DEMONSTRATION

Semi-Automated Threat Vulnerability & Risk Assessment (TVRA) for Medical Devices

NABIL MOUKAFIH, University of Warwick, Coventry, West Midlands, U.K.

HONGSEN ZHANG, University of Warwick, Coventry, West Midlands, U.K.

GREGORY EPIPHANIOU, University of Warwick, Coventry, West Midlands, U.K.

CARSTEN MAPLE, University of Warwick, Coventry, West Midlands, U.K.

STEVE TAYLOR, University of Southampton, Southampton, Hampshire, U.K.

LAURA CARMICHAEL, University of Southampton, Southampton, Hampshire, U.K.

Open Access Support provided by:

University of Warwick

University of Southampton

Published: 26 June 2024

PETRA '24: The PErvasive Technologies Related to Assistive Environments Conference
June 26 - 28, 2024
Crete, Greece

https://doi.org/10.1145/3652037.3663896
ISBN: 9798400717604

Semi-Automated Threat, Vulnerability & Risk Assessment (TVRA) for Medical Devices

Nabil Moukafih*
Nabil.Moukafih@warwick.ac.uk
University of Warwick - WMG
Coventry, UK

Hongsen Zhang
Hongsen.Zhang@warwick.ac.uk
University of Warwick - WMG
Coventry, UK

Gregory Epiphaniou
gregory.epiphaniou@warwick.ac.uk
University of Warwick - WMG
Coventry, UK

Carsten Maple
cm@warwick.ac.uk
University of Warwick - WMG
Coventry, UK

Steve Taylor
S.J.Taylor@soton.ac.uk
University of Southampton
Southampton, UK

Laura Carmichael
L.E.Carmichael@soton.ac.uk
University of Southampton
Southampton, UK

ABSTRACT

This paper presents a novel Threat, Vulnerability, and Risk Assessment (TVRA) methodology specifically designed for the Internet of Medical Things (IoMT) to address the unique cybersecurity challenges in the healthcare sector. Given the critical nature of healthcare services and the sensitivity of patient data, there is an urgent need for a robust, IoMT-specific TVRA approach. This work integrates the proposed TVRA methodology with SPYDERISK, an advanced risk management tool, showcasing its application through a Remote Patient Monitoring Systems scenario. The combination aims to enhance the security and reliability of healthcare services, ensuring the protection of sensitive health information and maintaining the trust of patients and providers.

KEYWORDS

Threat and Vulnerability Assessment, Risk Assessment, Risk Assessment, Information Security, IoMT

ACM Reference Format:
Nabil Moukafih, Hongsen Zhang, Gregory Epiphaniou, Carsten Maple, Steve Taylor, and Laura Carmichael. 2024. Semi-Automated Threat, Vulnerability & Risk Assessment (TVRA) for Medical Devices. In *The PErvasive Technologies Related to Assistive Environments (PETRA) conference (PETRA '24), June 26–28, 2024, Crete, Greece.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3652037.3663896

1 INTRODUCTION

The importance of cybersecurity in safeguarding the confidentiality, integrity, and availability of information across diverse sectors cannot be overstated in the digital the era [7]. The assessment of risks, threats, and vulnerabilities in the cybersecurity domain plays a pivotal role in protecting our daily lives, where digital interactions and transactions are ubiquitous. Therefore, it is necessary to conduct a continuous risk assessment and the implementation of effective security measures to mitigate potential threats in various areas [10], and the healthcare sector is one that requires special attention. IoMT has significantly improved patient care but also introduced a myriad of cybersecurity threats, risks, and vulnerabilities [8]. These cybersecurity issues could lead to unauthorised access to patient data, compromise of device functionality, even harm to patient safety. The complexity of the healthcare environment, combined with the critical nature of the data and services directly related to patients' lives, highlight the urgent need for comprehensive TVRA specifically targeted at its needs [12]. The TVRA methods currently offered in the market are often generic rather than a robust TVRA methodology tailored to the IoMT which is essential to identify, evaluate, assess, and mitigate potential security threats effectively [5]. To address this gap, this paper demonstrates a novel TVRA methodology for IoMT environment and integrates it with a cutting-edge risk management tool, Spyderisk [9], to become a new risk management solution for IoMT. We use Remote Patient Monitoring Systems as an example scenario. Implementing the proposed solution helps safeguard sensitive health information and the continuity and reliability of healthcare services, thereby reinforcing the trust and confidence of patients and healthcare providers alike.

