thinking applied to safety [4], one critical difference between many "traditional" system-engineering industries (defense and aerospace) and medical device development is that most medical device development is market driven, rather than contract driven [5]. In a contract-based program there is an identified customer, with a set of applications and workflows. In a market-driven program the workflow and use cases are defined by the developer, and the buyer needs to 'own' the integration of the offering into their specific systems and workflows. With this market driven context and the advent of medical device interoperability, the medical device industry is increasingly challenged to characterize medical devices in a system context. Model-Based System Engineering (MBSE) is a promising approach to address these biomedical-healthcare challenges, which is what the International Council on Systems Engineering (INCOSE) Biomedical-Healthcare working group is trying to demonstrate [6].

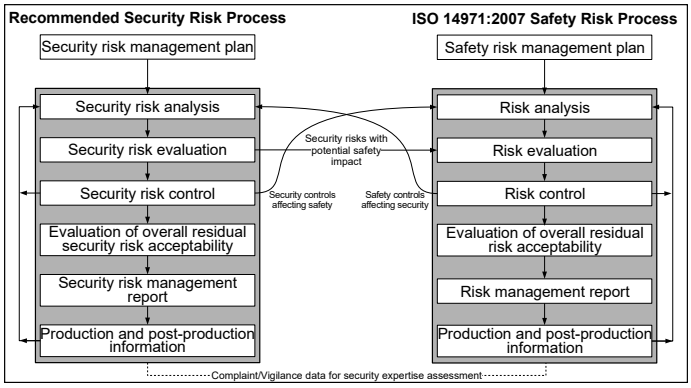

Figure 1: Managing safety and security risk convergence [1]

Our research is focused on medical devices model-based system architecture engineering with specific emphasis on assurance of safety and security concerns. The proposed method is consistent with ANSI/AAMI/ISO TIR57 [1] safety and security guidance and provides elaborated traceability links

[1] Contact author – ALL4TEC: marc.sango@all4tec.net and jean.godot@all4tec.net
[2] Contact author – RGB Medical Devices: agonzales@rgb-medical.com and rruiznolasco@rgb-medical.com

across system architecture, safety and security analysis process. The associated toolchain platform automates some parts of the proposed Model-Based System, Safety and Security co-Engineering (MB3SE) method and improves the traceability of system, safety and security data during the development of medical devices at the early phases of their life-cycle.

The paper is organized as follows. Section 1 introduces the proposed MB3SE for medical devices development. Then, the associated toolchain platform is described in Section 2. Section 3 presents the AQUAS medical device case study and its evaluation. Finally, we discuss the approach, the related works and learned lessons in Section 4 before concluding.

1. MB3SE METHOD

The proposed MB3SE method for medical devices is shown in Figure 2. It integrates two mainstreams: the first one concerns the model-based system architecture design, and the second one concerns the convergence between safety and security risk analyses.

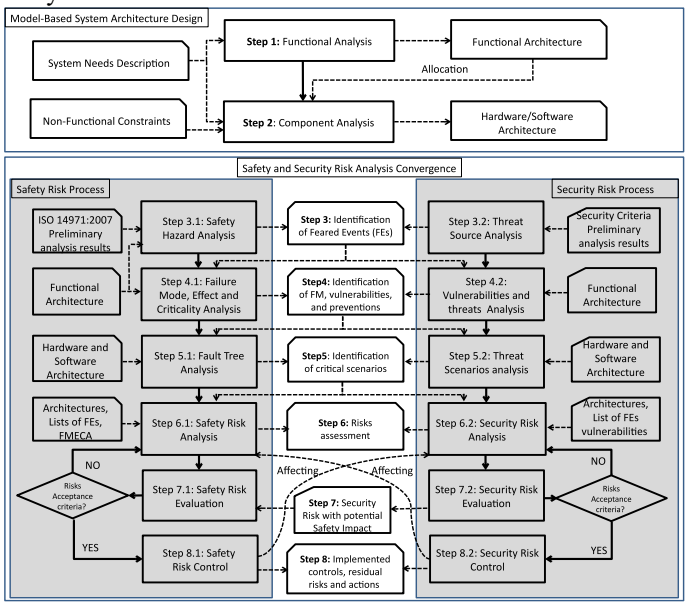

Figure 2: MB3SE method for medical devices

1.1. Model-Based System Architecture Design

This mainstream for a model-based system architecture analysis is based on classical model-based system architecture engineering, such as [7], and offers a support to share concepts with safety and security risk analyses convergence mainstream. It is composed of two steps:

STEP 1 – Functional Analysis: there are many ways to build functional analysis depending on the inherent context of each project and the organization. Anyway, during this design phase step, the commonly encountered functional analysis constitutes the major support for the understanding and the expression of the need. It also allows the definition of functional breakdown, functional data flow and functional scenarios describing chains or paths of expected behaviours. In this step, each function can be further decomposed into functional units, which can be allocated in system components.

