A Process Framework Combining Safety and Security: In Practice

Fergal Mc Caffery[1,2], Özden Özcan-Top[1], Ceara Treacy[1], Pangkaj Paul[1], John Loane[1], Jennifer Crilly[1] and Arthur Mc Mahon[2]

[1] RSRC&Lero, Dundalk Institute of Technology, Dundalk, Ireland

[2] STATSports Group, Newry, UK

fergal.mccaffery@dkit.ie, ozden.ozcantop@dkit.ie, ceara.treacy@dkit.ie, pangkajchandra.paul@dkit.ie, john.loane@dkit.ie, j.crilly@statsports.com, a.mcmahon@statsports.com

Abstract. Cyber-Physical-Systems provide huge potential for delivering highly effective solutions for multiple safety critical domains such as health, automotive, sports etc. Given the complexity of cyber physical systems, it is important to ensure the safety and security of such systems. Failure of such systems could result in potential harm to people and temporary downtime of important infrastructures with detrimental consequences for industry and society. This article describes a safety and security framework that could be implemented when building cyber physical systems for the safety critical medical device domain. We also provide details of how this framework was implemented in an organisation, STATSports Group, which develops cyber physical systems for performance monitoring of elite athletes to the specification required.

Keywords: Safety Critical Domain, Cyber Physical Systems, Security, MDevSPICE.

1 Introduction

Cyber-Physical-Systems (CPSs) "integrate physical devices, such as sensors and cameras, with cyber components to form an analytical system that responds intelligently to dynamic changes in the real-world scenarios" [1]. Some of usage areas of CPSs in healthcare are intelligent operating rooms, image-guided surgery and therapy, assisted living and fluid flow control for medicine. Given the safety critical health domain, it is important that CPSs are developed to adhere to the domains best practices standards and guidance documentation.

CPSs in the health domain routinely collect, measure and transmit sensitive Personal Health Information (PHI). This data is required to be kept secure through regulations and legislation. The impact of breaches of PHI is

extensive in terms of risk to patient safety [2] and potential costs and losses in reputation for organisations [3]. This research describes a framework to address both of these aspects.

2 A Safety and Security Framework for Medical Device Systems

The framework aims to assist developers to achieve regulatory compliance in safety and security through implementing safety practices and data security controls throughout the development process. It can be used for CPSs in the medical device domain as it combines regulatory process development with product centric risk assessment. Safety and security requirements for CPSs within healthcare are critical as many monitor real-world physical processes. The unique use of diverse communications technologies and mobile computing by CPSs, make safety and security for these systems different from other information systems as data is exposed to many new attack surfaces [4]. The framework promotes safety and security throughout the development process. The framework consists of two main components: (1) MDevSPICE® addresses the safety aspects of the framework [5] and (2) the Secure Data-Flow component addresses the security aspects (see Figure 1). MDevSPICE® consists of processes, purpose statements, capability levels, process attributes, base practices and outcomes. The Secure Data Flow component includes Data Flow Security Controls (DFSCs) founded in regulatory standards, which have been categorised for developer implementation through the ITU-T X.805 Security Architecture for Systems standard [6] and mapped to the risk centric threat model Process for Attack Simulation and Threat Analysis (PASTA) [7]. The secure data flow component also presents a corresponding testing suite designed for the DFSCs to access their effectiveness.

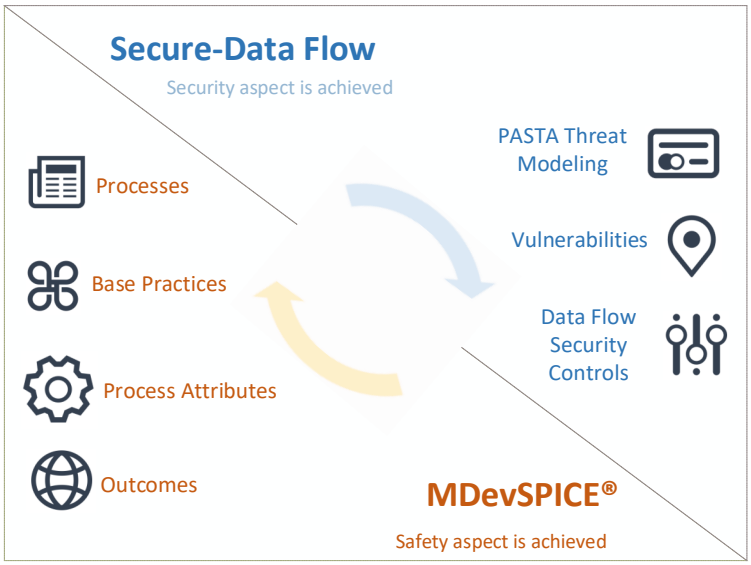

Fig. 1. Components of the Safety and Security Framework.