The remainder of the paper is shown as follows: Section 2 introduces the related work for risk management methodologies, and threat methodologies in the market. Section 3 describes the TVRA process and the example model of Remote Patient Monitoring Systems. Next, Section 4 demonstrates the implementation process of the key steps of the proposed TVRA method and automating them with a dedicated tool called SPYDERISK. Finally, the discussion part on this solution for cybersecurity and the healthcare industry is shown in Section 5, followed by conclusions in Section 6.

2 RELATED WORK

A TVRA is a systematic approach used in cybersecurity and risk management to identify, evaluate, and prioritize threats, vulnerabilities, and associated risks within an organization or system. Analysing how these threats could exploit vulnerabilities, and evaluating the potential risks and their impacts on the organization's assets information, and operations. Exemplars of risk assessment and threat modelling methodologies include STRIDE for identifying security threats in software applications [4], and PASTA, a seven-step, risk-centric framework [13]. These methodologies could be categorised into System, Organisational, Software/Code and Component level according to the level they focus on (as shown in Table 1). These methodologies provide systematic schemes to identify

PETRA '24, June 26–28, 2024, Crete, Greece

ACM ISBN 979-8-4007-1760-4/24/06
https://doi.org/10.1145/3652037.3663896

security threats, vulnerabilities and risks, analysis to design mitigation strategy and guide the prioritization of mitigation efforts. However, despite the availability of the sophisticated tools and methodologies mentioned above in the general field, a significant gap remains in the healthcare sector, particularly in the IoMT. The unique challenges posed by IoMT devices, including their heterogeneity, the critical nature of their operation, and their integration into healthcare IT ecosystems, underscore the need for a specialised TVRA methodology [8].

Table 1: Categorisation of current TVRA methodologies

Category	Methodology
System	CORAS, ATA, CRAMM, EBIOS 2000, FAIR, MAGERIT, MIGRA, Structured Risk Analysis, TARA, NIST SP800-30, HLRA, PASTA, LINDDUN, TRIKE, CTM, FTA, SDSTA, VAST, STPA
Organisational Level	CORAS, CRAMM, EBIOS 2000, FAIR, FRAP, ISAMM, MAGERIT, Marion, MEHARI 1998, MIGRA, OCTAVE, Structured Risk Analysis, SABSA, SRMP-ESORA, MAE, TOGAF, FEAv2, HLRA, OODA Loop, MeDRa, MedDevRisk
Software/Code Level	STRIDE, ATT&CK, CVSS, SDL, MTM, hTMM, VAST
Component Level	ATA, Dutch A&K Analysis, ATT&CK, FTA, hTMM

Cyber security risk management is commonplace in enterprises, and certification using standardised information security assurance processes is increasingly becoming demanded. ISO 27001 [1] provides a certification standard for checking whether identified threats are addressed by determining security risks and specifying measures that (if correctly implemented) will address those risks. Whilst these standards form a sound basis for risk analysis, the process of analysing risks is often manual and is therefore time-consuming, expensive and error prone. Moreover, the results of a manual analysis are often not reproducible, due to the human value judgements needed on the relevance of given threats. In addition, their results take the form of a document set which is difficult to consult and use when a system actually comes under attack. The need for automation of cyber security risk management has spawned research in risk modelling, analysis tools, and related methods. Automated tools such as SeaMonster and SecuriCad (https://www.foreseeti.com/) consider risk management from the perspective of attacks and other tools such as ThreatModeler (https://threatmodeler.com/) adopt a software-centric perspective. The risk assessment schemes discussed above represent different perspectives on cybersecurity risk assessment, but they do not account for the cybersecurity risks balanced against clinical benefit to the patient.

Current cybersecurity risk assessment tools fail to adequately address the intersection of cybersecurity threats, risks, and treatments with clinical benefit risks. Critically, the literature reveals a stark absence of a tailored TVRA methodology for the IoMT landscape, highlighting a significant gap in effective healthcare risk management. To fill this research gap, this paper proposes the integration of a proposed TVRA methodology and the risk automation tool SPYDERISK [3] to provide best cybersecurity practices within the healthcare industry, addressing the unique challenges of securing IoMT environments in the modern era.

3 METHODOLOGY

This section provides a description of the proposed TVRA along with an overview of the Remote Patient Monitoring System.

