SAFECARE

Integrated cyber-physical security for health services

Specification of the e-health security risk management model

Deliverable 6.12

Lead Author: PMS

Contributors: AMC, CNAM, PEN

Deliverable classification: (PU)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Version Control Sheet

Title	Specification of the e-health security risk management model
Prepared By	PMS
Approved By	N/A
Version Number	0.3
Contact	rene.verdonck@philips.com

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
0.1	30/12/2019	Initial draft	RV	RV
0.2	30/01/2020	AMC feedback and addition	TT	TT
0.3	02/02/2020	Updated based on PMS internal review comments and additions	RV	RV
1.0	24/02/2020	Updated based on review comments from AMC, PEN and CNAM	RV	RV
1.1	27/02/2020	Updated reference table	RV	RV

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 787002.

Contents

List of Figures

List of Tables

The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones. They are widely relying on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this proposal is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also participate in increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.

Executive Summary

This deliverable (D6.12) specifies the e-health security risk management model as part of SAFECARE WP6 “Integrated cyber-physical security solutions”.

In accordance with applicable legislations and related standards medical device manufacturers are required to employ cyber security risk management throughout the lifecycle of a medical device. In order to ensure the safety and effectiveness of the medical device the manufacturer also needs to evaluate cyber security aspects amongst other quality aspects of the medical device. The threat landscape for medical devices changes throughout its lifecycle and therefore continuous re-assessments are required in order to ensure the safety and effectiveness of the device.

Goal of the e-health security risk management model is to facilitate this risk management process throughout the lifecycle of the product. It provides a structured approach to identify and analyze the impact of vulnerabilities and threats for medical devices in scope of the assessment using a quantitative approach. Quantification is done by translating the identified risks into security analytics models as introduced by SAFECARE T5.7. The analytics component is used to:

- Measure how often identified vulnerabilities or threat scenarios are observed in the applicable installed base of the medical device in scope of the assessment
- Trigger defined remediation activities by the medical device manufacturer and/or associated service organization.
- Provide insights in effectiveness and usage of mitigating or optional security controls.
- Quantitative feedback will be used to validate the assumed likelihood/impact of the identified vulnerabilities and may result in corrective measures such as medical device security update.

Actors, assets and other specifics of identified vulnerabilities and threat scenarios are documented in the risk assessment including a graphical representation for each vulnerability/scenario using the bowtie methodology. These bowties are an abstract view of the security model of the medical device in scope and related identified threats, vulnerabilities, assets, actors and compensating controls.

1. Introduction

In order to provide optimal use within healthcare environments medical devices are becoming more interconnected and interoperable. Besides increasing complexity and exposure to external sources and threats medical devices are designed for a lifecycle of typically 5, 10 or even 20+ years depending on their intended use. Cyber security risk management is therefore key to ensure the safety and effectiveness of the medical devices throughout its lifecycle as recognized by the industry and legislators.

1.1. Purpose and scope

This document is a deliverable of the e-health security risk management model task 6.7. It details the requirements and related design aspects for the risk management model to be used by medical device manufacturers to identify vulnerabilities and determine associated risk in a structured, visual and quantifiable approach.

Scope is limited to medical devices that are capable of leveraging the e-health devices security analytics (D5.8) SAFECARE component. The model can be applied to other medical devices, however the quantitative part relies on the interconnection with the e-health devices security analytics solution.

1.2. Definitions

Term	Description
AAMI	Association for the Advancement of Medical Instrumentation (https://www.aami.org/)
AE titles	Application Entity Title
Availability	Property of ensuring timely and reliable access to and use of medical device information and functionality
CIA	Confidentiality, Integrity, Availability
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices
COTS	Common Of The Shelf Software
EoL	End of Life
EU MDR IVDR	EU Medical Device and In Vitro Diagnostics Regulation (https://ec.europa.eu/growth/sectors/medical-devices_en)
FDA	US Food and Drug Administration (https://www.fda.gov/home)
GDPR	General Data Protection Regulation (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)
HIPAA	Health Insurance Portability and Accountability Act (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html)

Term	Description
HIS	Hospital Information System
ICS Cert	Industrial Control Systems Computer Emergency Response Team
IEC	International Electrotechnical Commission (https://www.iec.ch/)
IMRDF	International Medical Device Regulators forum (http://www.imdrf.org/)
Integrity	Property of protecting the accuracy and completeness of assets
ISO	International Organization for Standardization (https://www.iso.org/)
NIST	National Institute of Standards and Technologies (https://www.nist.gov/)
OS	Operating System
PACS	Picture Archiving and Communication System
RIS	Radiological Information System
Safety	Safety is associated with accidental risks caused by component failures, human errors or any non-deliberate source of hazard, while security is related to deliberate risks originating from malicious attacks which can be accomplished physically or by cyber means
Safety risk analysis	Risk analysis on safety related aspects of the medical device
TPLC	Total Product Life Cycle
UL	Underwriters Laboratories (https://www.ul.com/)

Table 1 Definitions.

1.3. Methodology

This document was prepared using a combination of desktop research, interviews and workshops with subject matter experts for medical devices in scope of SAFECARE, experts on safety / cyber security risk management and standardization specialists. Methodology used in this document:

1. Provide insights in cyber security risk management for medical devices and related legislations and standards
   (chapter 2 "*Cyber security risk management for medical devices*")

2. List identified requirements for the e-health risk management model as identified based on expert interviews, workshops and desktop research.
   (chapter 3 "*Requirements*")

3. Provide an overview of interconnections of this solution detailing model inputs.
   (chapter 4 "Interconnections").

4. Provide an overview of the solution detailing model inputs (chapter 5 "e-health security risk management model definition").

2. Cyber security risk management for medical devices

2.1. Cybersecurity regulations and standards for healthcare

This chapter provides examples of cybersecurity regulations and standards for healthcare as used in a subset of countries or regions.

2.1.1. Australia

The focus of the Australian guidance for medical device cyber security[1] is on the Total Product Life Cycle (TPLC) approach meaning that cybersecurity aspects such as risk management should be applied throughout the total lifecycle of a medical device, from definition to End of Life (EoL). The guidance recommends NIST framework[2] for defining a risk management strategy and recognizes the following standards besides references to FDA guidances, IMDRF and South Korean ECRI:

- AAMI TIR 57[3]
- UL 2900[4]
- IEC/ISO 27799[5], 29147[6], 30111[7], and more

The guidance stresses the importance of information sharing and vulnerability disclosure and supply chain assessments.

2.1.2. Canada

The Canadian guidance documents[8] focus on the TPLC approach and refers to the same standards and guidance as Australia with special focus AAMI TIR 57, NIST 800-30[9] and UL 2900. For submissions of medical devices, its manufacturer needs to ensure that the submission contains a post-market patching/monitoring plan and security risk management in parallel with safety risk management in accordance with TIR 57.

[1] Australian Medical device cyber security draft guidance and information for consultation. Documentation can be found at: https://www.tga.gov.au/sites/default/files/consultation-medical-device-cyber-security.pdf

[2] NIST Framework for Improving Critical Infrastructure Cybersecurity. Documentation available at: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[3] AAMI TIR57: Principles for medical device security – Risk management. Documentation available at: https://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729

[4] UL 2900-1: Standards for software cybersecurity for network-connectable products. Documentation available at: https://standardscatalog.ul.com/standards/en/standard_2900-1_1

[5] ISO 27799:2016 Health informatics- information security management in health using ISO/IEC 27002. Documentation available at: https://www.iso.org/standard/62777.html

[6] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure. Documentation available at: https://www.iso.org/standard/72311.html

[7] ISO/IEC 30111:2019 Information technology – security techniques – vulnerability handling processes. Documentation available at: https://www.iso.org/standard/69725.html

[8] Canadian medical devices guidance documents. Documentation can be found at: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents.html

[9] NIST 800-30 Guide for Conducting Risk Assessments. Documentation can be found at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

2.1.3. Japan

The primary focus of the Japanese guidance for Ensuring Cybersecurity in medical devices[1] is on risk management. Since the latest revisions, cybersecurity is considered as a foreseeable hazard. Besides NIST SP800-53 it also refers to IEC 80001-2-2[2], IEC 80001-2-8[3] and emphasizes the shared responsibility of medical device manufacturers and healthcare practitioners.

2.1.4. EU MDR and IVDR security guidance

EU recently released EU Cybersecurity guidance detailing concepts around the relation between safety and security risk management and emphasizes on responsibility for medical device manufacturers and healthcare practitioners throughout the lifecycle of the device. It refers to a number of standards and best practices as used by the other countries

2.1.5. IMDRF principles and practices for medical device cybersecurity

In 2011 the International Medical Device Regulators Forum was initiated to discuss future directions for medical device regulatory harmonization. IMRDF published a Medical Device Cybersecurity Guide[4] which emphasizes the TPLC approach and shared responsibility for medical device manufacturers and healthcare practitioners. In addition, it details concepts on information sharing, post market requirements and coordinated vulnerability disclosure process for medical devices. The guidance contains many references as depicted in other guidances discussed in previous sections and more.

2.2. Regulations and implications for medical device manufacturers

Common requirements in regulations as for example discussed in previous sections are related to proper security risk management in accordance with applicable standards or recognized frameworks throughout the lifecycle of a medical device, from definition to End of Life (EoL).

