Cybersécurité des dispositifs médicaux : Environnement règlementaire.

Rapport de stage : ST02 Stage de fin d'études

Réalisé par : KAMGA KAMGA Alban Loique

Pour l'obtention du diplôme de Master Mention « Ingénierie de la santé »

Stage effectué au sein de l'entreprise Pixee Médical situé à 18, rue Alain Savary – 2500 Besançon France

Entre le 22 février et le 26 Juillet 2021

Disponible sur : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids101/

Tuteur Académique	Tuteur en entreprise
Mme Isabelle Claude Enseignante à l'université de technologie de Compiègne	**M. PAUPERT Florian** Responsable qualité et affaires règlementaires

Année Scolaire 2020 – 2021

Résumé

L'augmentation de la proportion des logiciels de santé dans la sphère des dispositifs médicaux, fait de la cybersécurité un enjeu majeur pour les fabricants et distributeurs de dispositifs médicaux. Dorénavant les vulnérabilités et les attaques sont plus importantes que par le passé. Pour contrer cela, anticiper sur les évolutions à venir et mettre sur le marché des dispositifs dignes de confiance, les exigences réglementaires ont été mises sur à jour par les autorités compétentes de chaque juridiction.

Le présent document décrit le processus de gestion de la cybersécurité d'une innovation technologique avec une approche basée sur les risques de sécurité informatique. L'analyse, l'évaluation et la maîtrise des risques ont été mises en place à partir de la méthode EBIOS développée par L'ANSSI. Elle est appliquée sur un logiciel connecté de navigation du genou utilisant la réalité augmentée. Elle permet durant tout le cycle de vie du dispositif de garantir la confidentialité de l'information, l'intégrité des données, l'accessibilité aux ressources et l'audibilité du système. Le socle de la démarche est fait sur le standard UL2900-2-1, accompagné et renforcé par les exigences et les recommandations des référentiels de cybersécurité de la FDA, la TGA et Européen.

Maîtriser la conception, sécuriser par la conception, commercialiser et suivre les activités de sécurité informatique après la commercialisation sont les sujets traités dans ce rapport.

Mots clés : Logiciels de santé, Dispositifs médicaux, Cybersécurité, Approche par les risques, Confidentialité, Accessibilité, Intégrité, Audibilité.

Abstract

The increasing proportion of healthcare software in the medical device sphere makes cybersecurity a major issue for medical device manufacturers and distributors. Vulnerabilities and attacks are now more important than in the past. To counter this, anticipate future developments and bring trustworthy devices to the market, regulatory requirements have been updated by the competent authorities in each jurisdiction.

This document describes the cybersecurity management process of a technological innovation with an approach based on IT security risks. The analysis, the evaluation and the control of the risks have been implemented using the EBIOS method developed by ANSSI. It is applied to a connected software of knee navigation using augmented reality. During the entire life cycle of the device, it guarantees the confidentiality of the information, the integrity of the data, the accessibility to the resources and the audibility of the system. The basis of the approach is the UL2900-2-1 standard, accompanied and reinforced by the requirements and recommendations of the FDA, TGA and European cybersecurity standards.

Mastering the design, securing by design, commercializing and tracking post-marketing cyber security activities are the topics covered in this report.

Keywords : Healthcare software, Medical devices, Cybersecurity, Risk-based approach, Privacy, Accessibility, Integrity, Audibility.

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs Personnes à qui je témoigne toute ma reconnaissance.

Sincères remerciements aux responsables de Master Mme. Françoise MERESSE, et M. Jean Mathieu PROT pour avoir permis d'effectuer ce stage, merci pour leurs disponibilités, leurs conseils, et leurs soutiens lors des démarches administratives ;

Merci à Mme. Isabelle CLAUDE pour l'encadrement durant ce stage, elle a été une source de motivation et d'encouragement pour moi durant toute ma formation. Ses conseils judicieux ont contribué à alimenter ma réflexion ;

Merci à M. Florian PAUPERT pour l'accueil chaleureux au sein de l'entreprise, ses précieux conseils, sa clairvoyance, et ses compétences multidisciplinaires m'ont été d'une aide inestimable dans toutes mes activités, et à la réalisation de ce mémoire ;

Merci à M. Sebastian HENRY et toute la grande équipe de Pixee Medical, l'agréable interaction avec chaque personne a aidé à réaliser mes missions, leur bienveillance m'a permis de m'intégrer au sein de l'équipe et de l'entreprise ;

Merci à tous les enseignants qui ont eu l'aimable attention de partager leurs connaissances nécessaires à résoudre les problèmes dans les tâches qui m'étaient confiées ;

Merci à toute la Famille KAMGA pour leur soutien inconditionnel et leur amour à mon égard ;

Je remercie également tous mes amis, camarades de la promotion et aînés pour leur encouragement, leur aide, et leur dévouement tout au long de cette formation.

Sommaire

Table des matières

Définitions

Dispositifs médicaux : tout instrument, appareil, équipement, logiciel, implant, réactif ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes :

– diagnostic, prévention, contrôle, prévision, pronostic, traitement ou atténuation d'une maladie,

– diagnostic, contrôle, traitement, atténuation ou compensation d'une blessure ou d'un handicap,

– étude, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique,

– communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus,

Et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens[1].

Conformité : satisfaction d'une exigence.

Cybersécurité : C'est le processus visant à empêcher l'accès non autorisé, la modification, l'utilisation abusive ou le refus d'utilisation, ou l'utilisation non autorisée d'informations qui sont stockées, consultées ou transférées d'un dispositif médical à un destinataire externe[2].

Dénis de service : Ce sont des actions qui empêchent le système de fonctionner conformément à sa finalité. Un équipement ou une entité peut être rendu inopérant ou contraint de fonctionner dans un état dégradé ; les opérations qui dépendent de la rapidité d'exécution peuvent être retardées.

Arthroplastie : C'est une Intervention chirurgicale consistant à rétablir la mobilité d'une articulation en créant un nouvel espace articulaire.

Vulnérabilité : C'est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Menace : C'est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation.

Système Fiable : Un système est fiable lorsque la probabilité de remplir sa mission sur une durée donnée correspond à celle spécifiée dans le cahier des charges.