3.1 Description of the TVRA

This section describes the process-based approach for ensuring security and safety of medical devices. It is based on the ISO/IEC 27005 information security risk management process described in (BSI Standards Publication, 2022) that includes the following core activities that are briefly described below:

- **Context Establishment**: Defining the scope and boundaries of the information security risk management process.
- **Risk Assessment**: Identifying, analysing, and evaluating risks. This involves the identification of potential threats and vulnerabilities that could affect the IoMT environments' assets and determining the likelihood and impact of these risks.
- **Risk Treatment**: Determining appropriate ways to handle identified risks, whether by avoiding, transferring, mitigating, or accepting them, and selecting specific control measures to treat the risks.
- **Monitoring and Review**: Continuously monitoring the risk environment and the effectiveness of implemented control measures and reviewing the process to make improvements.
- **Recording and Reporting**: Engaging stakeholders in the risk management process, ensuring that risk information is shared, and consulting with stakeholders in making risk management decisions.

The TVRA approach, while based on the principles of ISO/IEC 27005, is particularly tailored to the complexities of IoMT. It diverges from ISO/IEC 27005 by providing a granular focus on IoMT device classification, asset profiling, and use case-specific security requirements. This level of specificity addresses the unique vulnerabilities and threat landscape of medical devices, which are often subject to stringent regulatory controls and have a direct impact on patient safety. It also facilitates compliance with regulatory requirements and enables a clear articulation of risk to stakeholders. By focusing on IoMT-specific risks, the TVRA approach ensures that risk management processes are not only compliant with international standards but also relevant and effective in addressing the unique challenges of securing medical devices.

Finally, the TVRA approach relies on its extensive "knowledge base" that describes a list of threats and vulnerabilities that are specific to the healthcare sector. These catalogues are pivotal, as they detail potential security issues that can jeopardize patient safety and data integrity. They include a variety of threat vectors such as cyber-attacks from sophisticated hackers, exploitation of software and hardware vulnerabilities, and insider threats. These

input information as described in the figure below, will help healthcare organizations can implement targeted controls and mitigate risk around medical devices around their network. A high-level overview of the TVRA is depicted in Figure 1 and 2 below. The TVRA was divided into two sub-figures for readability purposes.

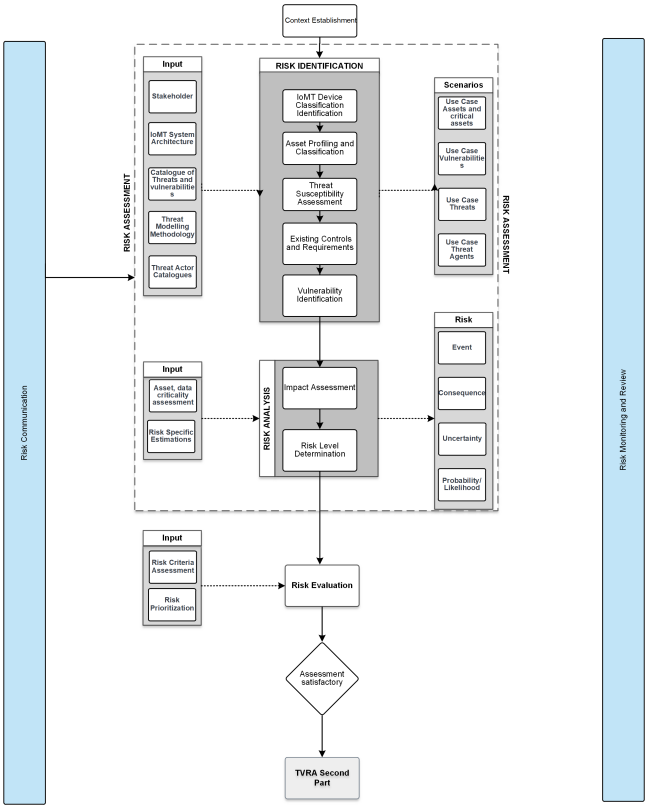

Figure 1: Overview of the first part of the TVRA.