Medical device manufacturers therefore need to ensure that processes and related documentation such as risk management files, requirements and design specifications and product designs must address cyber security related aspects by design in accordance with applicable standards and best practices throughout the lifecycle of the device.

[1] Japanese Guidance for Ensuring Cybersecurity in Medical Devices (Notification No. 0724-1, July 24, 2018). Documentation available at: https://www.pmda.go.jp/english/review-services/regulatory-info/0003.html

[2] IEC/TR 80001-2-2: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and control. Documentation can be found at: https://webstore.iec.ch/publication/7484

[3] IEC/TR 80001-2-8: Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2security needs, risks and controls. Documentation can be found at: https://webstore.iec.ch/publication/24908

[4] IMRDF Medical Device Cyber Security Guide. Documentation can be found at: http://www.imdrf.org/workitems/wi-mdc-guide.asp

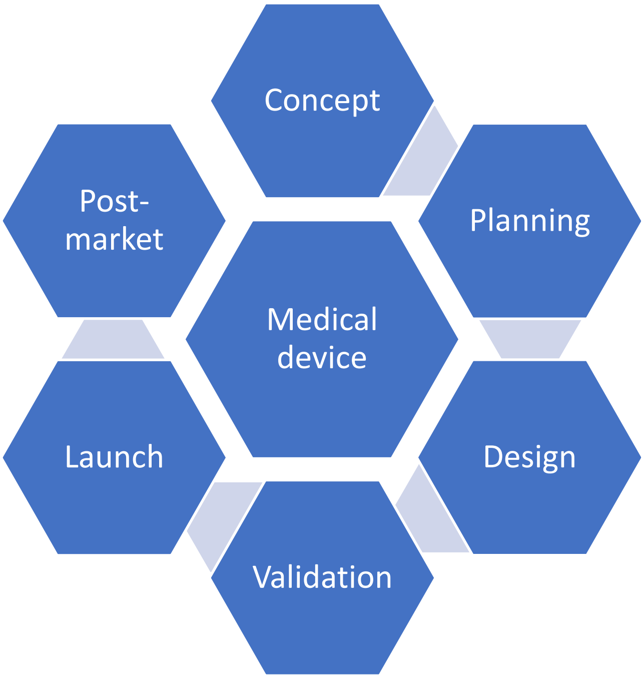


Figure 1 Medical device development lifecycle as defined by BSI[1]

The following steps are recommended to be taken and documented per medical device development stage as derived from the medical device development lifecycle as defined by BSI[1].

- **Concept** - based on intended use, determine which standards are applicable and define related security requirements to protect the confidentiality, integrity and availability of applicable assets. Conduct initial risk assessment.
- **Planning** – prototype solution and consider white box penetration testing to verify vulnerabilities identified during concept stage and to identify potential additional vulnerabilities. Update and complete initial risk assessment and related requirements documentation.
- **Design** – During implementation verify and validate implementation of mitigating security controls (defense in depth) and conduct white- or black box testing to identify potential additional vulnerabilities. Assess security impact of defects/design changes and start with recurring evaluation of in-product COTS components. Maintain risk assessment concerning findings and changes throughout this and following stages. Ensure cyber security related aspects such as vulnerability monitoring, cyber security maintenance plan and related patching are embedded into post-market surveillance activities for the medical device in scope.
- **Validation –** Ensure required cyber security related information and activities are embedded into regulatory submission files before submission. Monitor threat landscape of the medical device on continuous basis and adjust risk assessment and if deemed necessary based on risk assessment outcome update medical device.

[1] BSI Product development lifecycle. Information available at: https://www.bsigroup.com/en-GB/medical-devices/our-services/product-lifecycle/

- **Launch & Post market** Monitor threat landscape of the medical device on continuous basis and release updates based on outcome of risk assessment outcome. Consider upgrade paths during definition of future superseding releases, if no superseding releases planned or foreseen ensure safety and effectiveness of the medical device until End of Life (EoL).

2.3. Vulnerability classification

Vulnerability assessments results for COTS components might differ between vendor/community and medical device manufacturer for components which are used in a medical device. Risk reported by the medical device manufacturer is based on intended use of the medical device and related implemented security controls.

For example, network protocol vulnerability rating from the originating vendor or open source community is high or very high while the reported risk by the medical device manufacturer can be medium or low for a particular medical device (lower likelihood), since following mitigations are applied which will lower likelihood for exploitation:

- **Protocol not exposed on external interfaces** - Network segmentation within the medical device, binding to localhost or other means such as combined with firewall.
- **Limited access and configuration recovery** - User lockdown/kiosk mode and configuration parameter alert/block and revocation at system boot or defined time intervals.

This however does not imply that the vulnerability can remain unpatched. As recommended in the FDA Postmarket Management of Cybersecurity in Medical Devices[1] amongst others, the manufacturer needs to provide routine updates and patches for vulnerabilities even when they are not related to uncontrolled risk of patient harm.

2.4. Regulations and implications for healthcare practitioners

Healthcare practitioners are responsible for using devices as intended by the manufacturer, and follow operational instructions that have been provided. The manufacturer is responsible to provide these instructions, which should contain information such as the following:

- Expected environment in which the device is supposed to be used.
- Recommended cybersecurity controls the practitioners are expected to implement (e.g. access control policies, firewalls).
- Recommendations and instructions related to patch management.
- Recommended physical security measures practitioners are expected to take.
- Description of device security features present, such as OS hardening, antivirus or disk encryption.
- List of network ports and other interfaces that are expected to send or receive data.

[1] FDA Postmarket Management of Cybersecurity in Medical Devices. Documentation can be found at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

- A description of how audit logs are written, stored and archived. Instructions should be provided on how such logs can be inspected.
- Description of backup and restore features.
- Description of configuration options relevant to security. When possible, such options should use secure defaults. When diverging from a default setting has security implications, these should be clearly communicated.

The practitioners are responsible for following these instructions and assuring that security is maintained during the operation of the system, especially when changes take place in the environment in which the device is used. Additionally, practitioners should document their patch management and general security policies, and evaluate whether these are consistent with the recommendations and security properties documented by the manufacturer.

Personnel should be properly trained in the event of security issues, and maintenance (including the installation of security patches) should be done as required. When (suspected) incidents occur, or when vulnerabilities are discovered or reported, the practitioners should notify the manufacturer. If the practitioner wishes to carry out a type of penetration or security test on the device, this should be coordinated with the manufacturer.

Practitioners should evaluate whether the documented (security) properties provided by the manufacturer are consistent with their own security policies. When this is not the case, the manufacturer should be informed. They are then expected to either implement any necessary changes, or motivate why an exception should be made to the policy.

With respect to the specific issue of firewalling and network segmentation, there is a joint-responsibility between the practitioners and manufacturer: the practitioners should make sure open ports are not accessible from the internet or unnecessarily exposed to too many subnets or segments. However, the manufacturer should not design the device under the assumption that exposed services are inaccessible to attackers due to practitioner firewalls: this means these services must authenticate incoming connections even when a recommendation is documented that states that practitioners should restrict incoming traffic to these services.

When it is desired to make use of a device's remote maintenance option, both parties should establish a secure connection (for example through an VPN tunnel) and establish a procedure for utilizing this functionality. This procedure should contain mitigations against social engineering attacks (such as impersonation of the manufacturer over the phone). Credentials and cryptographic keys should be exchanged securely, and a method should be available to revoke or rotate them.

3. Requirements

As stated in the introduction the main goal of e-health security risk management model is to assist with the identification of potential vulnerabilities of a medical device, associated risk and definition of compensating security controls or measures. This chapter details applicable requirements for the e-health security risk management model from both medical device manufacturer as well as healthcare practitioner's point of view.

3.1. Generic requirements

- **Applicability of risk management model:** e-health security risk management model is intended to be used pre-market during the definition and implementation of the medical devices as well as post-market when used by healthcare practitioners and therefore throughout the entire lifecycle. Outcome of (re)assessments might result in changes related to the medical device itself or related development and maintenance processes.
- **Standards and best practices:** applicable international standards, industry best practices related to risk management and medical device standards and regulations as defined in chapter 2.1 are considered as input for the definition of the e-health security risk management model.
- **Safety and Security:** risks with potential safety impact shall be clearly marked for input into medical device safety assessment.
- **Assessment team:** assessment will be conduct using a team of trained experts and recommendation is to include experts for at least the following domains: cybersecurity, safety, architecture and clinical.

3.2. Functional requirements

- **Vulnerability scenario elements:** model shall use a defined list of assets, threat agents and access methods applicable for medical devices to determine potential threat scenarios.
- **Compliance assessment:** model shall use a defined list of mitigating controls derived from international standards to determine the level of compliance of the medical device in scope.
- **Common vulnerabilities:** model shall use a predefined example list and reference to active external sources with known medical device vulnerabilities as input for vulnerability identification.
- **Vulnerability identification and mitigations:** vulnerabilities are identified analyzing non-compliances with the defined list of mitigating controls, analysis of common vulnerabilities and brainstorm sessions with subject matter experts using the vulnerability scenario elements.
- **Risk classification:** define cyber security risk classification scheme to determine the severity, likelihood and risk for initial risks and perceived residual risk after implementation of related mitigation(s).
- **Visualization of risk:** The goal of the visual representation is to provide a high-level overview of the security design for the applicable medical device and to identify which controls need to be monitored by security analytics (T5.4). Therefore, the visual representation shall contain each identified vulnerability and related threat scenario elements, mitigating controls and residual risk.
- **Quantitative input for risk management:** Quantitative feedback received from security analytics is integrated into the post market surveillance process and might trigger a re-assessment.