STEP 2 – Component Analysis: this step describes the structure of the system based on the previous functional analysis and the associated non-functional constraints coming for example from safety and security risk analyses. The system structure is based on the component-based principle. The term "component" is understood here in the general sense, as a constituent of the system. It can be implemented as one or several subsystems, electronic cards, hardware/software components. In this step, the system architects collaborate with the different teams working on the development of the medical device to build hardware/software architectures of the whole system.

1.2. Safety and Security Analyses Convergence

This mainstream for a convergence between safety and security analyses is based on [1] recommendation to manage safety and security risk convergence and offers a support to identify shared and mapped concepts between safety risk process steps (Steps x.1 with x ϵ [3-8]) and security risk process steps (Steps x.2 with x ϵ [3-8]). The convergence is composed with the following steps:

STEP 3 – Identification of FEs: this step contributes to risk identification in order to improve the design of medical device architecture at early phases of the development. The identification of Feared Events (FEs) is conducted in three sub-steps. A preliminary hazard analysis is commonly conducted to identify safety-related FE or hazards. According to ISO 14971 standard, a hazard is a potential source of harm, which is physical injury or damage to the health of people, or damage to property or the environment. In our analysis, the potential hazards are proposed according to the literature, previous medical device projects and experience feedbacks. For example, in order to make the list of FEs related to the use of medical devices, families or categories of FE (mechanical hazards, biological hazards, etc.) are considered. A generic safety-related devices or systems are generally concerned with non-malicious events and how these can be avoided or mitigated.

Conversely, security addresses malicious events or attacks to a system by identifying the threat sources, their capabilities and the vulnerabilities that may be exploited. For the security, the threat sources are generally identified with the support of existing knowledge databases such as provided by EBIOS methodology [8]. The security-related FEs are generally identified and estimated in terms of security criteria (availability, integrity, authentication and confidentiality).

The latter sub-step prioritizes safety and/or security-related FEs and determines which FEs have most impact on patient safety and medical device user. Both safety and security deal with integrity and availability.

STEP 4 – Identification of FMs, vulnerabilities and preventions: at this step a Failure Modes, Effects and Criticality Analysis (FMECA) technique is used. For each safety-related FE identified in the previous step, the potential failure modes (FMs) of each component and function of architecture model are identified. For security, the components vulnerabilities, which can be exploited by the threats to cause the loss of each security criterion, are also identified. As in the previous step,

methodology and databases can support this operation. For instance, a safety/security co-analysis method, such as Failure Modes, Vulnerabilities and Effects Analysis (FMVEA) [9], can be used to show how the exploitability of identified vulnerabilities can lead to safety-related FE.

STEP 5 – Identification of critical scenarios: according to previous steps, safety-related or security-related scenarios are defined. This stage is supported by qualitative fault tree analysis and threat scenarios analysis, which describe the way failures and malicious events can be propagated inside the system architecture. This step is supported by the classical Fault Tree (FT) technique extended with malicious events [10]. As presented in [11], this extended fault trees can be back propagated to the architecture diagram to highlight critical scenarios in the architecture.

STEP 6 – Risk Assessment: ISO 14971 [2] defines a risk as a combination of the probability of occurrence of harm and the severity of that harm. For the estimation of the risks we use the conventional qualitative evaluation technique by using the risk level (R) as a relation of probability (P) and severity (S), shown in Equation (1).

$$R_{safety} = P \times S \quad \textbf{(1)}$$

- P = Probability of occurrence of failures that can lead to a safety-related FE and so to a harm
- S = Severity of a safety-related FE i.e., possible consequences that this FE could have

Table 1 shows the severity and probability scales used for the risk evaluation of the case study.