2.1 MDevSPICE® Component of the Framework

MDevSPICE® is a software process assessment framework that has been designed to enable medical device software developers to produce software that will be safe and easily integrated with other sub-systems of the overall medical device [5]. Relevant medical device software standards and software engineering best practices have been integrated within MDevSPICE®. Two of the prominent regulatory standards that have been integrated into MDevSPICE® are 'IEC 62304:2006: Software life cycle processes for medical device development [8]' and 'ISO 14971:2009: Application of risk management to medical devices'[9]. MDevSPICE® consists of 23 processes grouped into system lifecycle, software lifecycle and support processes as can be seen in Figure 2.

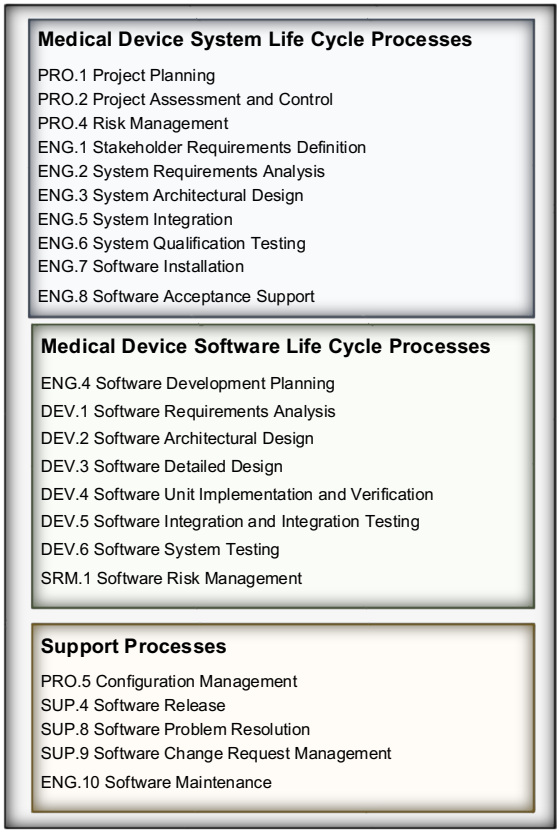

Fig. 2. MDevSPICE® Processes

Software development in safety critical domains such as healthcare is typically performed in a plan-driven manner. The V-Model lifecycle is well suited to medical device software development, given that it dedicates particular attention to both verification and risk management at every stage of life cycle. Software development approaches like agile and lean are preferred industry practice, as they enable iterative and incremental development, collaboration, communication, waste elimination, fast feedback, and balance of predictive upfront work, with adaptive just-in-time work and increasing quality. However, the necessity for intense controls and risk evaluation in safety critical domains require the implementation of agile and lean approaches be performed with some limitations and adaptations. In this context, there is an ongoing process in integration of agile and lean mind-set and practices into MDevSPICE® to make it more flexible and more solution oriented. Consequently, as part of this framework, we have integrated agile practices as part of the improvement recommendations which are provided as an output of performing an MDevSPICE® assessment.

2.2 Secure-Data Flow Component of the Framework

The secure data flow component adopts a risk-centric assessment to assist developers to meet regulatory requirements and secure data in flow [10] within a CPS. CPSs operate in an environment of ever-changing threats and attacks. Security of data flow in this environment requires a risk assessment approach that considers how the evolving threats and attacks could expose the organizations assets to vulnerabilities, weakness of software, hardware, or online service that can be exploited. Threat modelling analysis and threat modelling methods deliver an important basis for the specification of security requirements of information systems and information protection. It provides a process for assessment for securing data flow within CPSs that incorporates security controls into the MDevSPICE® processes.

The developed DFSCs were based on two medical device security standards IEC/TR 80001-2-2:2012 [11] and IEC/TR 80001-2-8:2016 [12]. IEC/TR 80001-2-2:2012 provides 19 high-level security-related capabilities (functions) and risks for consideration when connecting medical devices to IT-networks. These high-level capabilities provide only an understanding of the user needs, security risks that lead to the controls. Two of these capabilities, Transmission Confidentiality (TXCF) and Transmission Integrity (TXIG), concern data transmission. IEC/TR 80001-2-8:2016 identified security controls for each of the 19 security capabilities to consider during risk management activities. The DFSCs originated from the IEC/TR 80001-2-8 controls associated to the TXCF and TXIG capabilities. However, these controls did not cover all aspects of data transmission. Further mapping of the six standards utilized in IEC/TR 80001-2-8 development was completed to address the gap. The result was 63 DFSCs for consideration when completing a PASTA assessment for data flow security. The objective of the secure data flow process is to integrate the DFSCs into a PASTA assessment. The outcome of the secure data flow process provides a set of DFSCs for implementation into the MDevSPICE® software process to address data flow security.