3.3. Healthcare practitioner requirements

- **Notification of corrective actions**: Medical device manufacturer needs to send timely notifications about identified elevated risks. Notifications should also contain potential measures that can be taken by the healthcare practitioner to reduce the likelihood of a potential event. The healthcare practitioners are required to react appropriately upon receiving such notifications. The medical device manufacturer should be available to offer mitigation advice.
- **Notification of preventive actions**: Medical device manufacturer notifies healthcare practitioner on the availability of security updates for applicable medical devices and indication how to apply these patches e.g. installation executed by medical device manufacturer's service organization.
- **Security and privacy of inputs:** Medical device manufacturer assures that gathered security data, which serves an input to the model, is sufficiently protected in transit and does not contain patient data. The healthcare practitioners are required to follow instructions from the manufacturer regarding the secure installation and maintenance of the solution. Unavailability of the security analytics or risk management model solutions should not negatively affect availability of medical devices.

4. Interconnections

This section provides an overview of the interconnections between the e-health security risk management model and other SAFECARE components.

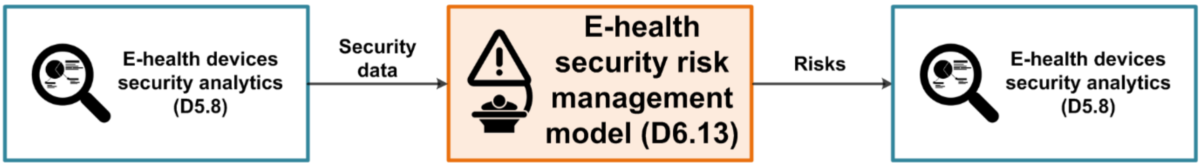

E-health devices security analytics (D5.8)
Security data
E-health security risk management model (D6.13)
Risks
E-health devices security analytics (D5.8)

Figure 2 Interconnections between security analytics and other components in SAFECARE

As shown in Figure 2, the e-health security risk management model only interacts with the e-health device security analytics (D5.8) component. In accordance with the DoA there should be a direct connection between the e-health security risk management model and the data exchange layer (D6.3), however it has been collectively decided by the consortium that this is no longer needed and that relevant events are reported by e-health device security analytics (D5.8) component instead.

e-health security risk management model:

- **Output**: list of vulnerabilities and related potential exploitation path including preventive and corrective controls. e-health device security analytics (D5.8) component will convert this output into models for monitoring sequence of potential events with malicious intent and monitoring of preventive and corrective controls.

- **Input**: e-health device security analytics (D5.8) component reports hits of the models for the defined sequence of events as well as for success/failure hits for the preventive and corrective controls. This data is used as input for further analysis of events and can trigger a re-assessment of the applicable or new vulnerability or refinement of the model.

For more details on format used for communication with e-health device security analytics see chapter 5.3.2

5. e-health security risk management model definition

5.1. Deployment view

The e-health security risk management model consists out of three main activities; risk assessment for medical device, security analytics and monitoring of the installed base for the applicable medical device as depicted in figure 3.

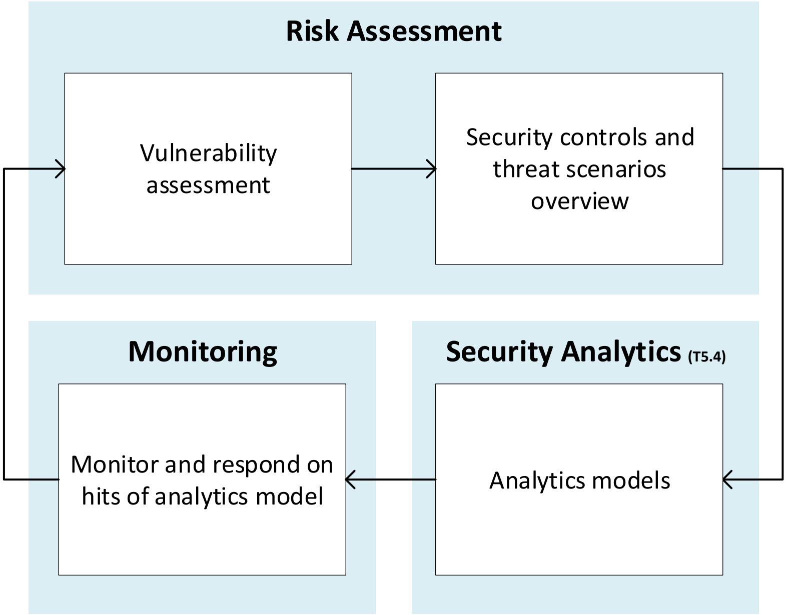

Risk Assessment
Vulnerability assessment
Security controls and threat scenarios overview
Monitoring
Monitor and respond on hits of analytics model
Security Analytics (T5.4)
Analytics models

Figure 3 Logical view of the e-health security risk management model

- **Vulnerability assessment:** Identify potential vulnerability/threat scenarios using a defined list of actors, assets and potential non-compliances with industry best practises.

- **Security controls and threat scenarios overview:** Define mitigating measures and identify key security controls and threat scenarios which are required to be monitored as part of the post-market surveillance process (monitoring). In addition, define a work instruction for the remote monitoring team detailing what needs to be done and in which order in case of a confirmed hit of a threat scenario and/or compromise of a key security control. Communication of scenarios and other key elements between risk assessment team and security analytics team will be done using bowties (see chapter 0).

- **Analytics models**: Convert the threat scenarios and security controls listed in the applicable bowtie to an analytics model(s) using brainstorm and proof of concept sessions to define how to detect the scenarios and compromise of controls. Implement the final analytics models into production environment and monitor them throughout a predefined timeframe.

- **Monitor and respond on hits of analytics model:** Monitor the installed base of applicable medical devices using the analytics model. In case of a hit use the work instruction to report it to the product security incident response team and remediate the issue. Product security incident response team evaluates the incident and reviews the risk assessment to determine if the likelihood, impact and associated risk needs to be re-evaluated. Based on the potential re-evaluated risk the outcome might result into changes for the affected medical device. Number of hits and related activities are recorded in the risk management file of the medical device.

5.2. Risk assessment methodology

Following steps are derived from the analysis of applicable standards as referred to in chapter 2 and are recommended throughout the risk assessment in order to identify and mitigate vulnerabilities to an acceptable level.

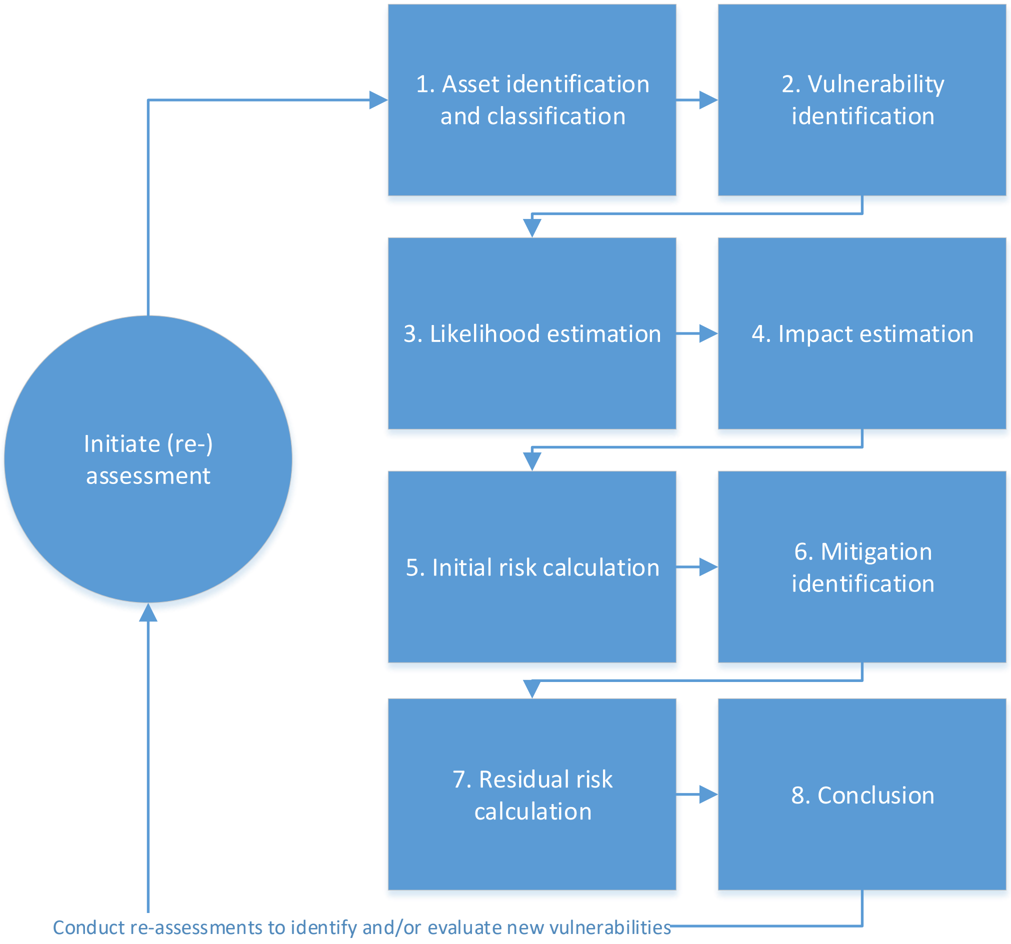

1. Asset identification and classification
2. Vulnerability identification
3. Likelihood estimation
4. Impact estimation
Initiate (re-) assessment
5. Initial risk calculation
6. Mitigation identification
7. Residual risk calculation
8. Conclusion
Conduct re-assessments to identify and/or evaluate new vulnerabilities

Figure 4 Risk Management steps.