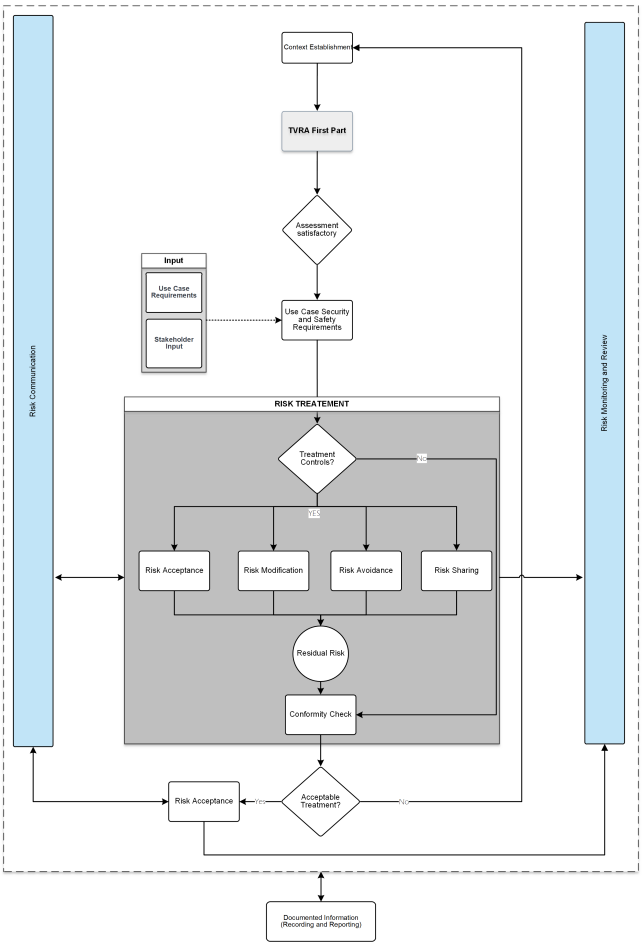

Figure 2: Overview of the second part of the TVRA.

3.2 3.2 Remote Patient Monitoring System (RPMS)

This section will introduce the RPM system [6] which will be used as a use case analysis in an IoMT environment. An RPM system is a technology-based healthcare approach designed to monitor and capture medical and other health data from patients via the patient monitoring devices and other sensors from the IoT in one location and electronically transmit that information securely to healthcare providers in a different location for assessment and recommendations [2]. Figure 3 shows an overview of the architecture of the RPM system with the description of key components.

- **Patient Monitoring Device**: The electronic devices used to collect health measurements (representing various health metrics of the patient) from the patient, such as heart rate monitors, blood glucose meters, or blood pressure cuffs.
- **Patient**: The individual whose health data is being monitored and collected. Usually, they have the ability to view their own health data and receive notifications through a mobile app or a patient portal.
- **Cloud Central Repository**: The collected health data is transmitted, by wire or wirelessly (such as Wi-Fi, cellular networks, or other wireless communication technologies), to a cloud central data repository, which is a secure, centralized cloud storage system where the patient's health data is stored and managed. It serves as the data hub for the system.
- **Third-Party Services**: External services that may interact with the RPM system, which could include additional analysis tools, billing systems, or electronic health records (EHR) systems.
- **Data Processing and Analysis**: Usually, this is an automated process or service that handles the initial processing and analysis of the health data before presenting it to the healthcare provider. The analysis result will then be sent to the health provider and healthcare provider interface.
- **Healthcare Provider**: By analyzing the result of data processing and analysis, they take medical care or actions for the patient and send the treatment plan to the patient via the healthcare provider interface.