Table 1: Severity and Probability Scale

Severity	Negligible	Limited	Important	Critical
Probability	Minimal	Significant	Strong	Maximal
Rank	1	2	3	4

To evaluate the cybersecurity risks, the Food and Drug Administration Management of Cybersecurity in Medical Devices Guidance [12] recommends that manufacturers define and document their process for objectively assessing the cybersecurity risks for their device(s). But it is recommended that such a process focus on assessing the risk of patient harm by considering Equation (2).

$$R_{security} = E \times S \quad \textbf{(2)}$$

- E = the exploitability of the cybersecurity vulnerability
- S= the severity of a security-related FE to patient harm if the vulnerability is exploited

Estimating the probability of a cybersecurity exploit is very difficult due to the complexity of exploitation. In the absence of data on the probability of the occurrence of harm, conventional risk management approaches suggest using a "reasonable worst-case estimate" scale as in Table 1.

The equations (1) and (2) show that both safety and security are articulated around the notion of risk. As presented in Figure 2, the safety or security risk assessment can be done through numerous iterations as long as the safety or security risk acceptance criteria is not achieved. For example, according to the severity and the probability it could be decided that the risks with very low severity and probability have to be accepted and the most significant should be avoided and the others reduced or transferred to third party. This step also considers existing compensating controls in order to reduce or mitigate risk.

STEP 7 – Security Risk with potential safety impact: a key purpose of this step is to evaluate whether the safety risks identified in previous step are controlled or uncontrolled under the exploitation of cybersecurity vulnerabilities. To estimate these existing risks for the patient and/or the user of the medical device, we use the same qualitative evaluation technique as in equation (1), where the probability of occurrence of a safety-related FE takes in consideration the exploitability of cybersecurity vulnerabilities.

STEP 8 – Implemented controls, residual risks and actions plan: the goal of this step is to determine the appropriated controls or mitigations to reach the risk acceptance criteria, then to verify that the residual risks are acceptable after the implementation of controls or mitigations actions. Required controls are implemented to be safety and security compliant. Then, it is necessary to study if the implementation of security controls does not affect the safety and conversely. This conducts to repeat steps 6, 7 and 8 until safety and security concerns are satisfied.

2. TOOLCHAIN PLATFORM

The proposed MB3SE method is partially implemented into the Eclipse based platform. The toolchain platform includes several independent tools as shown in Figure 3.

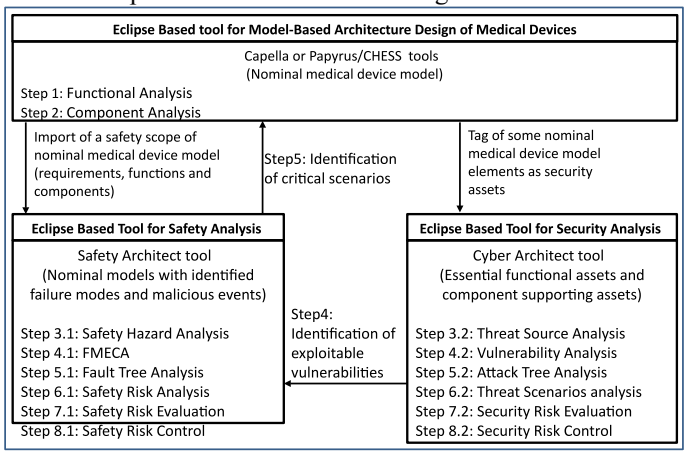

Figure 3: MB3SE toolchain platform

Capella [13] and Papyrus/Chess [14] tools are part of the toolchain for the model-based architecture design, and Safety Architect [15] and Cyber Architect [16] are part for the safety and security analyses. These tools support some steps of the MB3SE methods, as depicted in Figure 3. The bridges have also been developed between these tools to get a seamless toolchain platform. During the exchanges of data between tools, the bridges provide traceability links across system architecture, safety and security analyses processes to facilitate a collaborative work between system, safety and security engineers.

3. TOF-CUFF CASE STUDY

We validate the proposed MB3SE method and the associated toolchain platform described in the previous sections by analyzing the case study of RGB medical device in the scope of the AQUAS project. RGB has developed and CE marked a Blood Pressure (BP) and NeuroMuscular Transmission (NMT) monitoring device, named TOF-Cuff Monitor [17]. A NMT device supports the anesthesiologist in controlling muscle relaxation during hospital operating room interventions. Muscle relaxation, depth of anesthesia, and pain are the three key parameters to be controlled by the anesthesiologist. The RGB company is now confronted with the challenge to develop a closed-loop controller for BP and NMT that will infuse drugs in automatic mode under the supervision of the anesthesiologist.