Liste de sigles

CE: Conformité Européenne

US FDA: United State Food and Drug Administration

ANSM: Agence nationale de sécurité du médicament et des produits de santé

WIFI: Wireless Fidelity

SMQ: Système de management de la qualité

CT: Computer tomography

ISO: international organization for standardization

DM: Dispositif Médical

TGA: Therapeutic Goods Administration

ANSSI: Agence Nationale de la sécurité des Systèmes d'Information

AR: Augmented Reality

MDCG: Medical Devices Coordination Group

U: Underwriters Laboratories

SMQ: Système de management de la qualité

SR: Source de risque

ANSSI: Agence Nationale de la sécurité des systèmes d'information

OV: Objectif Visé

NIST: National Institute of Standards and Technology

ISAO: Information Sharing and Analysis Organizations

CBOM: Cybersecurity Bills Of Materials

USB: Universal Serial Bus

SBOM: Software Bills Of Materials

Liste de figures

Liste de tableaux

Introduction

Afin de valider la dernière année de formation en ingénierie de la santé à l'université de technologie de Compiègne, option technologies biomédicales et territoires de santé ; j'ai effectué un stage de 22 semaines au sein de Pixee Medical. C'est une Start up française qui développe les solutions innovantes pour la chirurgie orthopédique. Le stage a permis de mettre en pratique les connaissances théoriques apprisses pendant les dernières années d'études et de consolider l'expérience professionnelle dans le monde de l'industrie médicale.

Durant cette période passée dans le département qualité et affaires réglementaires, la principale mission a été de satisfaire les exigences de cybersécurité en vigueur pour la prochaine version d'un logiciel de navigation du genou installé sur une plateforme d'exécution qualifiée, connecté à un réseau wifi et avec un ports USB C activé. En parallèle, la seconde mission était de mettre sur pied un process pour la gestion des activités de cybersécurité dans le système de management de la qualité de l'entreprise.

Le processus de conformité a été subdivisé en plusieurs micro processus où le stagiaire joue le rôle de pilote de ces micro processus sous la responsabilité du manager processus qui n'est personne d'autre que le responsable qualité et affaires réglementaires.

Le présent rapport met en avant la méthodologie utilisée, présente les différentes étapes qui ont permises d'appréhender dans un premier temps les enjeux du projet, Ainsi que la roadmap utilisée pour mener à bien la mission. Il comporte quatre grandes parties parmi lesquelles :

- La présentation générale de l'entreprise et ses activités ;
- La problématique de la mission et les objectifs à atteindre ;
- Un processus de maitrise réglementaire ;
- Une synthèse

I. Présentation de Pixee Medical

A- Présentation

Pixee Medical est une Start up française située dans la sous-région de Besançon à l'adresse 18 rue Alain Savary, 25000 Besançon. La société apporte une nouvelle vision pour la chirurgie orthopédique, spécialisée dans la conception, le développement, la fabrication, la commercialisation, le service après-vente et les prestations associées de logiciels pour la chirurgie orthopédique et instruments chirurgicaux réutilisables associés.

B- Origine de Pixee Medical

La société a été créée en 2017 dans le but d'apporter une solution technologique complète aux distributeurs de prothèses destinée à l'arthroplastie totale des articulations (le genou, la hanche et l'épaule). Elle utilise la réalité mixte au sein des blocs opératoires, et plus particulièrement pour la chirurgie orthopédique.

C- Organisation

Pixee Medical s'articule autour d'une équipe de collaborateurs aux compétences complémentaires permettant d'être au plus proche des attentes des clients tout en leur apportant des solutions issues des nouvelles technologies et approches thérapeutiques.

Les partenaires de Pixee Medical sont les industriels spécialisés dans le développement de logiciels de santé, dans la fabrication d'instruments chirurgicaux et les laboratoires de recherche affiliés aux universités et aux écoles d'ingénieurs.

Les clients de Pixee Medical sont les fabricants et distributeurs de prothèses orthopédiques. Les utilisateurs des produits de Pixee Medical sont les centres de soins et plus particulièrement les chirurgiens orthopédiques.

D. Solutions médicales

D.1- Le système de navigation KneePlus

Le logiciel KneePlus est un dispositif médical autonome peropératoire, indiqué pour le remplacement total du genou primaire. Ce logiciel autonome est livré sous la forme d'une application Android installée dans une plateforme d'exécution qualifiée. L'objectif principal est d'assister le chirurgien pendant l'intervention grâce à un affichage optique en réalité augmentée (AR).

Les références anatomiques requises sont collectées pendant l'intervention. Toutes les coordonnées collectées sont traitées par les algorithmes de KneePlus pour fournir au chirurgien une orientation pertinente du guide de coupe équipé d'un marqueur vers l'anatomie du patient.

Les références anatomiques sont prises par le chirurgien. Seules des recommandations sur la meilleure façon de faire les acquisitions sont fournies à l'utilisateur.

Pour atteindre l'objectif clinique, le logiciel KneePlus utilise différents types de solutions :

- Un composant technique qui offre une détection et une estimation rapide, précise et exacte de l'orientation des instruments dans l'espace ;
- Une interface utilisateur ergonomique et intuitive pour une utilisation facile du produit et un affichage adapté des valeurs angulaires.

Le logiciel KneePlus doit être accompagné des instruments KneeTools pour fonctionner. Ces instruments spécifiques intègrent des marqueurs qui permettent au logiciel de les détecter dans l'espace. Les instruments sont le pointeur, la référence de l'os, le mécanisme d'orientation, l'adaptateur de guide de coupe.