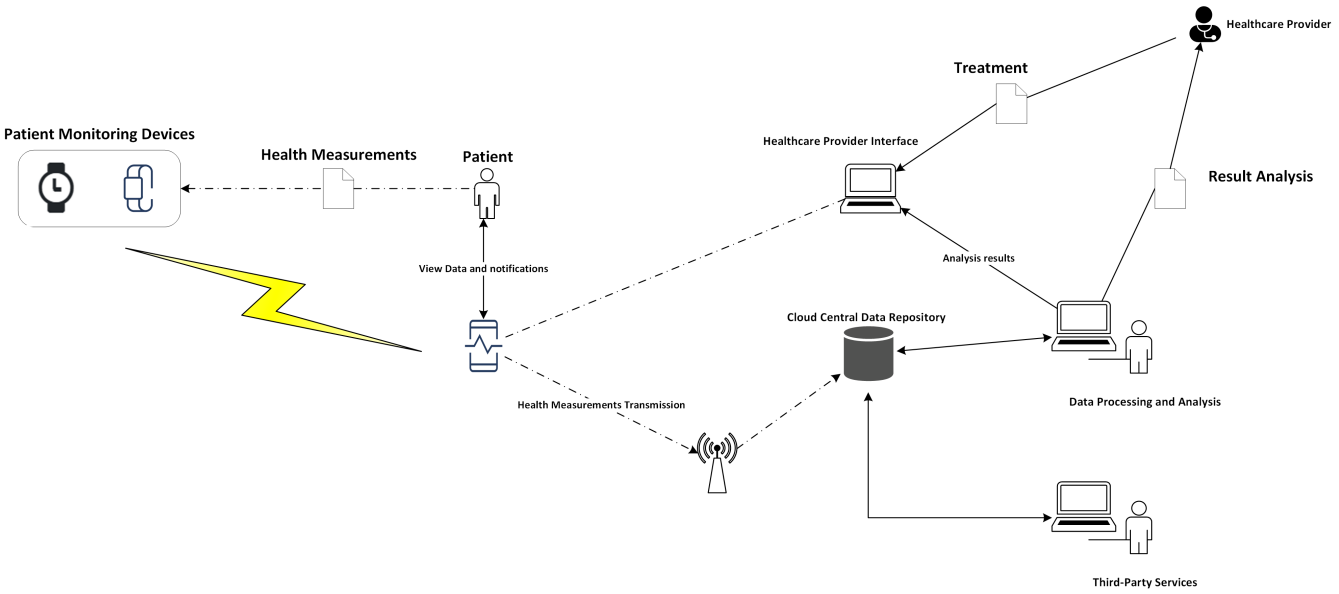

Figure 3: Architecture of Remote Patient Monitoring Systems.

- **Healthcare Provider Interface**: The platform or interface through which healthcare providers can access patient data for review and analysis.

The flow between these components starts with the collection of health data from the patient, then transmitted to the cloud repository. This data can be accessed by healthcare providers and third-party services for further analysis. The results of this analysis inform the treatment provided by healthcare providers, completing the loop of continuous patient care. This innovative approach allows for continuous monitoring of patients outside of conventional clinical settings, such as in the home, enhancing access to healthcare services and improving the management of chronic diseases [11].

4 IMPLEMENTATION OF THE TVRA AND SPYDERISK

4.1 Application of TVRA process key steps

The TVRA process was applied to the remote patient monitoring system use case. In this section, we will only summarise the outcomes of the risk assessment:

- Context Establishment: The scope of the TVRA is the RPMS system in the Figure 1. The most critical assets in the use case are:
  - **Patient Health Data**: This is arguably the most critical asset in an RPM system. It includes sensitive personal health information, and also treatment data, and its compromise could lead to severe privacy violations and potential health risks.
  - **Data Processing Servers**: These servers not only store sensitive data but also process it for analysis. A breach here could lead to massive data loss or manipulation.
  - **Healthcare Provider Interfaces**: These are the platforms through which healthcare providers access patient data. Unauthorized access or disruption could hinder medical care.
- Applicable Catalogues: The TVRA uses a knowledge base that provides relevant information for risk assessment in the RPMS use case
  - **Applicable threat actors catalogue**: a list of threat actors was prepared for this using the Methods and Objectives (MOL) library in the Threat Agent Risk Assessment, or TARA methodology (IT@ Intel White Paper, 2009). The catalogue considers threat agent, their motivation and their technical capabilities. For example a medical physicist with privileged access to a medical device often has the highest capabilities to create the most critical threats
  - **Applicable Threat and Vulnerability Catalogues**: This list details applicable threats and vulnerabilities derived from widely known taxonomies such as ENISA taxonomies and NIST (NIST) and that can be extended to the use case. For example. Threats such as unauthorized access, data interception, and service disruptions are included in the catalogue but also applicable in the use case as they pose significant risks to the confidentiality, integrity, and availability of crucial assets, including patient health data, data processing servers, and healthcare provider interfaces.
- Stakeholder Input: The proposed TVRA also considers key stakeholder - key stakeholder inputs—ranging from patients' privacy preferences to healthcare providers' clinical data requirements—play a pivotal role. These insights, combined with information from the relevant catalogues, shape a comprehensive risk profile that informs targeted mitigation strategies

The risk assessment outcome and analysis in the TVRA is automated by a dedicated tool called Spyderisk as detailed in the next subsection.

4.2 Automated risk calculation via simulation tooling within the TVRA Process

Spyderisk [10] is an automated risk management toolkit developed by UoS at TRL 6, developed over 9+ years, and open-sourced under the open community project https://github.com/SPYDERISK. It follows the ISO 27005 methodology for cyber security risk management and supports the modelling of socio-technical systems via assets such as computers, networks, software, physical spaces, humans, organisations and jurisdictions. Spyderisk is a knowledge-based tool, where domain knowledge has been encoded in its knowledge base representing different key aspects of risk in different domains: for example It has been applied to trust in communication network situations targeting healthcare [8], data privacy protection [12] and GDPR compliance [5]. The work described in this paper has concerned the link between the domains of cybersecurity and healthcare, as discussed in section 5.2.