STEP 1 – Functional Analysis: the objective of the medical use case in the AQUAS project is to incorporate a new functionality to the TOF-Cuff NMT Monitor for the automatic closed-loop control of both monitored vital parameters BP and NMT to maintain them within the target range defined by the user. The main operating functions and functional exchanges are shown in Figure 4. In this Capella diagram, two functional chains are highlighted: the "Electrical Discharge Functional Chain" (blue color in the diagram) and the "Vasoactive Drug Transmission Functional Chain" (red color in the diagram).

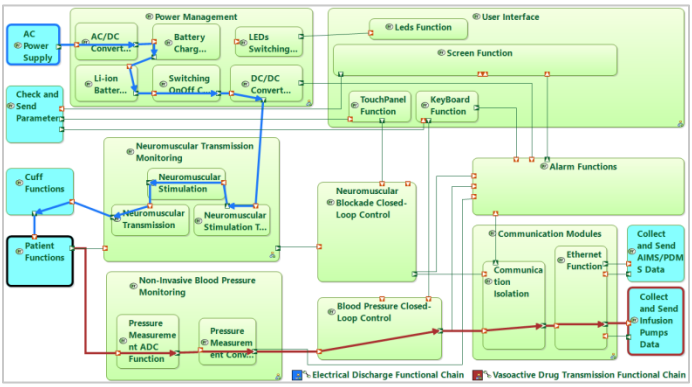

Figure 4: TOF-Cuff functional architecture

STEP 2 – Component Analysis: the previous functional analysis constitutes the major support for the understanding and the expression of the use case needs. Based on the functional analysis and non-functional associated constraints, RGB has designed the block diagram of two electronic boards. Figure 5 presents the high-level of hardware architecture model with two physical paths, which implements the two functional chains mentioned in previous step.

The behaviors of these physical components are responsible for implementing the identified functions. The management of the deployment of behaviour components on physical components and the allocation of functions on behaviour components is not presented in this paper. Figure 6 shows an example of allocation matrix automatically generated by the Capella tool.

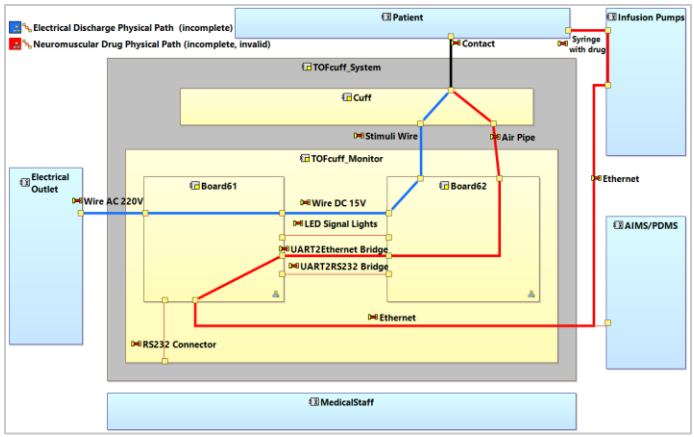

Figure 5: TOF-Cuff hardware architecture

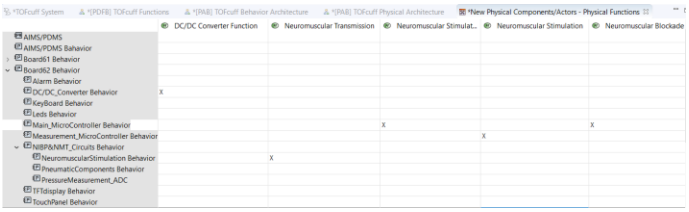

Figure 6: Functions to components allocation matrix

STEP 3 – Identification of FEs: several safety-related and security-related FEs have been identified. In the scope of this paper, only one FE, the "loss of the integrity of the vasoactive drug dose rate", is considered. The main safety-related risk is to infuse a too high dose rate of drug which could seriously harm the patient.