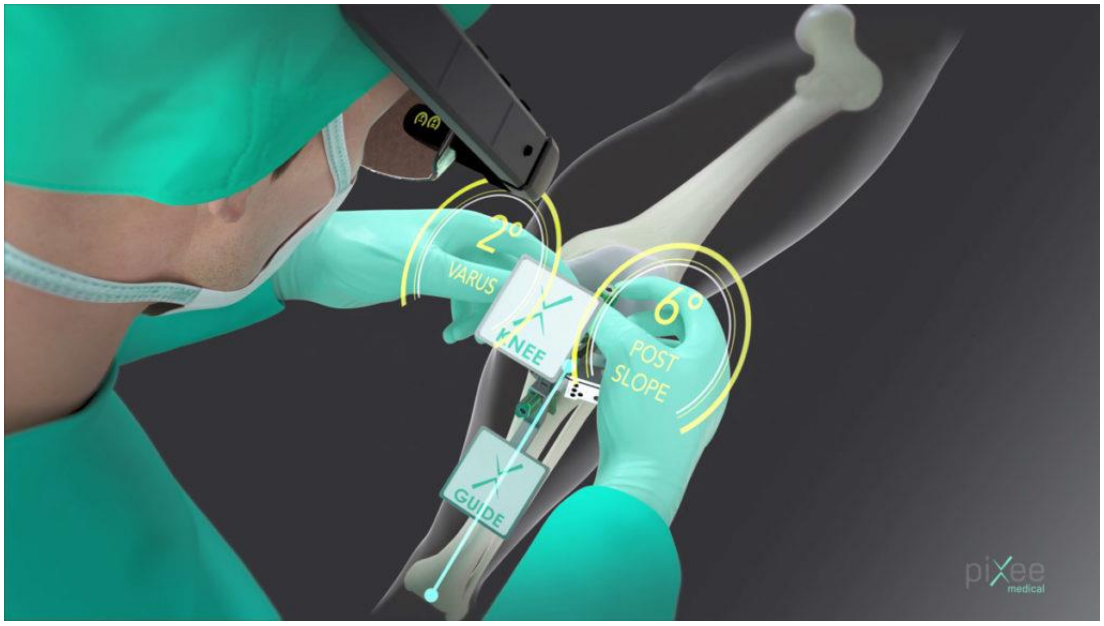

Figure 1 : Navigation en réalité augmentée pour l'arthroplastie total genou (Source [3])

D.2- Le système de planification Shoulder

Le système Shoulder est utilisé dans le processus d'arthroplastie totale de l'épaule ou l'arthroplastie totale inversée de l'épaule. Il est utilisé dans la phase préopératoire pour étudier le système d'articulation de l'épaule, dimensionner les parties usées et simuler l'imbrication durant une opération virtuelle effectuée par un spécialiste. Les parties usées sont remplacées par des implants artificiels afin de réduire la douleur et de restaurer l'amplitude de rotation et la mobilité. Lors de la mise en place d'une prothèse d'épaule, la qualité de l'implant et la précision de l'acte chirurgical sont très critiques. L'évaluation du succès de la chirurgie se fait sur la restauration de la mobilité du patient et la disparition de la douleur.

Cette solution médicale est prévue pour la planification préopératoire du remplacement primaire de l'épaule à partir d'images CT. Elle comprend une base de données sécurisée permettant d'accéder à l'interface de planification et de gérer les cas des patients.

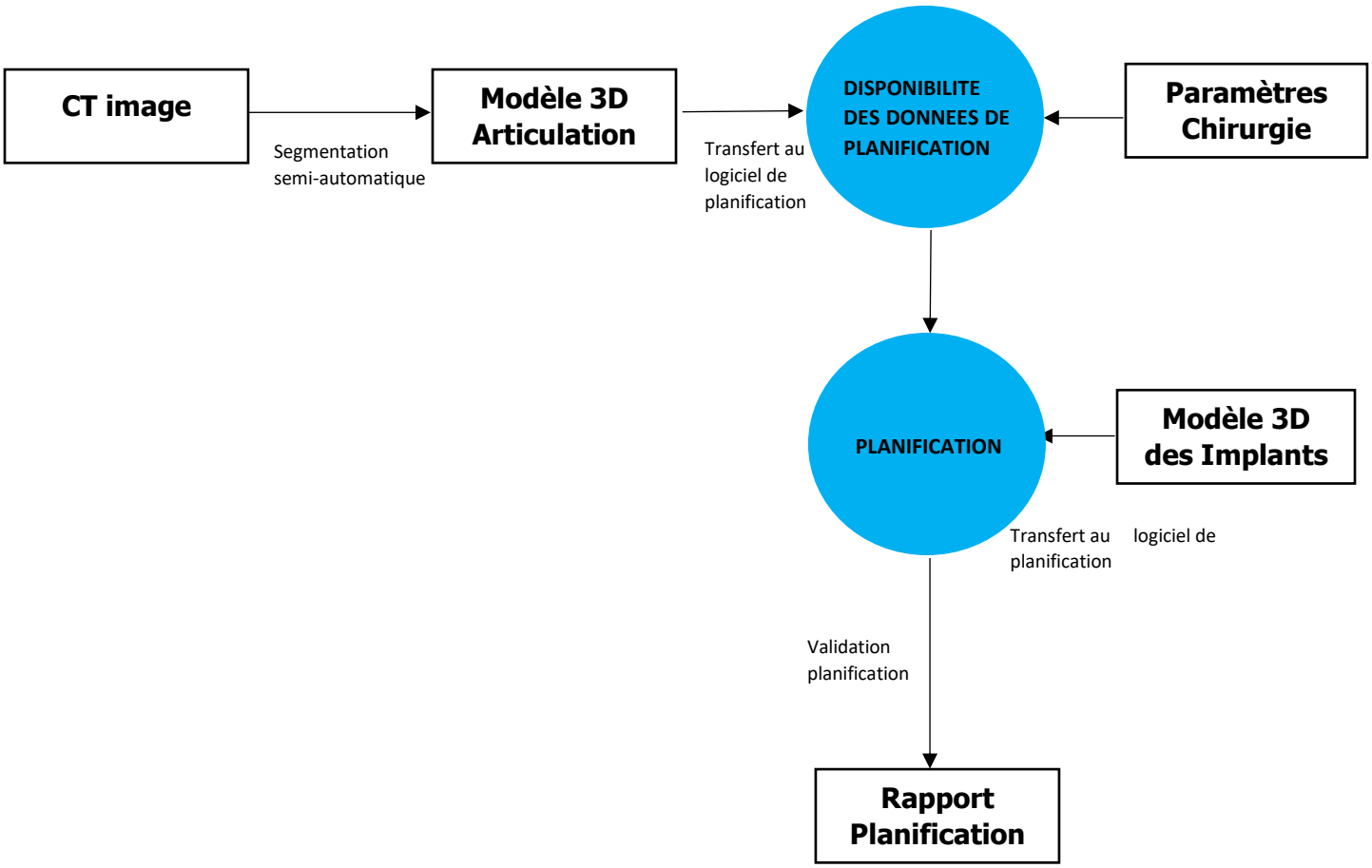

Figure 2: Synoptique général du processus de planification de la hanche (source : auteur)

II. Projet de remise en conformité d'une solution médicale

A- Contexte et Enjeux

L'entreprise Pixee médical obtient en 2018 la certification ISO 13485 version 2016 pour son système de management de la qualité. Une année plus tard, le premier dispositif développé par la société acquiert le marquage CE. Ce dispositif est un système composé des instruments chirurgicaux réutilisables et un logiciel considéré comme un dispositif médical installé sur une plateforme d'exécution qualifiée (système de navigation KneePlus §I.D.1). Pendant le développement de cette première version, tous les périphériques internes à la plateforme d'exécution susceptibles d'établir une connexion informatique avec un périphérique externe sont désactivés (Bluetooth, NFS, Wifi). Cette spécification provient des mesures de maitrise de risque de cybersécurité, établies pour prévenir et réduire autant que possible, les risques d'intrusions non autorisés qui peuvent provoquer les dénis de service. Avec cette mesure le dispositif est à l'abri des vulnérabilités. Jusqu'à lors, les données de navigation sont projetées sur le champ opératoire de la salle de chirurgie en utilisant l'affichage holographique de la plateforme d'exécution.