2.3 Implementation

We have implemented the Framework in STATSports[1], a company which develops CPSs, which include hardware sensors, firmware and software algorithms to provide performance monitoring technology to the sports industry.

A. Current Practices

[1] www.statsports.com

STATSports aims to provide technology that meets regulatory requirements for data security and exceeds what is required in the sports domain for product safety. The company understands the requirements for compliancy with both the General Data Protection Regulation (GDPR) [13] and The Health Insurance Portability and Accountability Act (HIPAA) [14] for securing personal and health data. This understanding is due to the fact that in the future STATSports plans on releasing monitoring technology for the healthcare industry and the imminent GDPR requirements for data security. The company recognizes there are significant changes required in development to ensure that data security and product safety are a key part of the process to meet GDPR and HIPAA compliancy. Therefore, STATSports is committed to ensuring they embarked upon implementing best practice processes for both safety and security to successfully transition the development of technology for the sports domain to the medical device domain.

In order for STATSports to make this transition, the first step was to perform an MDevSPICE® assessment to observe the process gaps and challenges in relation to safety and security. This assessment provided insights on the safety and security practices prior to the implementation of the framework. Twenty-three processes were assessed and the following areas for improvement were identified below.

1. There was no single point of contact for gathering new requirements/requirement changes in the organization. The organization's Sport Scientists were directly contacting developers and demanding features to be developed. This resulted in developers' receiving different tasks from multiple sources and it was difficult to understand which new features should be prioritized.
2. A major challenge was that new requirements and features were constantly introduced throughout development.
3. Safety and security requirements were not formally defined and managed, this could give rise to potentially significant changes (i.e. architectural changes) later in the development, particularly if software was released without inclusion of these critical requirements.
4. Frequently, requirements lacked sufficient detail - this lead to instances of redevelopment as Sport Scientists were not always available to provide clarity in relation to requirements.
5. Threats to security and associated vulnerabilities of the system were unknown.
6. Which security controls to implement were unknown.
7. Continuous Risk Assessment and Risk Mitigation for both Safety and Security were not performed.
8. There was no formal traceability from system requirements to the testing and release phases.
9. Limited company experience implementing security in agile software development and how to implement the security guidelines that include security controls

B. Implemented Solutions

The findings' number in the above list in Section 2.3.A will be tagged against the corresponding improvement action below. STATSports has now introduced Scrum practices in relation to the software development process issues combined with lifecycle traceability that is required to demonstrate that safety processes are in place (addresses 1-4). A Senior Sports Scientist (SSS) now works closely with the development team in a Product Owner role. Every new request or requirement change coming from different Sport Scientists and other stakeholders are delivered to the SSS, and are then prioritized by this person (1). The SSS identifies the business value of the features/user stories while the developers assess the risks involved in implementation, with associated safety, security, technical and business risks now tracked throughout development specifically, both safety and security requirements are linked with risks which are assigned to development team members (2, 3, 4). The product backlog and sprint backlog contain features/user stories that are maintained in a prioritized order in a tool, named Jira[2] (1, 3, 4). Jira is used with another tool Confluence[3] to provide traceability of requirements/features and user stories (1, 2, 8).

In addition, a security focused analyst was recruited into the development team and contributes to the architectural design to ensure emphasis on data security (3, 5, 9). The security analyst starts the PASTA process in defining the appropriate level of security requirements to support the business goals in collaboration with the SSS (1, 3). The technical scope is then defined upon receipt of the prioritized requirements from the SSS and coordinated with the architecture design (1, 6, 9). This required STATSports to list all software/hardware, the various technologies, components and services that were associated with the application (4, 6). This followed with the decomposition of the application into components, via Data Flow Diagrams (DFDs) and Use Case Diagrams, which were used to analyze the threats (5, 7). The vulnerabilities were identified for the use cases and the DFSCs required to address these vulnerabilities were presented (5, 7). The DFSCs were represented in the backlog in relation to each feature that is included for development in the sprint (1, 2, 6).