Assumption: At the initial step of the risk management, we assumed, only in the context of this paper, that a risk value in [0,3] is acceptable (green cells), in [4,6] is tolerable (yellow cells), in [8,12] is high (orange cells) and equal to 16 is unacceptable (red cell), as illustrated in Figure 7.

Risks evaluation table

Evolution between raw risk evaluation (displayed in italic) and net risk evaluation (displayed in bold)

Likelihood \ Severity	1. Negligible	2. Limited	3. Important	4. Critical
1. Minimal				
2. Significant				
3. Strong				*Risk related to the alteration of vasoactive drug dose rate*
4. Maximal				

Figure 7: Risk acceptance scale

Risk acceptance criteria: At the final step of the risk management, we assumed, only in the context of this paper, that the risks in the green cells of the table of Figure 7 are acceptable risks.

STEP 4 – Identification of FMs, vulnerabilities and preventions: the identification of the FMs, vulnerabilities, threat sources and existing controls or barriers in Safety Architect tool consists in analysing locally each functions or components. The goal is to determine the effects of these safety and security artefacts. Figure 8 shows an example of a local analysis, where the potential errors in the input ports or the exploitability of a vulnerability by a threat source, and potential loss of safety or security barriers can lead to the erroneous of the output port.

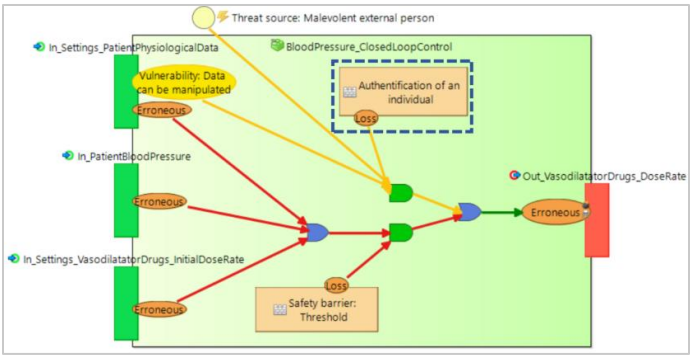

Figure 8: Example of local analysis (the artefact in the blue square appears during Step 7)

STEP 5 – Identification of critical scenarios: from the previous local analysis, the Safety Architect tool generates for each selected FE the Fault Tree (FT) extended with security analysis artefacts (e.g., vulnerabilities and threat source). Figure 9 depicts the obtained FT for the FE "Loss of integrity of the vasoactive drug dose rate". It represents the critical scenario, which can lead to the FE occurrence.

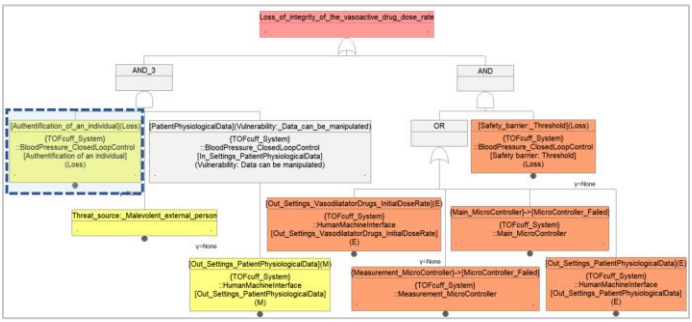

Figure 9: Fault tree related to the FE identified in Step 1 (the artefact in the blue square appears during Step 7)

STEP 6 – Risk Assessment: at this step, the risk related to the FE is assessed according to the scenarios identified in previous step. As shown in Figure 10, the existing "Safety barrier: Threshold" reduces the severity and the likelihood, but it is still not enough to reach the acceptance criteria. Further improvement is required.

Risks evaluation table

Evolution between raw risk evaluation (displayed in italic) and net risk evaluation (displayed in bold)

Likelihood \ Severity	1. Negligible	2. Limited	3. Important	4. Critical
1. Minimal				
2. Significant			Risk related to the alteration of vasoactive drug dose rate	
3. Strong				~~Risk related to the alteration of vasoactive drug dose rate~~
4. Maximal				

Figure 10: Risk assessment with an existing safety barrier

STEP 7 – Security Risk with potential safety impacts: in the step 5, Figure 9 shows that, if the identified vulnerability "data can be manipulated" is exploited, the resulting threat can lead to the FE. In addition, the risk assessment of the previous step 6 shows that the risk, after applying of safety risk control, remains high according to the risk acceptance criteria. These analyses show that security risk can have a potential impact to safety. To reduce the risk level, the security control or the security barrier, "authentication of an individual" is added in previous analysis of Figure 8 accentuated by the blue square. Then the FT is updated as shown in Figure 9 with a new leaf highlighted by the blue square. The risk analysis is also updated. The resulting risk evaluation in Figure 11 shows that the risk is reduced and the risk reaches the acceptance criteria.