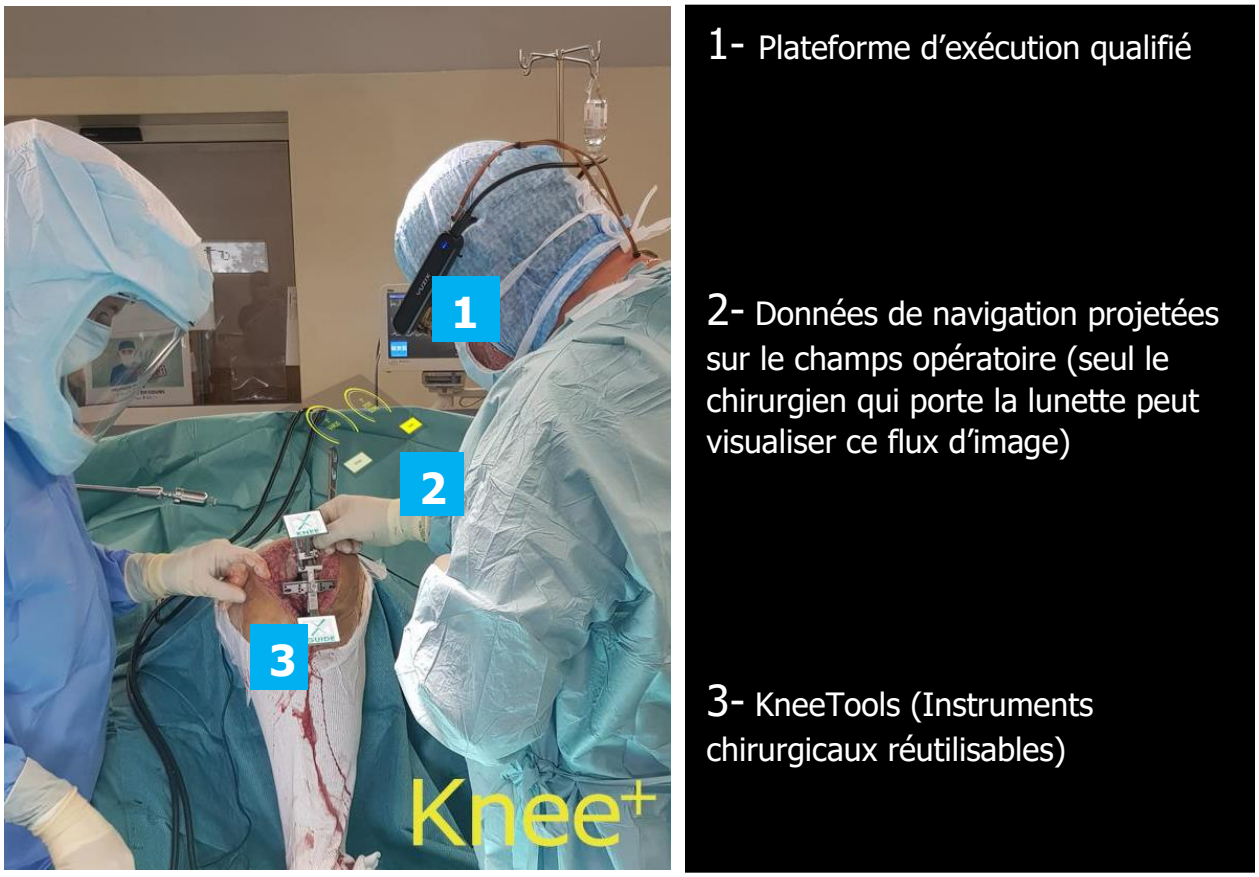

Figure 3 : Système de navigation du genou de la société Pixee Medical (Source[4])

Après la mise sur le marché européen, la société décide en Septembre 2020 de s'attaquer au marché Américain. La FDA « *Food and Drugs Administration* » est l'organisme gouvernemental Américain responsable de la protection de la santé publique. C'est l'entité responsable de réglementer la fabrication, la commercialisation et la distribution des dispositifs médicaux sur le territoire Américain[5]. La première soumission de la documentation technique envoyée à la FDA avec les mêmes caractéristiques que celui envoyé à l'organisme notifié en charge du marquage CE revient avec des interrogations sur le management de la cybersécurité du dispositif. Dès lors, l'entreprise trouve la nécessité de mettre en place un SMQ de sa cybersécurité. Mais cela n'empêche que La Start Up réussit à démontrer que les dispositions prises plus haut (Désactiver toutes les connexions), permettent de placer le logiciel hors de portée des menaces de cybersécurité.

Quelques mois plus tard, une nouvelle spécification va être ajoutée au cahier de charge marketing puis traduit en spécification fonctionnelle. C'est celle de donner la possibilité au système de dupliquer l'affichage des données de navigation sur un second écran sans fil. Cette nouvelle fonctionnalité impose à la plateforme l'utilisation du composant WIFI pour établir la connexion avec l'écran secondaire. Cela va plonger le système dans un réseau informatique et le rendre plus vulnérable aux attaques extérieures. Pixee Médical va également lancer le développement d'un second produit, Shoulder qui nécessite être connecté à internet pour parvenir à son utilisation prévue. Ces deux facteurs vont pousser la structure à intégrer la gestion de la cybersécurité dans le cycle de vie de leurs dispositifs médicaux.