Spyderisk provides automation of some functionality of the TVRA process, notably automated calculation of risk likelihoods. Initial steps of the TVRA process provide input to the Spyderisk in that they specify the environment, the elements in, and the priorities of the key stakeholders in the medical device system under test (SUT). The operator of the tool specifies impact levels for different types of risk on different assets in the SUT. Spyderisk enables simulation of the situation and illustrates the level of different types of risk via determination of their likelihood based on propagated likelihoods throughout the system. An illustrative example of Spyderisk for the RPM scenario is shown in Figure 4.

Here, there are three domains:

- The patient and the elements associated with them - the phone, app, sensor, locations where phone can be located).
- The Cloud Central Data Repository – a third party who stores data from sensor via phone app, runs analysis process and generates results.
- The healthcare provider, who interacts with the Data Repository's UI to view analysis results and generate a treatment plan for the patient.

The key data flow in the scenario is that the Sensor is managed by the Sensor App on the Patient's Phone. The App transmits the resulting Patient Measurements to the Data Repository, where it is stored and analyzed by the Analysis Process. This generated Analysis Results, which are viewed by the Healthcare Provider, who generates Treatment Data, which is sent back to the App on the Patient's phone and viewed by Patient. This data flow occupies the top third of Figure 4. The middle third models the ICT infrastructure, and the lower third models organizations and physical spaces.

As an example of a key risk, the tool has identified a "High" level risk of "Loss Of Authenticity" at the Patient Measurements data. This means forging or alteration of data in a way designed to induce false behaviour in other assets consuming the data. Clearly, this risk is serious since this data is input to the Sensor Analysis Process, whose results are used by the Healthcare Provider to make judgements about the Patient. Navigating the risk in the Spyderisk UI shows a direct cause: that a compromised service "Sensor App" (on the Patient's Phone) injects fake content into the encrypted flow of "Patient Measurements" via "DB": if an attacker can compromise service "Sensor App", they can access its cryptographic key and alter data "Patient Measurements" flowing between "Sensor App" and "DB". This illustrates the propagation of threats – the Healthcare Provider may make incorrect judgements because they rely on Analysis Results data, which in turn relies on Patient Measurement Data, and which is generated on the Patient's Phone by the Sensor App. Here, Spyderisk recommends secure configuration of the Patient's Phone as a control: passwords or other authentication are set up including resetting default passwords for all user and administrator accounts, auto-run features disabled to prevent execution without user authorisation for files from removable storage or from the internet, and unnecessary software and especially network accessible services removed or disabled.

5 DISCUSSION

5.1 Automation of Risk Assessment in the TVRA process

In this work, we used Spyderisk to automate several processes within the proposed TVRA. By automating the key processes, we can identify threats by mapping attack paths, calculates risk based on likelihood and impact, suggests practical mitigations, and generates comprehensive reports for compliance. This automation streamlines the TVRA process, making risk assessment more efficient and effective for cybersecurity professionals managing complex IT systems.

Moreover, the knowledge base garnered from the TVRA process can significantly enrich the Spyderisk tool through a knowledge engineering/domain modeling process. The catalogues used, a product of knowledge acquisition designed to facilitate the TVRA process, can also serve as a foundational knowledge base to augment the capabilities of Spyderisk, and implementation of this is planned as further work. Given that TVRA and Spyderisk operate under a similar overarching schema, integrating knowledge from one to the other is seamlessly efficient. This compatibility not only simplifies the mapping process but also fosters broader contributions to the Spyderisk Open Community Project, enhancing the collective cybersecurity knowledge base.

5.2 Link between domains of medical devices and cybersecurity

A key observation in this work is that there are two different domains coming together: that of the medical world and the cybersecurity world. Both worlds have risk assessment methodologies, exemplified by ISO 14971 for the safety of medical devices and the ISO 27000 family for information security (notably ISO 27005 for risk assessment). The processes of ISO 14971 and ISO 27005 are largely similar, in that both consider the causes of risks to be threats, and that consequences of risks harm assets ("anything that has value" [ISO 27005], which can include non-ICT concepts such as people and places). The nomenclature of the two domains is different, but it is possible to map between them, as shown in the example of Figure 5.