5.2.1. Asset identification and classification

The first step is to profile the medical device being assessed. Gather information about the hardware, software, data assets, and services that could be compromised, and classify those assets. See chapter 5.6 for a list of recommended assets and related classification.

5.2.2. Vulnerability identification

The next step is to identify threats that needs to be rated based on the intended use of the medical device, foreseeable misuse and requirements / (intended) design with elevated focus on safety risk control measures to ensure the safety and effectiveness of the device. This can be accomplished by threat modeling, asset/impact assessment a vulnerability assessment, or any combination thereof. Guidance for these methodologies is documented in various standards e.g. the USA National Institute of Standards and Technology SP800-30 section 2.3[1].

While any of the above mentioned methods for identifying threats can be utilized, at minimum, evaluate compliance with

- IEC/TR 80001-2-2[2] chapter 5 "Security Capabilities" and related implementation guidance IEC/TR 80001-2-8[3] and IEC/TR 80001-2-9[4]
- Appendix D of NIST special publication 800-53 rev 4[5]
- ENISA baseline security recommendations for IoT[6]

The relevant non-compliances need to be translated to specific vulnerability scenarios and the associated risk for the medical device needs to be assessed.

As part of recommended post-market surveillance activities review reported incidents (e.g. FDA MAUDE database[7], ICS CERT alerts and advisories[8]) of equivalent medical devices and determine if the exposed/exploited vulnerability is applicable for the medical device in scope. If so, ensure that the vulnerability is captured in the risk assessment.

[1] National Institute of Standards and Technology SP800-30: Guide for Conducting Risk Assessments. Documentation can be found at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[2] IEC/TR 80001-2-2: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and control. Documentation can be found at: https://webstore.iec.ch/publication/7484

[3] IEC/TR 80001-2-8: Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2security needs, risks and controls. Documentation can be found at: https://webstore.iec.ch/publication/24908

[4] IEC/TR 80001-2-9: Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities. Documentation can be found at: https://webstore.iec.ch/publication/31953

[5] National Institute of Standards and Technology SP800-53 rev 5 (DRAFT): Security and Privacy Controls for Federal Information Systems and Organizations. Documentation can be found at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[6] Enisa baseline security recommendations for IoT. Documentation can be found at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[7] FDA Manufacturer and User Facility Device Experience (MAUDE). More information can be found at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm

[8] ICS Cert alerts and advisories. More information can be found at: https://www.us-cert.gov/ics

In addition, conduct vulnerability testing on prototypes and re-test previous versions of the medical device in case of an update/upgrade of an existing version. Recommendation is to review and define test designs and related test cases based on UL 2900-2.1[1] chapter 13 to 19.

Any risk with potential safety impact are clearly marked and later evaluated as part of the safety risk analysis. Recommendation therefore is to include medical device safety and clinical experts in the assessment team to ensure these potential safety items are identified, marked and assessed.

5.2.3. Likelihood estimation

When assessing likelihood assume a hostile and adversarial operating environment without assumptions regarding effective security mitigations being present, for example; "Healthcare practitioner is responsible for securing the network" should not be an acceptable mitigation statement. Once a risk is identified, estimate the likelihood of the threat and the likelihood of the vulnerability, using the method outlined in this section.

Medical devices have different user groups classified as intended users and adversary users. Proposed definition of these groups are threat actors is detailed in chapter 5.5. Impact either adversarial or accidental of a threat actor may differ based on skill level, motive, opportunity and size of the actor population. These aspects need to be taken into account as part of likelihood determination as detailed below based on NIST[2] and OWASP[3].

Threat actor	Adversarial	Accidental (non-malicious)
Skill level	How technically skilled is the threat actor ? - No technical skills - Some technical skills - Advanced computer user - Network and programming skills - Security penetration skills	How able is the threat actor? - Actor executing fixed/automated tasks - Trained privileged actor - Trained regular actor - Not (well) trained regular actor - Neither focused nor (well) trained on preventing errors/mistakes - Actor easily making mistakes or unrecoverable errors

[1] UL 2009-2-1 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems. Documentation can be found at: https://standardscatalog.ul.com/standards/en/standard_2900-2-1_1

[2] NIST Guide for conducting risk assessments. Documentation can be found at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[3] OWASP threat modeling. Documentation can be found at: https://wiki.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Threat actor	Adversarial	Accidental (non-malicious)
Motive	How motivated is the threat actor to find and exploit the vulnerability ? - Low or no reward - Possible reward - High reward	How likely is the threat agent to make unnoticed mistakes due to stress or inattention? - Low - Possible - High
Opportunity	What resources and opportunity are required for the threat agent to find and exploit the vulnerability? - Full access or expensive resources required - Special access or resources required - Some access or resources required - No access or resource required	How often and to what extent does the threat actor have access to the system ? - No authorized access or required for access - Authorized for specific, occasional trained access - Frequent access but only for specific tasks - Routine daily and/or untrained access
Size	How large is the threat actor population? - Developers - System administrators - Intranet users - Authenticated users - Anonymous internet users	How large is the threat agent population? - Developers - System administrators - Healthcare practitioner IT or service engineer - Authenticated users

Table 2 Threat actor likelihood estimation.

As for example stated in the FDA fact sheet regarding its role in medical device cybersecurity[1] and ENISA study cyber security and resilience for smart hospitals study report[2], medical devices are becoming more interconnected and interoperable and are like equivalent systems vulnerable for security breaches, potentially impacting the safety and effectiveness of the medical device. Besides proprietary software introduced by the manufacturer, medical device are also using common of the shelf (COTS) hardware and software components which in turn also can introduce vulnerabilities throughout its lifecycle. Vulnerability rating by vendors or community maintaining these COTS components might differ based on implemented security controls and exposure of these components in the medical device. Therefore, when determining likelihood vulnerability factors such as ease of discovery, ease of exploit, awareness of the vulnerability and detectability need to be taken into account as detailed below.

[1] FDA fact sheet: The FDA's role in medical device cybersecurity. Documentation can be found at: https://www.fda.gov/media/123052/download

[2] Enisa Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures. Documentation can be found at: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Vulnerability factor	Exploitability
Ease of discovery	How easy is it to discover (or to be exposed to) the vulnerability? - Practically impossible - Difficult - Easy - Automated tools available
Ease of exploit	How easy is it to exploit this vulnerability (unnoticed)? - Theoretical - Difficult - Easy - Automated tools available
Awareness	How well known is the vulnerability? - Unknown - Hidden - Obvious - Public knowledge
Detectability	How likely is an exploit to be detected? - Active detection on medical device - Logged and reviewed - Logged without review - Not logged

Table 3 Vulnerability likelihood estimation.

The relevant threat actor and vulnerability factor combination determines the likelihood level for the identified risk. The e-health security risk management model uses the following definition for likelihood level.

Likelihood level	Description
Very High (VH)	A potentially High (H) likelihood can be elevated to Very High (VH) likelihood when it is confirmed by documented/quantitative assessment that virtually no (effective) mitigating factors are present
High (H)	The threat actor is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective. • Requires only an unskilled or unintentional attacker using common equipment, or • Related security control measures are not designed or implemented effectively, or

Likelihood level	Description
	• Vulnerability can be found using automated scanning tools, is publicly known or has been exploited before
Medium (M)	The threat actor is motivated and capable, but controls are in place that may impede exploitation of the vulnerability. In general, choose Medium when the likelihood is neither High nor Low
Low (L)	The threat actor lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited: • Requires a highly skilled attacker using advanced equipment, and/or • Related security control measures are well defined and multi-layered, and/or • Vulnerability is very difficult to discover and hasn't been exploited before
Very low (VL)	A potentially Low (L) likelihood can be lowered to Very Low (VL) likelihood when it can be confirmed by documented/quantitative assessment that mitigations are fully adequate and effective without any need for further action.

Table 4 Likelihood level estimation scale

5.2.4. Impact estimation

Medical devices are designed with a predetermined intended use in mind. Impact on confidentiality, integrity and availability related to the assets as specified in chapter 5.6 combined with the intended use of a medical device might have a different impact outcome depending on the device type/classification. Therefore, the intended use shall be taken into account when determining the impact of a vulnerability.

For example:

- Impact to the availability of a life-sustaining medical device shall yield a high impact rating (ventilator, defibrillator, etc.) and may require additional safety risk analysis, whereas impact to the availability of a non-emergency medical device may yield a lower impact rating.
- Impact to data integrity on a system used to make clinical decisions on dosage or treatment (radiation, anesthesia, etc.) shall yield a high impact rating and may require additional safety risk analysis, whereas impact to data integrity on non-critical data may yield a lower impact rating.
- Impact to data confidentiality on a system containing sensitive data (e.g. patient data) shall yield a high impact rating, whereas impact to confidentiality of non-sensitive data may yield a lower impact rating.