B. Problématique et objet du stage

Le logiciel KneePlus est le premier produit mis sur le marché par Pixee Medical. Il a été mis sur le marché en Janvier 2021. Les chirurgiens orthopédiques avant l'utilisation du système doivent être au préalable formé par des ingénieurs d'application. Durant la formation seul le chirurgien orthopédique qui porte la lunette de réalité augmentée a une vue de l'écran de navigation et ses différents paramètres (paramètres de coupe, indications et contre-indications, messages d'erreur). Des réclamations sont alors remontées à ce sujet par l'équipe commerciale. Ces réclamations concernent pour la plupart la durée de formation de plus en plus longue, la qualité de la formation qui ne produit pas les résultats escomptés et l'engouement des chirurgiens qui diminue à cause des redondances pendant la formation. La première solution trouvée à ce problème est celle d'optimiser les process de formation. Une fois la formation des chirurgiens terminée, les opérations sur le genou vont être effectuées avec le système de navigation KneePlus ; Pendant les chirurgies, le problème ressurgit. Les ingénieurs d'application censés accompagner le chirurgien n'ont aucune visibilité sur les manipulations et la vision du chirurgien. L'impact de l'accompagnement des ingénieurs d'application est alors très réduit, puisqu'il est proscrit d'interchanger la plateforme d'exécution, entre le chirurgien et l'ingénieur d'application pendant un acte chirurgical. En cas de non-respect de cette mesure la stérilité du champ opératoire n'est plus garantie. Après une analyse de la réclamation sur ce

problème par une équipe pluridisciplinaire, une demande de modification va être introduite et valider pour ajouter une nouvelle fonctionnalité au système. C'est celle de dupliquer la vue du chirurgien sur un second écran pour permettre aux ingénieurs d'application et à l'équipe médicale de suivre également l'acte chirurgical en temps réel. Cette nouvelle fonction va rendre le système vulnérable aux attaques informatiques. D'où la nécessité aujourd'hui de sécuriser le système par des moyens de conception et développement ; Puis démontrer aux autorités compétentes que toutes les mesures ont été prises pour assurer la fiabilité et la sureté du système.

III. Processus de maitrise réglementaire

A. Démarche Opérationnelle

La roue de Deming est utilisée comme l'élément principal durant l'exécution des missions de stage. Elle permet de mieux appréhender le problème et d'améliorer continuellement le résultat. Cette méthode a été utilisée dans la version CAPD définie comme suit : **Check** (Vérifier), **Act** (agir), **Plan** (Planifier) ensuite **DO** (faire).

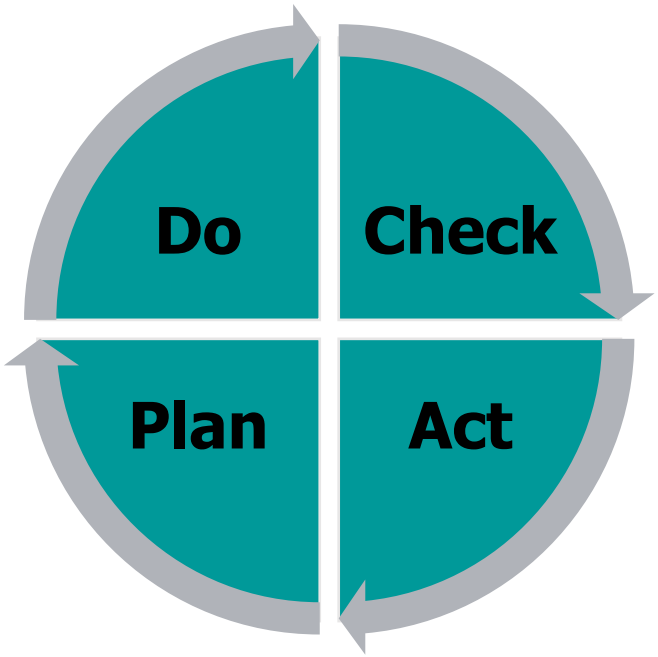

Figure 4 : Cycle d'amélioration continu (source : Auteur inspiré de [6])

- **Check : Vérifier**

  Cette partie marque le début des travaux, elle permet de prendre connaissance et analyser la documentation existante de toute l'entreprise. Elle débute par la revue de La documentation du système de management de la qualité de la Start up ; rédigée et documentée principalement par rapport à la norme ISO 13 485[7]. Puis consolider de manière progressive avec les exigences du 21 CFR parts 820[8]. Une attention particulière a été faite sur les éléments suivants :

  - Le manuel qualité : Il permet d'avoir une vue globale sur la gestion de la qualité de l'entreprise. L'origine, les missions, l'organigramme et les activités de la société sont décrites ;
  - Les principaux processus : Ils permettent de comprendre les objectifs et la finalité des différentes activités de la société ;
  - Les procédures de conception et développement (mécanique et informatique) ;

- La procédure de gestion des documents et des enregistrements : Elles permettent de comprendre comment rédiger, référencier et enregistrer un nouveau document avant de le sauvegarder dans le réseau ;
- Quelques instructions (Utilisation la gestion électronique des documents, consultation des sources de veille et la gestion des idées et suggestions d'amélioration) : Elles permettent de connaitre comment utiliser l'application destinée à la gestion de la documentation électronique. Elles permettent également de participer activement au cycle de veille réglementaire, de soumettre ou d'apporter des idées d'amélioration à la société…

La documentation technique notamment la description de l'appareil, l'utilisation prévue et la documentation d'accompagnement permettent de mieux comprendre les dispositifs médicaux conçus, développés et commercialisés par la société.

- **Act : Agir**

Une fois l'analyse préliminaire terminée, plusieurs rencontres sont planifiées avec l'équipe projet. Cela inclut, des rencontres et des échanges répétés avec Le Directeur de la recherche et du développement, le responsable qualité et affaires réglementaires, Le program manager, les chefs de projet, les ingénieurs affaires réglementaires et les développeurs. Une de ces entrevues permet de poser les premières bases des travaux à effectuer pour satisfaire aux exigences de sécurité informatique et de présenter le retroplanning des activités. Elle permet également de partager les rôles et les responsabilités dans le processus de conformité ou de récupérer un premier avis des différents membres de l'équipe projet, afin d'améliorer l'ébauche de retroplanning élaboré.

Durant cette phase les discussions sur les sociétés de prestation de service de cybersécurité avec lesquelles l'équipe souhaite travailler est également au programme. Cela permet de faire une sélection ou pas en se basant sur des critères bien précis comme :

- La compétence et la complémentarité de la société de consulting avec celle de l'équipe en place ;
- Les couts de la prestation ;
- La capacité à interagir et la promptitude dans les échanges ;
- La mobilité de la société de conseil ;
- Les références et l'expérience.

- **Plan : Planifier**

Dans cette phase la roadmap du projet est établie. Toutes les activités sont répertoriées dans un rétroplanning définitif mais ajustable en fonction des alinéas de la démarche. Chaque activité doit avoir un pilote, une date line, les différentes sous activités. Le rétroplanning doit contenir les activités qui permettent la prise en main des référentiels tels que le nouveau règlement européen 2017/745[1], le Content Premarket Submissions for Management of Cybersecurity in Medical

Devices and [9], Postmarket Management of Cybersecurity in Medical Devices[10], Les standards du laboratoire UL (Software Cybersecurity for Network-Connectable Products, Part1: General Requirements [2] and Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems[11]), les guides européens comme le MDCG 2019 – 16[12]. Une fois les standards revus, il faut tirer toutes les exigences et les recommandations de cybersécurité ; répondre à ces exigences et les documenter.