Risks evaluation table

Evolution between raw risk evaluation (displayed in italic) and net risk evaluation (displayed in bold)

Likelihood \ Severity	1. Negligible	2. Limited	3. Important	4. Critical
1. Minimal			Risk related to the alteration of vasoactive drug dose rate	
2. Significant			~~Risk related to the alteration of vasoactive drug dose rate~~	
3. Strong				
4. Maximal				

Figure 11: Risk assessment with safety and security barriers

STEP 8 – Implemented controls, residual risks and actions: consistently with the case study analysis context and the FE considered in the Step 1, we identify at this last step one safety barrier already implemented and one security barrier not yet implemented, as presented in Figure 12. Although, it remains some residual risks, the evaluation of the joint safety and security barriers shows that the acceptance criteria assumed in step 1 is achieved. As the security barrier is not yet implemented it is recommended to iterate the process to estimate the residual risks that will remain when all the joint barriers will be implemented.

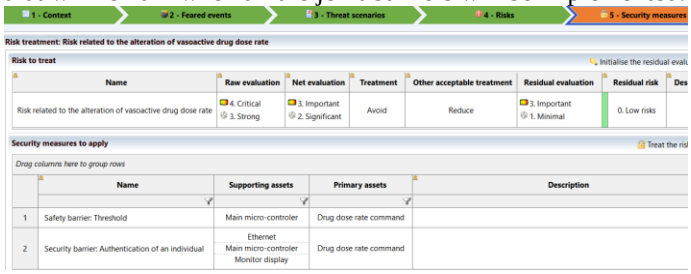

Figure 12: Risk treatment process

4. DISCUSSIONS AND LEARNED LESSONS

The medical devices are strongly regulated. For example, in the European Union, the current medical devices regulation MDR 93/42/EEC is still applicable and a new MDR 2017/745 was approved on 2017 and will be fully applicable on 2020. These regulations specify the requirements that a medical device must comply, but the best way to do it is through the compliance with the harmonized standards.

There are a lot of harmonised standards related to safety. Regarding risk management, it is mandatory to be compliant with EN ISO 14971:2012 [18] to perform a risk assessment since the initial design of a medical device and during all its life. However, there are not harmonised standards related with cybersecurity, but there are some standards that should be considered, such as [19] and [20]. These cybersecurity standards are more related to health information or patient data security management. There are no harmonized standards or framework for security risk management for medical devices. While there exist, some research works for safety and security co-engineering approach [21], there are no guidance to bridge safety and security risk management in industrial domains, particularly in medical domains. Our work is related to the recently published principles for medical device security and risk management [1].

Regarding development life cycle, the EN 62304:2006 [22] standard requires following the well-known V-model for the software life cycle processes of a medical device. The new MDR 2017/745 does not require a specific device life cycle, but its requirements are more addressed to the processes, especially when referred to the design phase. The mission of INCOSE biomedical-healthcare working group is to demonstrate the value of modern system engineering method, such as MBSE [6]. Our work is related to this and we try to demonstrate the value of the MB3SE to support the design of medical device architectures. In addition, some recent documents, such as [23], recognizes the importance of incorporating security and safety engineering throughout a system's life-cycle.

From the related works and from the evaluation of the MB3SE method proposed in this paper, we learned the following lessons of the co-engineering between system engineers, safety engineers and security engineers.

- It is helpful to list the supporting assets within the study's boundaries. The current TOF-Cuff architecture considered in this paper includes an Ethernet output, but an optional Wi-Fi output should be available for the new device. In this case some guidance for securing wireless medical devices, such as [24], should be considered.
- The clear diagrams with stakeholder viewpoints are very helpful for the understanding of all stakeholders.
- Although the toolchain facilitates the collaborative works between stakeholders by providing some traceability links across system architecture, safety and security analysis process, the subjective risk management activities should remain in the responsibility of risk management experts.
- Although the qualitative risk levels may be quite subjective, a systematic approach can ensure that the system, safety and security stakeholders are able to understand them. It is usually helpful for the stakeholders the use of graphs to visualise the positioning of risks relative to one another.