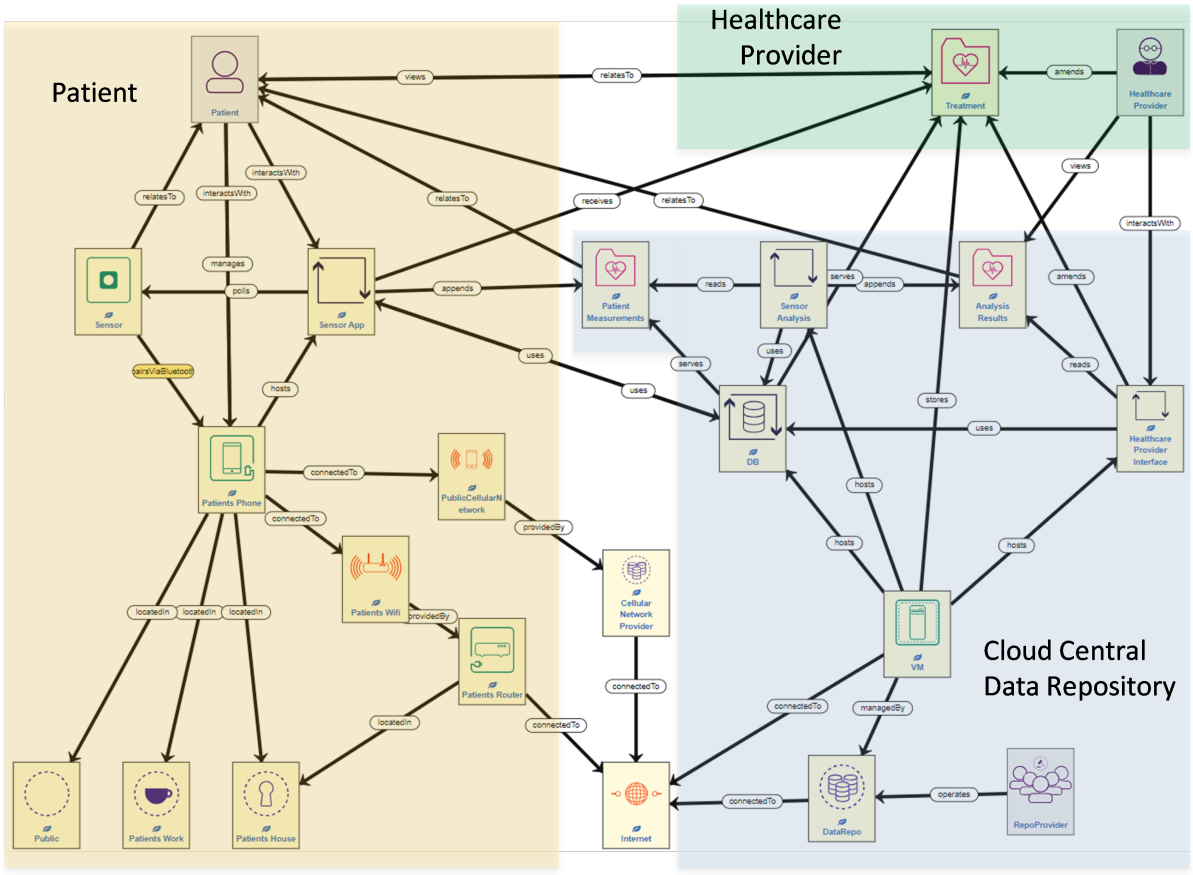

Figure 4: Spyderisk Risk Model for RPMS system.

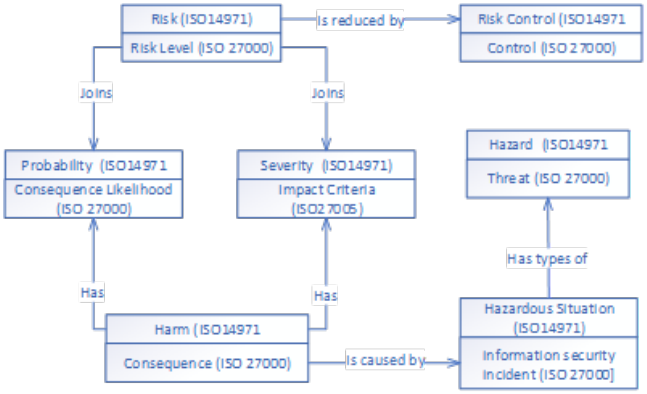

Figure 5: Mapping between cybersecurity risk concepts and medical device risk concepts.

A challenge remains, in mapping the cause and effect relationships exemplified by threat & consequence in the cybersecurity domain link to and hazard and harm in the medica device domain. A case in point is to understand how cybersecurity threats and risks lead to medical harms and which controls from cybersecurity can reduce the likelihood of such harms.