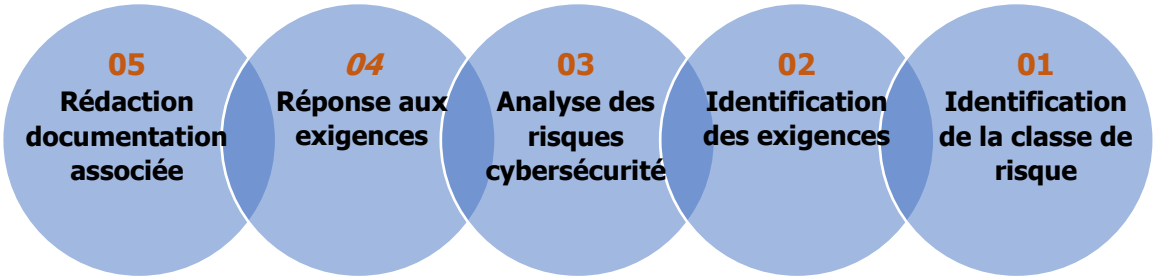

Figure 5 : Macro retroplanning des activités de stage (Source : Auteur)

B. Environnement règlementaire

Le NIST (National Institut of Standard and Technology) donne aux fabricants les bases de la conception et du développement de la sécurité informatique des dispositifs médicaux. Il s'agit essentiellement de concevoir un appareil capable de[9] :

- Identifier les attaques et les menaces.
- Protéger le système contre les dénis de service.
- Détecter les intrusions.
- Répondre en cas d'attaque.
- Récupérer ses capacités ou les services altérés.

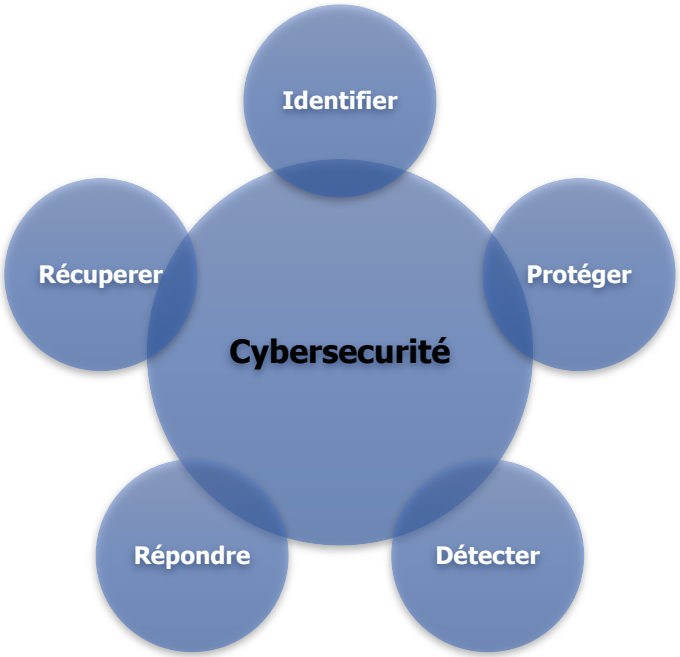

Figure 6 : Cycle des fonctions de base de cybersécurité(Source[9])

Pour mener à bien la définition et les spécifications des fonctions de base, il est capital voir indispensable de caractériser les différents constituants du système. Pour cela il faut effectuer le CBOM (Cybersecurity bills Of Materials) ou le SBOM (Software Bills Of Materials). Ils fournissent une liste descriptible de toutes les composantes, les sous composantes et les unités logicielles du système ; y compris les logiciels tiers et open source (OTS, SOUP…).

Le processus de conception prend également comme entrées les aspects règlementaires, qui viennent ici cadrer le cycle de vie des produits. C'est pour cette raison qu'il est important d'identifier toutes les spécifications règlementaires et de les croiser aux spécifications techniques.

1. Identification de la classe de sécurité du dispositif médical

Les dispositifs médicaux sont classés en fonction de l'usage auxquels ils sont destinés et des dommages potentiels qu'ils peuvent poser pendant leurs utilisations prévues. Globalement les autorités réglementaires de chaque territoire (USA, Europe, Australie, Corée…) utilisent les mêmes règles de classification, chacun

avec des spécifications propres à sa région. Les dispositifs sont classés de la classe I à la classe III en passant par les classes IIa et IIb. La classe I présente les appareils avec le risque le plus faible. La classe III comprend les dispositifs avec le risque le plus élevé.

- **Classification européenne**

Jusqu'au 26 Mai 2021, les fabricants de dispositifs médicaux peuvent au choix classer leurs produits selon la directive ou le nouveau règlement dans la procédure de marquage CE. Après cette date les fabricants de DM devront enregistrer leurs produits uniquement suivant le nouveau règlement européen 2017/745 ou 2017/746.

Directive 93/42/CEE

La directive 93/42/CEE du 14 Juin 1993 relative aux dispositifs médicaux donne en son annexe 9 les règles d'application et de classification des différentes classes de dispositifs médicaux. Les critères utilisés pour déterminer la classe de risque dépendent des facteurs comme : le temps, le caractère invasif ou non du dispositif, le caractère actif ou non du dispositif…

Le logiciel de navigation est destiné à être utilisé avec un kit d'instrument, mais vu que les règles de classification s'appliquent séparément, la classe du logiciel n'influence pas sur celui des instruments et vice versa.

Le tableau suivant établit une correspondance entre les règles de classification et les caractéristiques du logiciel considéré comme un dispositif médical. Le signe « **–** » signifie que le dispositif ne respecte pas la règle mentionnée et le signe « **+** » signifie le contraire. La dernière colonne renseigne sur la classe la plus élevée correspondant à une règle respectée.

Dispositif non- invasif	Règle 1	Règle 2	Règle 3	Règle 4		Classe
+/-	+	-	-	-		Classe I
Dispositif Invasif	Règle 5	Règle 6	Règle 7	Règle 8		Classe
+/-	Non- Appliqué					Non-Appliqué
Autres règles appliquées au DM actifs	Règle 9	Règle 10	Règle 11	Règle 12		Classe
+/-	-	-	-	+		Classe I
Règle spéciale	Règle 13	Règle 14	Règle 15	Règle 16	Règle 17	Classe
+/-	-	-	-	-	-	Non-Appliqué

Tableau 1 : Tableau de correspondance entre les grands groupes de classification et les règles associés (source : Auteur inspiré de [13])

En application des règles de classification de la directive qui stipulent au paragraphe §2.5 de l'annexe 9 que, si plusieurs règles s'appliquent au même dispositif du fait des utilisations indiquées par le fabricant, la règle qui s'applique est la plus stricte, le dispositif étant classé dans la classe la plus élevée[13].