CONCLUSION

This paper describes a Model-Based System, Safety and Security co-Engineering (MB3SE) method and an associated toolchain for the design of medical devices. The MB3SE method is based on the TIR57 safety and security guidance, and the INCOSE Biomedical-Healthcare Model-Based Systems Engineering works. The toolchain is based on a system architecture modelling tool, a safety risk analysis tool and a cybersecurity risk analysis tool. The proposed method and toolchain are illustrated by considering a RGB's TOF-CUFF monitor device used in the scope of the AQUAS project as a medical device use case. RGB Company aims to include within their product development life cycle safety and security considerations. The method and tool-chain presented in this paper are going to be enhanced with additional testing, simulation or verification techniques and tools. For example, our future work is to include the model-based testing in our MB3SE method to provide a systematic approach to test the mitigations or controls identified or added during the safety and security analyses phase.

ACKNOWLEDGMENTS

This work is supported by the AQUAS project. This project has received funding from the Electronic Component Systems for European Leadership JU under grant agreement No 737475.

REFERENCES

[1] ANSI/AAMI/ISO TIR57: Principles for medical device security – Risk management. Approved 5 June 2016 by Association for the Advancement of Medical Instrumentation, Arlington.
[2] ANSI/AAMI/ISO 14971:2007 Medical devices – Application of risk management to medical devices. Association for the Advancement of Medical Instrumentation, 2007.
[3] F. Wu and S. Eagles, Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality. Biomedical Instrumentation and Technology, 50(1): 23–34, 2016.
[4] Nancy G. Leveson, Engineering a safer world – Systems Thinking Applied to Safety. The MIT Press, Cambridge, 2011.
[5] Guide to the Systems Engineering Body of Knowledge (SEBoK) – Part 4 Applications of Systems Engineering – Healthcare Systems Engineering.
[6] Biomedical-Healthcare MBSE Challenge Team: Modelling for a Healthy Future.
[7] Jean-Luc Voirin, Model-based System and Architecture Engineering with the Arcadia Method. 1st Edition ISTE Press – Elsevier, Published Date: 22nd November 2017.
[8] Expression of Needs and Identification of Security Objectives-EBIOS Security knowledge Based – 25 January 2010.
[9] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, Security application of failure mode and effect analysis (FMEA), SafeComp, 2014.
[10] I. Nai Fovino, M. Masera, and A. DeCian. Integrating cyber-attacks within fault trees. Reliab Eng Syst Saf, 94(9):1394–402.
[11] M. Sango and R. de Ferluc. An Integrated Model-Based Tool-Chain for Safety Assessment in Early Validation of System Architectures. IMBSA, 2017.
[12] FDA, "Postmarket Management of Cybersecurity in Medical Devices," 27 December 2016.
[13] Capella, http://www.polarsys.org/capella/ [Accessed 2 Oct. 2018]
[14] Papyrus/CHESS, https://www.polarsys.org/chess/
[15] Safety Architect, https://www.all4tec.com/safety-architect
[16] Cyber Architect, http://www.all4tec.com/cyber-architect
[17] TOF-Cuff NMT monitor, http://www.rgb-medical.com/en/special-product/tof-cuff-nmt-monitor [Accessed 2 Oct. 2018]
[18] EN ISO 14971:2012. "Medical device – Application of risk management to medical devices ". Corrected version of [2].
[19] ISO 27799:2016. "Health informatics – Information security management in health using ISO/IEC 27002".
[20] ISO/IEEE 11073. "Health informatics – Medical health device communication"
[21] S. Kriaa et.al, "A survey of approaches combining safety and security for industrial control systems," Rel. Eng. & Sys. Safety, vol. 139, pp. 156–178, 2015.
[22] EN 62304:2006. Medical device software – Software life-cycle processes
[23] R. Ross, M. McEvilley, and J. Carrier Oren, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160 v1, March 2018
[24] G. O'Brien, S. Edwards, K. Littlefield, N. McNab, S. Wang, and K. Zheng, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, NIST Special Publication 1800-8, August 2018