Estimate the technical impact of the risk using the methods outlined in Table 5 Technical impact factors.

Technical impact factors	Impact
Loss of confidentiality — System and data confidentiality refers to the protection of information from unauthorized disclosure (e.g., loss of trade secrets, intellectual property, or personal data). Unauthorized, unanticipated, or unintentional disclosure of personal data could violate regulatory regional or contractual obligations. Confidentiality includes personal data and also extends to intellectual property of the medical device manufacturer (e.g., software code, protocols, documents) or that healthcare practitioners consider secret or proprietary (e.g., business intelligence such as diagnostic procedure type, mix, frequency).	How sensitive is the data? - Non-IP/personal data disclosed - IP data disclosed - Personal data (including staff, service engineers and patients) disclosed - Sensitive data disclosed - All data disclosed
Loss of integrity — System and data integrity requires information to be protected from improper modification. integrity is lost if unauthorized changes are made to the data or system by either deliberate or accidental acts. If the loss of system or data integrity is not corrected, continued use of the compromised system or corrupted data could result in inaccuracy, fraud, or introduce safety concerns. Further, loss of integrity of audit logs is particularly problematic in detecting and correcting security issues. Violation of integrity may be the first step in a successful attack against system availability or confidentiality	How much data could be corrupted and how damaged could it get? - Corrupt session data - Corrupt customization/service data - Corrupt patient/personal data - All data corrupted How could system configuration changes impact integrity? - Creation of privileged accounts - Deactivation of security controls

Technical impact factors	Impact
Loss of availability — If a medical device (or data managed by the medical device) is lost or unavailable to healthcare practitioners, the healthcare practitioners organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may introduce safety concerns, or result in lost productivity	How much service could be lost and how vital is it? - Short, temporary secondary services interrupted with full recovery - Short, temporary primary services interrupted with full recovery - Secondary services/data interrupted - Primary services/data interrupted - All services completely lost

Table 5 Technical impact factors

Determination of impact level is a combination of the technical impact and the intended use of the device. The e-health security risk management model uses the following definition for impact level.

Impact level	Description
Very High (VH)	A potentially High (H) impact can be elevated to Very High (VH) impact when severe impact is confirmed by documented/quantitative assessment.
High (H)	Exercise of the vulnerability • Can constitute a violation of regulatory directives • Can result in the highly costly loss of major assets or resources. • Can significantly violate, compromise, or impede a healthcare practitioners and medical device manufacturers mission, reputation, or interest.
Medium (M)	Exercise of the vulnerability • Can result in the costly loss of tangible assets or resources • Can violate, compromise, or impede a healthcare practitioners and medical device manufacturers mission, reputation, or interest. In general, choose Medium when the IMPACT is neither High nor Low
Low (L)	Exercise of the vulnerability • Can result in the loss of some technical assets or resources or • Can noticeably affect a healthcare practitioners and medical device manufacturers mission, reputation, or interest
Very low (VL)	A potentially Low (L) impact level can be lowered to Very Low (VL) when negligible impact is confirmed by documented/quantitative assessment.

Table 6 Technical impact level estimation scale

5.2.5. Initial risk calculation

Consider the existence and effectiveness of existing controls such as encryption, firewalls, OS and application hardening, application whitelisting etc. and subtract accordingly from the likelihood and impact factors and use the following risk calculation formula:

Risk rating = (Likelihood-existing mitigations)*(Impact-existing mitigations)

Reduction of rating by subtraction is not specifically documented with NIST/OWASP. Impact of mitigations could have been modeled with subtraction or multiplication. Subtraction was chosen for simplicity. Customization of the model is endorsed by both NIST/OWASP.

The calculated value represents the initial risk rating using the following risk rating scale

	Impact				
Likelihood	**Very Low**	**Low**	**Medium**	**High**	**Very High**
Very High	Medium	Medium	High	High	Very High
High	Medium	Medium	High	High	Very High
Medium	Very Low	Low	Medium	High	High
Low	Very Low	Low	Low	Low	Medium
Very Low	Very Low	Very Low	Very Low	Low	Low

Table 7 Risk rating scale

Risk level	Description
Very High (VH)	If an observation or finding is evaluated as a Very High risk, there is a strong and immediate need for corrective measures.
High (H)	If an observation or finding is rated as High risk, there is a strong need for corrective measures
Medium (M)	If an observation is rated as Medium risk, corrective actions are needed and a plan shall be developed to incorporate these actions within a reasonable period of time.
Low (L)	If an observation is described as Low risk, the risk management team shall determine and document whether corrective actions are still required or decide to accept the RISK.
Very low (VL)	If an observation is described as Very Low RISK, the RISK management team can decide to accept the RISK without considering further actions.

Table 8 Recommended actions per risk rating

Recommendation is to quantify impact of actors, assets, likelihood (means) and technical impact based on best practices such as CVSS[1]. CVSS is amongst others a well-known vulnerability

[1] Common Vulnerability Scoring System. More information can be found at: https://www.first.org/cvss/

classification scheme in the IT-world. Consider to use CVSS 3.1 scoring in vulnerability notifications towards healthcare practitioners and other external stakeholders.

5.2.6. Mitigation identification

As a next step, identify additional mitigations to further reduce the likelihood and/or impact factors when deemed necessary based on the initial risk calculation as defined in chapter 5.2.5. It is recommended to review industry best practices for guidance and potential mitigations for the identified risk/vulnerability. In case mitigations are not available on time, temporary workarounds could be investigated to directly reduce risk. Note that impact on risk and likelihood of additional mitigations is determined in chapter 5.2.7.

5.2.7. Residual risk calculation

Consider the newly identified security controls, and subtract accordingly from the likelihood and impact factors and use the same formula and risk classification as detailed in chapter 5.2.5.

5.2.8. Conclusion

Ensure that all previous outcomes are documented and add a conclusion stating the residual risk for the medical device and what further actions are required. These further actions could be to implement additional controls or improved documentation. Consider mitigations for accepted risks to be included in roadmaps for future updates and releases. Recommendation is to ensure sign-off by senior management for residual risk acceptance and implementation of security controls/processes for the product release in scope.

In case of elevated security risks ensure that healthcare practitioners and applicable bodies such as ICS CERT, notified bodies and others are notified regarding corrective measures that healthcare practitioners can take and planned or available preventive measures from the medical device manufacturer such as a software update and how to obtain them.

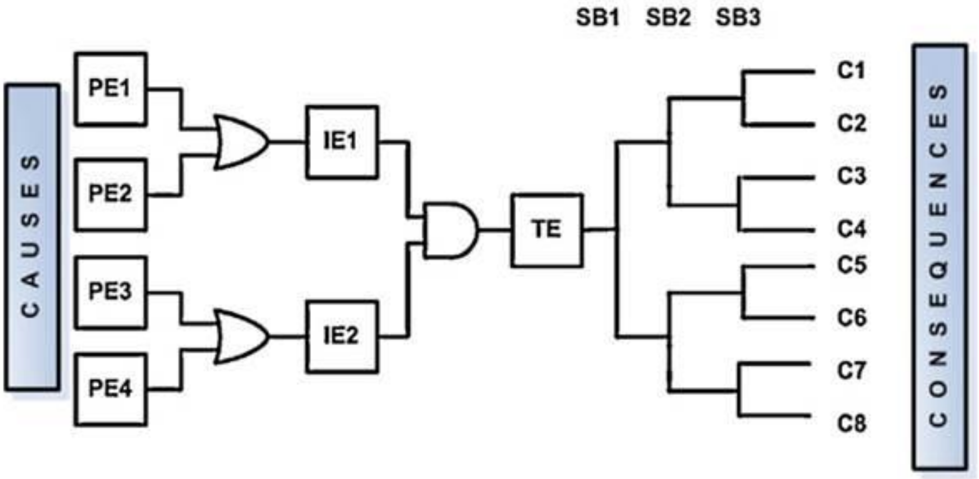
5.3. Risk representation methodology

As a next step, the implemented security controls and identified vulnerabilities will be converted into a graphical overview detailing the security model and related risks of a medical device. As part of WP3 the EBIOS methodology is used for this purpose, however based on positive experience with the BowTie methodology for assessing medical device safety risks our recommendation is to evaluate both methodologies and integrate best-fit solution into the risk assessment template.

5.3.1. Bowtie methodology

The Bowtie methodology is used for this graphical representation. Origin of this methodology is in the chemical industry, where it proved to be useful for accident scenario modeling:

> "Bow tie (BT) is one of the best graphical and numerical approaches to accident scenario modeling from primary causes to final consequences. BT diagram begins with fault tree analysis where primary events leading to the occurrence of a top event are shown on the right-hand side and will continue with event tree analysis (ETA) where all possible consequences based on the success or failure of safety barriers are shown on the left-hand side. Therefore, BT provides a comprehensive modeling of causes-consequences of an accident scenario."