Pour le cas de Pixee Medical, le logiciel est utilisé de façon continue pendant son utilisation prévue sur une durée de moins de 30 jours ; c'est un dispositif médical actif qui respecte la règle 12 : Il est donc un dispositif de classe I selon la directive 93/42/CEE. Puisque le système permet de mesurer les références anatomiques d'un patient, et que le bénéfice clinique revendiqué implique une précision de la mesure ; et une non-conformité de la mesure pourrait entrainer un effet négatif sur la santé du patient alors à la classe I du dispositif va s'ajouter la fonction de mesurage (Im).

Règlement (UE) 2017/745 du parlement européen et du conseil

Le règlement (UE) 2017/745 du parlement européen et du conseil du 5 avril 2017 donne en annexe 8 Les nouvelles règles d'application et de classification des dispositifs médicaux. Contrairement à la directive 93/42/CEE, les logiciels considérés comme Dispositifs médicaux sont pris en compte et mieux détaillés dans cette classification.

La classification dépend toujours de la durée d'utilisation, du caractère invasif ou actif du dispositif. Comme dans la directive, la classe de sécurité des appareils en association avec un dispositif n'influe pas sur la classe de celui-ci.

Le tableau suivant établit une correspondance entre les règles de classification et les caractéristiques du logiciel médical considéré comme un dispositif médical. Le signe « **–** » signifie que le dispositif ne respecte pas la règle mentionnée et le signe « **+** » signifie le contraire. La dernière colonne renseigne sur la classe la plus élevée correspondant à une règle respectée.

Dispositifs non invasifs	R1	R2	R3	R4						Classe
+/-	+	-	-	-						Classe I
Dispositifs invasifs	R5	R6	R7	R8						Classe
+/-	Non - Appliqué									Non- Appliqué
Dispositifs actifs	R9	R10	R11	R12	R13					Classe
+/-	-	-	+	-	-					Classe IIa
Règles particulières	R14	R15	R16	R17	R18	R19	R20	R21	R22	Classe
+/-	-	-	-	-	-	-	-	-	-	

Tableau 2 : Tableau de correspondance entre les grands groupes de classification et les règles associés (source : Auteur inspiré de[1])

En application des règles de classification du règlement qui stipule dans son point §3.5 du chapitre II de l'annexe 9 : **Le logiciel est clairement identifié comme un dispositif médical de classe IIa.**

- ## Classification Australienne

Pour la classification des dispositifs médicaux, la TGA, l'autorité de règlementation australienne des produits thérapeutiques a développé un outil d'aide qui permet de déterminer la classe de risque d'un dispositif médical en répondant de manière interactive à des questions. La première étape consiste à prédéterminer le groupe auquel appartient le dispositif médical. Les groupes vont de A à E, avec un dernier groupe qui rassemble tous les dispositifs dont les caractéristiques ne correspondent à aucun des groupes. Ensuite, l'outil pose une multitude de question qui permet à la fin de déterminer la classe du dispositif. Cet outil est consultable sur le site internet de la TGA à l'adresse suivante : *https://www.tga.gov.au/sme-assist/interactive-decision-tools*

Scénario de sélection de classe à risque du logiciel de navigation

1- Choisir la branche qui correspond au dispositif médical (Voir les descriptions en annexe)

GROUPE A | **GROUPE B** | **GROUPE C** | **GROUPE D** | **GROUPE E** | **AUTRES**

2- C'est un dispositif invasif ou non-invasif ?

Non-Invasif | **Invasif**

3- En fonction de l'utilisation prévue de votre dispositif non invasif, quelle est sa catégorie ?

Contact avec la peau | **Gère les substances** | **Autres**

4- Votre dispositif médical non invasif est fourni stérile ?

Oui | **Non**

5- Le dispositif médical a t-il une fonction de mesurage ?

Oui | **Non**

6- Est-ce un dispositif médical actif ?

Oui | **Non**

7- Le dispositif est-il un DMIA

Oui | **Non**

8- C'est un logiciel médical actif, programmé ou programmable ?

Oui | **Non**

9- Le dispositif est-il destiné à fournir des informations uniquement à un professionnel de la santé concerné ?

Oui | **Non**

10- Le dispositif fourni des informations pour poser un diagnostic sur une maladie ou pathologie ?

Entrainer la mort | **Détérioration sévère** | **Progression** | **Autres**

Sur la base des sélections effectuées, la classification du logiciel est de Classe Im selon la règlementation australienne.

Les dispositifs de classe Im sont considérés comme présentant un risque moindre. Ils doivent faire l'objet d'une certification d'évaluation de la conformité de la part de leur fabricant avant de pouvoir être inscrits dans le registre australien des produits thérapeutiques. Cette certification peut être fournie par la TGA ou par un organisme notifié européen.

- **Classification Américaine**

Contrairement à la réglementation (UE) européenne et même Australienne, la FDA aux Etats-Unis n'utilise pas d'algorithme basé sur une série de questions pour déterminer la classe des dispositifs médicaux. Une classification est établie pour un groupe de 1700 types génériques d'appareils regroupés en 16 spécialités médicales[14]. Les appareils de classe I et II peuvent être exemptés de contrôle généraux et contrôles spéciaux, sinon un dossier pour le marquage 510k sera requis pour la commercialisation. Les dispositifs de classe III doivent obligatoirement passer par une approbation préalable à la mise sur le marché sur le territoire américain. Pour déterminer donc la classe de risque des dispositifs médicaux, il faut au préalable trouver le numéro de règlement ; deux possibilités s'offrent pour y arriver :

- Rechercher une partie du nom de l'appareil, ou le panneau de l'appareil. Le nom et le panneau des appareils classés par la FDA se retrouve dans le 21 CFR Parts 862-892.
- Ensuite, lancer la base de données de classification à l'adresse suivante : https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpcd/classification.cfm