A sprint duration of one week is adopted to manage constantly changing requirements (2, 3). Sprint Review and Retrospective meetings take place at the end of the week in addition to a Daily 15-min Stand-up meeting (1-9). User stories are defined with the associated acceptance criteria, which provide the essential information for the purposes of verification and validation (3, 4). The meetings ensure all members of the development team are kept up to date with progress. It also allows the team to raise issues with the process and identify risks (1-9).

As the system consists of hardware and firmware in addition to software, the framework is also applied to hardware/firmware development and testing. This ensures full traceability for product development from

[2] https://www.atlassian.com/software/jira
[3] https://www.atlassian.com/software/confluence

inception, to prototyping and through to final release (8). All versions of firmware and hardware are captured using confluence and all bugs, hardware/firmware faults and resolutions are logged and viewed in Jira, offering a full historic record of product evolution (1, 2, 5, 8).

We have observed that implementing the secure data flow component in a one-week sprint process was not possible due to understanding all data flow calls and identification of the controls and assessment of threats. In addition, testing requirements of the security controls need to be put in place within that sprint. These require development of a test suite against test cases which would include penetration testing. As a solution for this, we proposed running sprints in two-week intervals and running penetration testing on product release.

3 Conclusion

The Safety and Security Framework for Cyber Physical Systems is a new approach that was developed to promote safe and secure products in the safety critical healthcare domain.

The implementation of the framework in STATSports has revealed issues and opportunities for improvement in terms of both safety and security. The interoperability of the two components was our main consideration. Action items were identified and prioritized. Secure Data-Flow processes including security risk assessment and threat modelling were performed at the initial phases of the project from a higher level of abstraction. During the later stages, security of data flow and security controls were continuously revisited and repeated however not meeting every sprint. The framework has assisted the company in moving towards compliance with HIPAA and the GDPR in relation to data security. It has stimulated the development of suitable policies and procedures for data security required by the GDPR and HIPAA for regulatory compliancy, not only in development but also organization wide. Implementation of the framework has also promoted the inclusion of security in the initial stages of the development of a new product. As a result of the implementation of the framework, STATSports has overcome difficulties they have had in relation to handling changes throughout development. In addition, through introducing Agile and security practices the company has significantly improved the traceability of requirements right throughout development. The company now understands the security vulnerabilities of their system and has put appropriate controls in place.

Future work in the evolution of the framework will involve the execution of data security testing within MDevSPICE® using agile development.

Acknowledgement: This research is supported by the Science Foundation Ireland Research Centres Programme, through Lero - the Irish Software Research Centre (http://www.lero.ie) grant 10/CE/I1855 & 13/RC/2094S.

References

[1] S. A. Haque, S. M. Aziz, and M. Rahman, "Review of cyber-physical system in healthcare," *international journal of distributed sensor networks,* 2014.

[2] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical devices (Auckland, NZ),* vol. 8, p. 305, 2015.

[3] "2016 Cost of Cyber Crime Study & the Risk of Business Innovation-Cyber Security Analysis," Ponemon Institute, Available: https://saas.hpe.com/en-us/asset/2016-cost-cyber-crime-study-risk-business-innovation-ponemon-institute-cyber-security-analysis, Accessed on: 30.05.2017.

[4] G. Howser and B. McMillin, "Using Information-Flow Methods to Analyze the Security of Cyber-Physical Systems," *Computer,* vol. 50, no. 4, pp. 17-26, 2017.

[5] M. Lepmets, F. McCaffery, and P. Clarke, "Development and benefits of MDevSPICE®, the medical device software process assessment framework," *Journal of Software: Evolution and Process,* vol. 28, no. 9, pp. 800-816, 2016.

[6] *International Telecommunication Union ITU-T " Recommendation X.805 Security architecture for systems providing end-to-end communications."*, 2003.

[7] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons, 2015.

[8] *IEC 2006. IEC 62304: Medical Device Software - Software Life-Cycle Processes.*

[9] *ISO 2009. ISO 14971 - Medical Devices - Application of Risk Management to Medical Devices.*

[10] C. Treacy and F. McCaffery, "Data Security Overview for Medical Mobile Apps Assuring the Confidentiality, Integrity and Availability of Data in Transmission," *International Journal on Advances in Security,* vol. 9, no. 3 & 4, pp. 146-157, 2016.

[11] "IEC, TR 80001-2-2:2012 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 controls.," 2012.

[12] "IEC, TR 80001-2-8:2016 Application of risk management for IT-networks incorporating medical devices — Application guidance Part 2-8 : Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2. 2016, pp. 1–56," 2016.

[13] *Reg (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Dir 95/46/EC (General Data Protection Regulation)* 2016.

[14] *OCR Privacy Brief: Summary of the HIPAA Privacy Rule*, 2003.