The Bowtie methodology has been adopted by other types of industry including medical device industry to determine product safety hazard analysis by the EU Crystal project (WP 402)[1]. Within the product safety domain, the Bowtie diagrams are used to represent the overall product safety design where risk control measures are plotted between causes, hazardous situations and consequences. Public information on the BowTie approach is readily available, e.g.:

> "BowTie is one of many barrier risk models available to assist the identification and management of risk. (…) BowTie is a visual tool which effectively depicts risk providing an opportunity to identify and assess the key safety barriers either in place or lacking between a safety event and an unsafe outcome[2]. "
>
> "It can be a challenge to see the bigger picture through the maze of safety studies that are conducted. BowTies provide a summary of all of them, getting the key pieces of information out and giving a good overview. In the process, gaps in original safety studies float to the surface which can be answered in a BowTie workshop.[3]"
>
> "Besides being easy to understand, BowTies also provide an overview and insight that is not obtained by any other method of risk analysis & assessment. This is because BowTie actually reduces complexity to a manageable size without losing the context and focus on the critical elements. All too often risk analysis can become progressively more complex, and people in the organisation will stop accepting the increase in complexity. BowTies avoid this and make sure that everyone is kept involved by keeping the complexity at the right level.**Erreur ! Signet non défini.**"

The BowTie approach is represented in **Erreur ! Source du renvoi introuvable.**. While centred on a critical event, BowTie is composed of a fault tree on the left-hand side identifying the possible

[1] EU Crystal project website: http://www.crystal-artemis.eu/

[2] The Civil Aviation Authority website: http://www.caa.co.uk/default.aspx?catid=2786&pagetype=90

[3] The BowTieXP website: http://www.cgerisk.com/software/risk-assessment/bowtiexp

events causing the critical event, and an event tree on the right-hand side showing the possible consequences of the critical event. Important is the separation of the occurrence of a hazardous situation and the consequence by an event tree. The red crosses in the figure represent barriers (risk control measures) that prevent the cause from causing the event (left side) or that mitigate (i.e. reduce) the severity of the consequence.

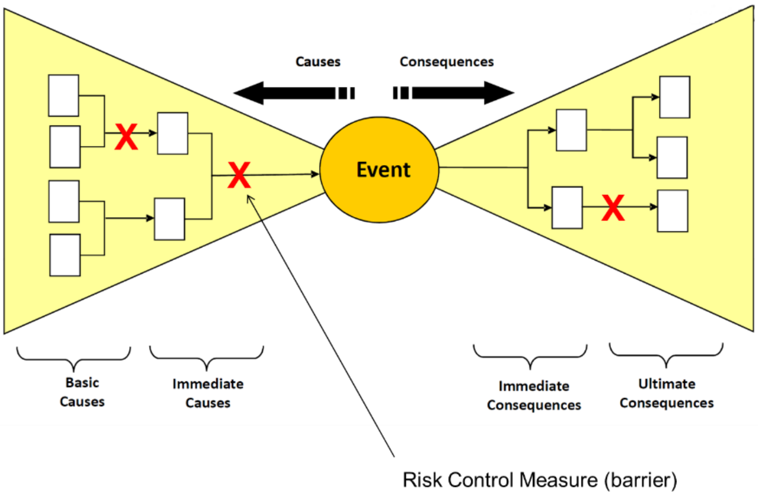


Figure 5: Representation of the BowTie analysis technique.

In the product safety domain, the following simplified representation is used:

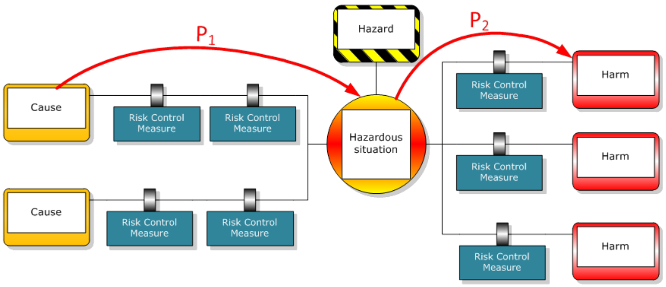


Figure 6: Representation of the BowTie as used in the product safety domain.

In this diagram, the focus is on the safety design and less on the exact details of the sequence of events causing the hazardous situations. The sequences of events are grouped together as "cause". It is important to note that by starting at defining the hazardous situations, a top-down or outside-in approach is followed. As such, the BowTies are a good starting point for explaining why a system is safe and also a good starting point for safety risk assessments. It provides a framework to plot and group actual events as occurring in the real systems in the field.

In the next section, the elements of this Bowtie diagram are explained by using the safety design of a medical device with motorized movements close to the patient.

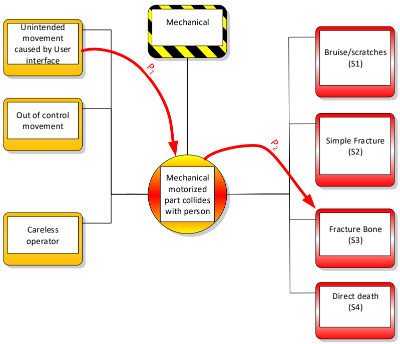


Figure 7 Safety bowtie example for a medical device with motorized movements

In this diagram, the *Top event* (or Hazardous situation) is shown in the middle of the diagram and defined as "motorized part collides with person". On the right side possible *consequences* are indicated ranging from "Bruise/scratches" to "Direct death". The consequences can be classified with an impact severity. On the left side, possible *causes* are indicated. Note that this diagram can also be used to express likelihood calculations:

- $P_{1:}$ On the left side we can express the likelihood for the cause to occur and to result in the hazardous situation.
- $P_{2:}$ On the right side we can express the likelihood for hazardous situation to result in the consequences.

The likelihood of a cause resulting in the consequence is expressed as: P_1 x P_2.

The risk is expressed as the combination of the severity classification of the consequence and the likelihood.

Safety measure can be used to reduce the risk by reducing the likelihood and/or by reducing the severity.

In the next diagram, the risk control measures are added. The position in the diagram represents the effect of the risk control measure. The measures on the left side reduce P_1 i.e. the likelihood on the hazardous situation and the measures on the right side reduce the likelihood on the consequence i.e. reduce the severity of the impact.

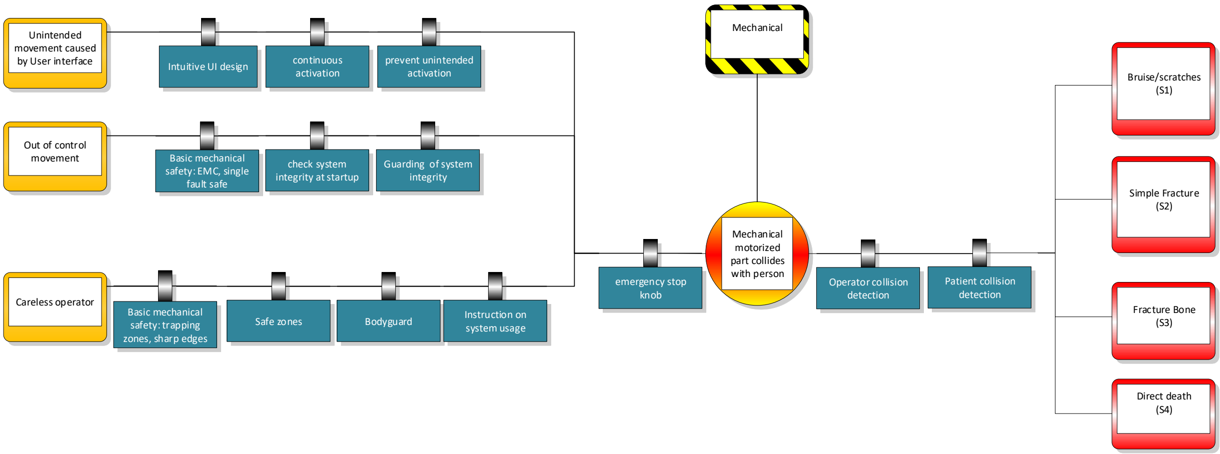

Unintended movement caused by User interface
Intuitive UI design
continuous activation
prevent unintended activation
Out of control movement
Basic mechanical safety: EMC, single fault safe
check system integrity at startup
Guarding of system integrity
Careless operator
Basic mechanical safety: trapping zones, sharp edges
Safe zones
Bodyguard
Instruction on system usage
Mechanical
emergency stop knob
Mechanical motorized part collides with person
Operator collision detection
Patient collision detection
Bruise/scratches (S1)
Simple Fracture (S2)
Fracture Bone (S3)
Direct death (S4)

Figure 8 Safety bowtie example for mechanical collisions with safety measures.

A further enhancement on the BowTie Approach is indicated in the following diagram.

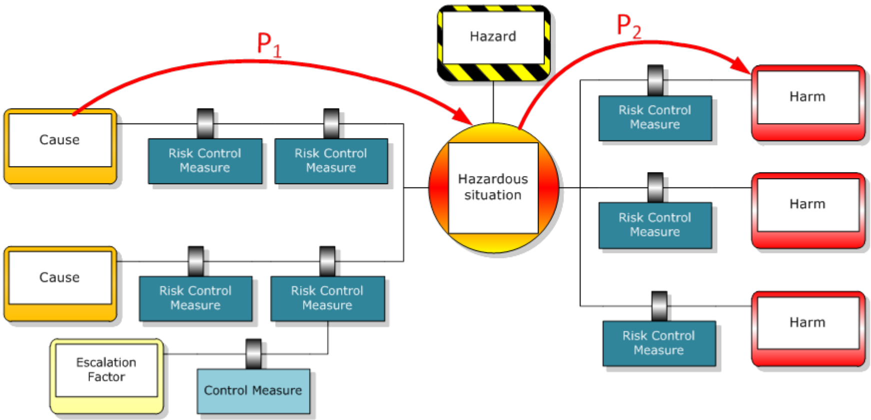


Figure 9: The BowTie approach extended with an escalation factor.