Research into cybersecurity's impact on medical devices underscores the CIA Triad's (Confidentiality, Integrity, and Availability) (see e.g. [7]) pivotal role in healthcare. Integrity is paramount; incorrect data can lead to adverse treatment outcomes. Availability's importance varies with the condition, where delays can critically affect care. Confidentiality breaches, while not directly altering treatment, violate privacy and heighten cyber-attack risks. This work highlights the necessity of robust data security in medical devices for patient safety and legal compliance.

Current work being undertaken involves understanding different types of patient harm and mapping them to the cybersecurity risks described above. Patient harms can be actual harms, for example incorrect configuration of an infusion pump caused by unauthentic configuration data giving the patient an overdose; or can be compromise of clinical benefits, for example those quoted in MEDDEV 2.7/1 rev.4 [9]:. "positive impact on clinical outcome", "patient's quality of life", "outcomes related to diagnosis", "positive impact from diagnostic devices on clinical outcomes", and "public health impact". Sources such as this provide taxonomies of clinical benefit and harm, and other literature, e.g., Williams & Woodward [3] provides sources of medical devices, vulnerabilities and suggests

mappings to clinical harms (i.e. compromises to clinical benefits). This is work in progress and is at the stage of knowledge gathering via literature survey. Subsequent steps will involve classifying this knowledge into the types as depicted in Figure 5 for update of the Spyderisk knowledge base. Results from this work will be published in due course.

6 CONCLUSIONS

To address the pressing cybersecurity problems and unique challenges faced by the healthcare sector in the digital age, this paper proposed a specialized TVRA methodology process for IoMTs that is automated by a dedicated risk management tool, SPYDERISK to become a novel solution to identify, evaluate, assess, and mitigate potential security threats effectively in IoMT environment. The deployment of the proposed TVRA methodology alongside SPYDERISK within the Remote Patient Monitoring Systems framework marks a considerable progression in the protection of healthcare services. This integration offers a fortified healthcare environment, enhancing security measures for all stakeholders involved.

ACKNOWLEDGMENTS

The research described has been carried out as part of the MedSecurance Project (grant agreement No.101095448) and the NEMECYS Project (grant agreement No.101094323), both of which have received funding from the European Union's Horizon Europe Research and Innovation Programme.

REFERENCES

[1] 2022. ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization. https://www.iso.org/standard/iso-iec-27001-2022-v1

[2] F. A. C. de Farias, C. M. Dagostini, Y. de A. Bicca, V. F. Falavigna, and A. Falavigna. 2020. Remote patient monitoring: a systematic review. *Telemedicine and e-Health* 26, 5 (2020), 576–583.

[3] M. Howard and S. Lipner. 2006. *The security development lifecycle.* Microsoft Press Redmond.

[4] X. Lyu, Y. Ding, and S. H. Yang. 2019. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications* 4, 3 (2019), 221–232.

[5] Vangelis Malamas, Fotis Chantzis, Thomas K Dasaklis, George Stergiopoulos, Panayiotis Kotzanikolaou, and Christos Douligeris. 2021. Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access* 9 (2021), 40049–40075.

[6] L. P. Malasinghe, N. Ramzan, and K. Dahal. 2019. Remote patient monitoring: a comprehensive study. *Journal of Ambient Intelligence and Humanized Computing* 10 (2019), 57–76.

[7] Carsten Maple. 2017. Security and privacy in the internet of things. *Journal of Cyber Policy* 2, 2 (2017), 155–184.

[8] RJ McFarland and SBO Olatunbosun. 2019. An exploratory study on the use of internet of medical things (iomt) in the healthcare industry and their associated cybersecurity risks. The Steering Committee of The World Congress in Computer Science. *Computer Engineering and Applied Computing (WorldComp). https://csce. ucmss. com/cr/books/2019/LFS/CSREA2019/ICM2519. pdf* (2019).

[9] Stephen Phillips, Steve Taylor, Michael Boniface, and Mike Surridge. 2023. Automated knowledge-based cybersecurity risk assessment of cyber-physical systems. (Sept. 2023).

[10] Paul Rohmeyer and Jennifer L Bayuk. 2019. *Financial cybersecurity risk management.* Apress, Berkeley, CA.

[11] S. Samonas and D. Coss. 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security* 10, 3 (2014).

[12] Sriram Tarikere, Ian Donner, and Daniel Woods. 2021. Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G. *Bus. Horiz.* 64, 6 (Nov. 2021), 799–807.

[13] H. T. Yew, M. F. Ng, S. Z. Ping, S. K. Chung, A. Chekima, and J. A. Dargham. 2020. Iot based real-time remote patient monitoring system. In *2020 16th IEEE international colloquium on signal processing & its applications (CSPA).* IEEE, 176–179.