In this diagram, an escalation factor or barrier decay mechanism is added. An escalation factor is a condition that leads to increased risk by defeating or reducing the effectiveness of a risk control measure. The impact of the escalation factor can be reduced by putting additional risk control measures in place. By examining the escalation factors (and the risk control measures that are used to manage them), the methodology reveals important factors that many other types of risk analysis fail to consider. Note that the escalation factors are not direct causes for the hazardous situation, but may indirectly increase the risk. As such, by using the concept of escalation factors, the main causes of a hazardous situation are separated from the indirect causes.

In the example of the mechanical collision safety design, the following escalation factor may be applicable:

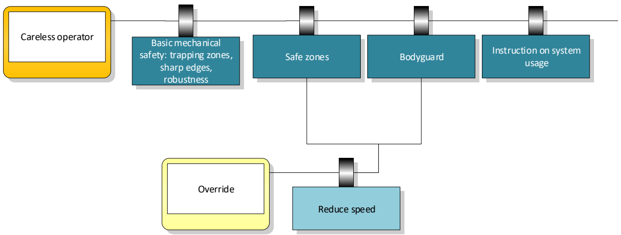

Careless operator
Basic mechanical safety: trapping zones, sharp edges, robustness
Safe zones
Bodyguard
Instruction on system usage
Override
Reduce speed

Figure 10: The mechanical safety diagram extended with an escalation factor and corresponding measure.

The concept of escalation factors can also be represented by the *swiss cheese model*:

Even after designing a safe system and with the risk control measures in place, incidents may occur in the field. This is easily explained by the swiss cheese model. This model was originally formally propounded by Dante Orlandella and James T. Reason of the University of Manchester[1], and has since gained widespread acceptance. It is sometimes called the cumulative act effect.

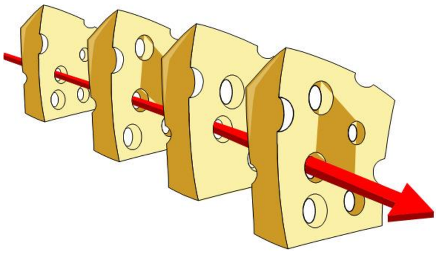
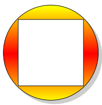


Figure 11: The Swiss cheese model.

> “The *Swiss cheese model* of accident causation illustrates that, although many layers of defence lie between hazards and accidents, there are flaws in each layer that, if aligned, can allow the accident to occur. This model is used in risk analysis and risk management, including aviation, engineering, healthcare, and is the principle behind layered security, as used in computer security and defence in depth. It likens human systems to multiple slices of swiss cheese, stacked side by side, in which the risk of a threat becoming a reality is mitigated by the differing layers and types of defences which are "layered" behind each other. Therefore in theory, lapses and weaknesses in one defence do not allow a risk to materialize, since other defences also exist, to prevent a single point of weakness.“

5.3.2. Translation to medical device cyber security

The elements of a Bowtie diagram can be mapped on the cyber security terminology as indicated below:

Symbol	Description[2]	product safety term	cyber security term
	A ***hazard*** is defined as: "the condition, object or activity with the potential of causing injuries to personnel, damage to equipment or structures, loss of material or reduction of ability to perform a prescribed function".	Hazard	Asset
	***Top event***: As long as a hazard is controlled, it is in acceptable state. Certain events can cause the hazard to be released. Such an event is called the Top Event. The Top Event is not a catastrophe yet, but the dangerous characteristics of the hazard are now in the open. There may be several Top Events related to a particular Hazard.	Hazardous situation	Event (in case of potential safety implications mark as ‘**SAFETY**’
	Often there are usually several factors that could cause the *Top Event*. In BowTie methodology these are called ***Threats***. In the cause and effect relationship between Threat and Top Event, each *Threat* should, individually, be sufficient cause for the *Top Event* to occur if no measures are taken to control it.	Cause or sequence of events	Threat (actor)
	When a *Top Event* does occur it can lead to certain potential ***consequences***. A *consequence* is a potential event resulting from the release of the hazard which results directly in loss or damage. *Consequences* in BowTie methodology are unwanted events that an organization 'by all means' wants to avoid.	Harm	Impact

[1] Reason, James (1990-04-12). "The Contribution of Latent Human Failures to the Breakdown of Complex Systems". Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences 327 (1241): 475–484. doi:10.1098/rstb.1990.0090

[2] Definitions copied from: "What is a BowTie" Across Safety Development GmbH

	Risk management is about controlling risks. This is done by placing ***barriers*** (or ***Controls***) to prevent certain events from happening. A *control* can be any measure taken that acts against some undesirable force or intention, in order to maintain a desired state. In BowTie methodology there are proactive *controls* (on the left side of the *Top Event*) that prevent the *Top Event* from happening. There are also reactive *Controls* (on the right side of the *Top Event*) that prevent the *Top Event* resulting in unwanted consequences.	Risk control measure	Control measure
	In an ideal situation a *Control* will stop a *Threat* from causing the *Top Event*. However, most *Controls* are not 100 % effective. There are certain conditions that can make a *Control* fail. In Bowtie methodology these are called ***Escalation Factors***. An *Escalation Factor* is a condition that leads to increased risk by defeating or reducing the effectiveness of a *control*.	Escalation factor	Control measure vulnerability
	Escalation Control: a *Control* to manage an *Escalation Factor*	Risk control measure	Control measure

Table 9 Bowtie element mapping to medical device cyber security aspects

5.4. Quantification of risk

Risks can be quantified by measuring and monitoring the occurrences of causes and the top events. The Bowtie diagram can be used to indicate the "measuring points". Measuring points at both sides of a barrier provide an indication of the effectiveness of the barrier.

An example from the product safety is shown in de diagram below.

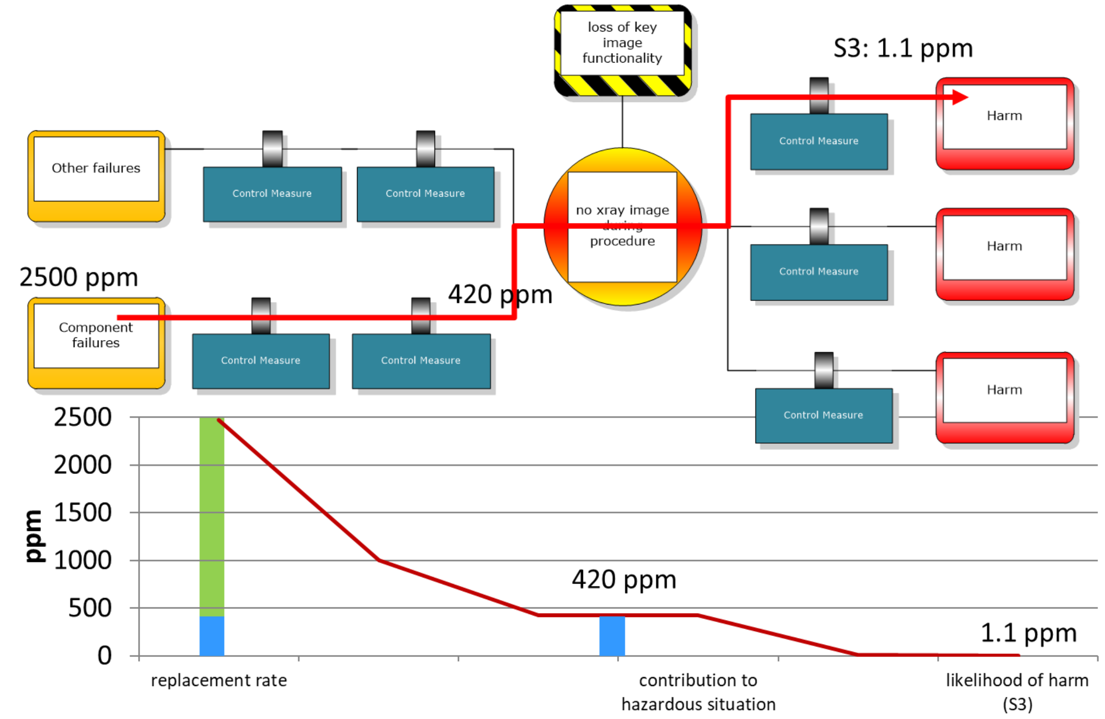


Figure 12: A measuring example from the product safety domain.

In this diagram, the BowTie is related to component failures that block the generation of x-ray images. When x-ray imaging is not available during an interventional treatment, the treatment may have to be aborted and a critical patient may pass away (classified as an S3 case). The failure rate of the components can be measured by monitoring service work orders and counting the number of replaced parts. In addition, it can be counted how many times the system fails during an interventional procedure and how many times an abort of the procedure results in a S3 case. The example in the diagram indicates that the failure rate of the components is 2500 ppm (= per million examinations). The risk control measures on the left side take that only 420 ppm is really impacted the examinations. And the risk control measure on the right side reduce the risk on a S3 case to 1.1 ppm.

5.5. Threat actors definition

This chapter contains the threat actors definition as required per functional requirement "Vulnerability scenario elements".

Threat actor	Description	Occurrence
Security Researcher	Skilled person focused on in depth evaluation of the medical device for exposing design and maintenance related IT vulnerabilities to medical device manufacturer, regulators, security community and general public (also known as white hat hacker).	Adversarial[1]
Advanced Network Threat	Highly advanced/automated (persistent) attack of (non-)specific networks by hackers and malware without motive to specifically attack the medical device.	Adversarial
Hardware defects	Hardware defects of the medical device which might endanger the confidentiality, integrity and availability of the assets.	Accidental
Software defects	Software defects of the medical device which might endanger the confidentiality, integrity and availability of the assets.	Accidental
Intruder	An intruder is not assumed to do any action accidentally (also known as a black hat hacker).	Adversarial
Malicious code	Malicious code introduced during development or malware/ransomware.	Adversarial
Infrastructure outage	Telecommunications, electric power	Accidental
Insider	Healthcare practitioner staff, not skilled attacker but trying to gain professional benefit	Adversarial

[1] *Focus and intent of security researchers is to improve medical device security often in cooperation with medical device manufacturer via coordinated vulnerability disclosure, bug bounty programs or other means for cooperation, however from a medical device perspective this actor will try to use the device outside its intended use and therefore is classified as adversarial.*

Threat actor	Description	Occurrence
Trusted Insider	Healthcare practitioner staff, IT or System Admins, IT savvy, not skilled attacker but trying to gain professional benefit	Adversarial
Clinical Users	Trained healthcare practitioner staff certified to operate the medical device	Accidental
System Admins	Person who is tasked to perform basic administrative tasks on the system (includes healthcare practitioners IT and biomeds).	Accidental
Natural or man-made disaster	Fire, Flood, Windstorm, Hurricane, Earthquake, Bombing, Overrun etc.	Accidental
Engineer	An authorized service engineer/employee, who is responsible to service the medical device, interacts with both clinical and (nonclinical) assets of the system.	Accidental
Automated or Remote access	Automated medical device access from other medical devices e.g. third party integrations. Remote access by medical device vendor.	Accidental

Table 10 Threat actors.

5.6. Technical assets definition for medical devices

This chapter contains the technical assets definition as required per functional requirement "Vulnerability scenario elements". This definition is an addition and tailoring of the list as defined by WP3.

Technical asset	Description
Sensitive data	Health related personal data of e.g. patient, operator, physician or service engineer in databases, images, reports, logging with ePHI (On media, in memory, in transit and on display)
Personal data	Non-health related personal data of e.g. patient, operator, physician or service engineer in databases, images, reports, logging (On media, in memory, in transit and on display)
Healthcare practitioner IT assets	Healthcare practitioners IT assets accessible via network (communication from/to other medical devices, staff IT equipment, PACS, RIS, HIS, any other networked node). Recommendation is to provide a physical topology and dataflow detailing ePHI flow, encryption, and ports used by medical device and adjacent/compatible devices.

Technical asset	Description
Audit trail data	Audit trail data detailing access to/from medical device and related assets such as sensitive and personal data.
Configuration-Calibration-Customization-data	All system settings incl. BIOS, OS configuration settings, anti-malware settings, medical application database configuration, logical interfaces, network addresses, AE titles role permissions, user names & (encrypted) passwords, logging without ePHI.
System software	All software of the medical device including OS, COTS / open source software and proprietary application software integrated into or pre-requisite for the medical device
Hardware	Medical device hardware such as proprietary hardware, PC based hadware, mobile devices / handhelds, physical interfaces (e.g. network interface card(s), wireless, bluetooth, zigbee, serial, USB, proprietary interfaces), Smart cards.
Removable media with ePHI	Static mages and other ePHI stored on removable media (E.g. USB, CD, DVD, printouts).
Removable media and manuals without ePHI.	Software CDs, service documentation, instruction for use.
Logging data	All types of logging data as used for pro- and re-active service activities which might include sensitive and personal data depending on the use-case and related type of logs.
Product Documentation	Documentation as created for and provided to medical device users e.g. paper or electronic instruction for use, service documentation and training tools. This asset also includes confidential documentation from the medical device manufacturer related to architecture and design of the medical device in scope.

Table 11 Medical device related assets

5.7. Requirements mapping

This chapter provides requirements mapping to design details listed in the previous chapters.

Section	Requirement	Design chapter
Generic requirements	Applicability of risk management model	5.1
	Standards and best practices	5.1.2, 5.1.3

Section	Requirement	Design chapter
	Safety and Security	5.1.2
	Assessment team	5.1.2
Functional requirements	Vulnerability scenario elements	5.1.1, 5.4, 5.5
	Compliance assessment	5.1.2
	Common vulnerabilities	5.1.2
	Vulnerability identification and mitigations	5.1.2
	Risk classification	5.1.5, 5.1.7, 5.3
	Visualization of risk	5.2
	Quantitative input for risk management	5.3
Healthcare practitioners requirements	Notification of corrective actions	5.1.8
	Notification of preventive actions	5.1.8

Table 12 Requirements mapping.

6. Related deliverables

The e-health security risk management model consists out of the following deliverables:

- **Risk assessment template** – template that guides the assessment team through the required stages of the risk assessment. Automation is used to automatically calculate the initial and residual risk and provide list of inputs for the bowtie detailing the applicable actors, assets and related security controls.

- **Post market surveillance integration example** – Besides the risk management template T6.7 will also provide an example of
  - Post-market surveillance process example with scope on medical device security.
  - Cyber Security maintenance plan example
  - Document detailing technical information about the impact propagation model and potential cascading effects on medical devices

7. Conclusion

This document specifies the requirements and design aspects of the e-health security risk management model. The model is fit for purpose for medical devices since it is based on applicable international standards, industry best practices and legislations for medical devices.

Besides the requirements and scenarios as defined in SAFECARE deliverables D3.4 “Initial requirements analysis” and D3.6 “Definition of the cyber-physical scenarios of threats”, other sources for common or well-known vulnerabilities are used as examples/input to provide a head start for those starting with this model in a medical device context.

As part of initial experiments conclusion is that the methodology is practical and especially the visualization aspect using the bowtie methodology triggers subject matter and medical device experts to define new vulnerabilities and/or new preventive and corrective controls for existing vulnerabilities and therefore enhancing the allover security posture of the medical device.

Next step is to further refine and implement the model into templates and related processes, as well as the interconnection with the e-health devices security analytics (D5.8) component.

8. References

Reference	Link
AAMI TIR57 Principles for medical device security – Risk management	https://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729
Australian Medical device cyber security draft guidance and information for consultation	https://www.tga.gov.au/sites/default/files/consultation-medical-device-cyber-security.pdf
BSI Product development lifecycle	https://www.bsigroup.com/en-GB/medical-devices/our-services/product-lifecycle/
Canadian medical devices guidance documents	https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents.html
Common Vulnerability Scoring System	https://www.first.org/cvss/
Enisa baseline security recommendations for IoT	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
Enisa Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
EU Crystal project website	http://www.crystal-artemis.eu/
FDA fact sheet: The FDA's role in medical device cybersecurity	https://www.fda.gov/media/123052/download
FDA Manufacturer and User Facility Device Experience (MAUDE)	https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm
FDA Postmarket Management of Cybersecurity in Medical Devices	https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
Healthcare and Wellness Systems	
ICS Cert alerts and advisories	https://www.us-cert.gov/ics
IEC/TR 80001-2-2: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and control	https://webstore.iec.ch/publication/7484
IEC/TR 80001-2-8: Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2security needs, risks and controls	https://webstore.iec.ch/publication/24908
IEC/TR 80001-2-9: Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities	https://webstore.iec.ch/publication/31953
IMRDF Medical Device Cyber Security Guide	http://www.imdrf.org/workitems/wi-mdc-guide.asp
ISO 27799:2016 Health informatics-information security management in health using ISO/IEC 27002	https://www.iso.org/standard/62777.html

Reference	Link
ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure	https://www.iso.org/standard/72311.html
ISO/IEC 30111:2019 Information technology – security techniques – vulnerability handling processes	https://www.iso.org/standard/69725.html
Japanese Guidance for Ensuring Cybersecurity in Medical Devices (Notification No. 0724-1, July 24, 2018)	https://www.pmda.go.jp/english/review-services/regulatory-info/0003.html
National Institute of Standards and Technology SP800-30: Guide for Conducting Risk Assessments	https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
National Institute of Standards and Technology SP800-53 rev 5 (DRAFT): Security and Privacy Controls for Federal Information Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
NIST Framework for Improving Critical Infrastructure Cybersecurity.	https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
NIST Guide for conducting risk assessments	https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
OWASP threat modeling	https://wiki.owasp.org/index.php/OWASP_Risk_Rating_Methodology
Particular Requirements for Network Connectable Components of	-
The BowTieXP website	http://www.cgerisk.com/software/risk-assessment/bowtiexp
The Civil Aviation Authority website	http://www.caa.co.uk/default.aspx?catid=2786&pagetype=90