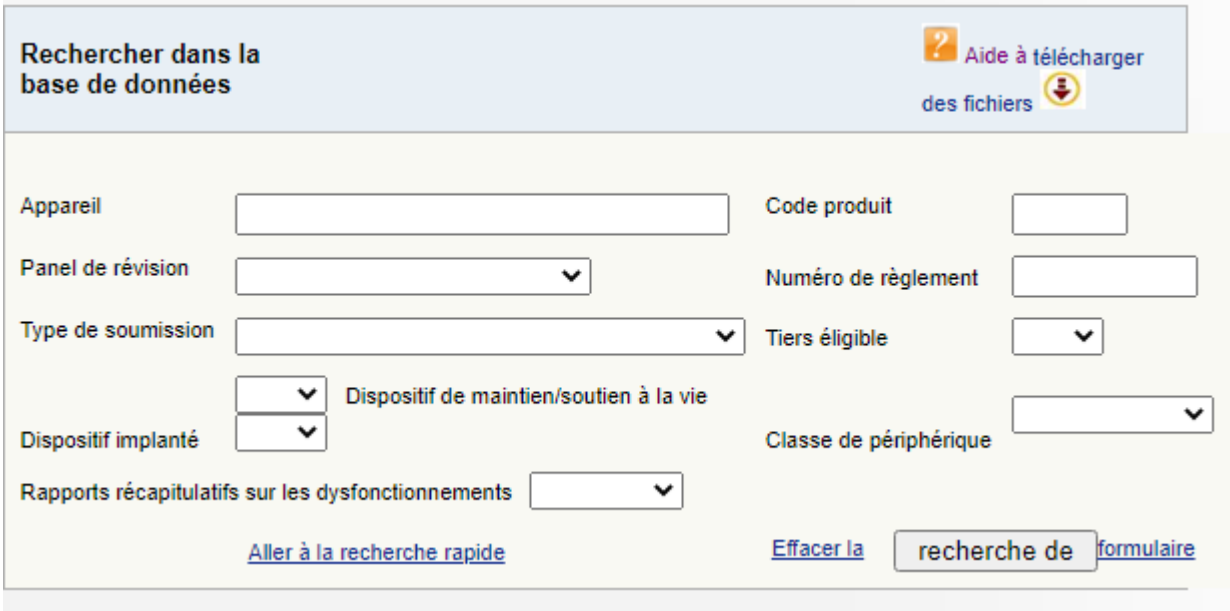

Figure 7 : Informations nécessaires à la recherche de la classe d'un DM selon la FDA (source :[15])

- Cliquer sur recherche une fois les informations entrées
- Puis identifier/choisir l'appareil et la réglementation associée

Ou passer par une classification officielle par la FDA, dans ce cas il faut soumettre une demande 513(g).

Contrairement à l'enregistrement effectué en Europe où le logiciel était enregistré séparément de ses accessoires, aux Etats unis le logiciel et ses accessoires mécaniques sont enregistrés comme un seul système. La première approche a dont été utilisée pour déterminer la classe de risque du système. Le tableau suivant recapitule toutes les informations obtenues de la classification avec l'outil proposé par la FDA.

Appareil	Instrument Stéréotaxique Orthopédique
Description du règlement	Instrument stéréotaxique.
Définition	Guidage stéréotaxique lors des interventions de chirurgie orthopédique. Indiqué pour la chirurgie orthopédique des articulations ou de la colonne vertébrale. Les instruments stéréotaxiques neurologiques sont classés sous le code produit HAW.
État physique	L'appareil se compose d'une caméra, d'un ordinateur, de divers réseaux de suivi de forme, d'une interface informatique pour la communication entre l'utilisateur et l'appareil.
Méthode technique	L'utilisateur charge le logiciel préopératoire pour planifier la procédure chirurgicale, puis enregistre l'anatomie du patient pendant la chirurgie pour permettre au logiciel de suivre l'anatomie du patient, les implants et les outils chirurgicaux en temps/espace réel.
Zone cible	Articulations orthopédiques et procédures vertébrales où le suivi de l'instrumentation est souhaité.
Réglementation Spécialité Médicale	Neurologie
Panel de révision	Orthopédique
Code produit	OLO
Examen précommercialisassions	Appareils orthopédiques (OHT6) Appareils Stéréotaxiques, traumatologiques et de restauration (DHT6C)
Type de soumission	510(k)

Numéro de règlement	882.4560
Classe du système	**II**
Cycle de vie total du produit (TPLC)	Rapport de code de produit TPLC
Exemption des BPF ?	Non
Rapport de dysfonctionnement récapitulatif	Éligible
Dispositif implanté ?	Non
Dispositif de maintien/soutien à la vie ?	Non
Norme de consensus reconnue	11-350 ASTM F2554-18 : Pratique standard pour la mesure de la précision de position des systèmes chirurgicaux assistés par ordinateur
Examen par un tiers	Non éligible à un tiers

Tableau 3 :Informations accompagnant la classe de risque des DM aux Etats unis (source : Auteur inspiré de[15])

Il en ressort que **le système est catégorisé comme un DM de classe II, Selon la règlementation Américaine**. Les autorités américaines ne s'arrêteront pas là. La sécurité informatique est aujourd'hui un réel problème pour les dispositifs médicaux, le nombre de cyberattaque est garantissant et se multiplie. Une nouvelle classe de risque va être initialisée dans le guide d'accompagnants des fabricants dans le processus de réponses aux exigences de cybersécurité: C'est le « tiers (*cybersecurity Risk for medical devise*) » [9]. Il a été mis sur pied pour proportionner les efforts des fabricants en fonction des risques dans le processus de conformité aux exigences règlementaires de cybersécurité. Il classe les appareils et les logiciels en deux niveaux :

- **Le Tiers 1 « Higher cybersecurity risk »** : ce sont des dispositifs médicaux capables de se connecter par réseau filaire (RJ45, USB…), sans fil (Wifi, Bluetooth, NFS…) ou internet à d'autres dispositifs médicaux ou des systèmes non médicaux. Et donc, un incident de cybersécurité sur le dispositif médical peut entrainer un préjudice sur le patient ou son environnement. Un défibrillateur cardiaque implantable est considéré par exemple comme un dispositif médical de tiers 1.
- **Le Tiers 2 « Standard cybersecurity risk »** : Tous les dispositifs médicaux qui ne respectent pas les règles du tiers 1 sont classés comme les DM avec les risques standards.

Cette classification permet de mettre plus ou moins d'accent dans la documentation technique liée à la cybersécurité. Il existe des dispositifs médicaux de classe de risque III (stent coronaire) qui sont des Tiers 2 et des dispositifs de classe II tel qu'une pompe à infusion qui sont des Tiers 1.

Une fois le dispositif médical ou le système classé (Classe de sécurité et Tiers), les fabricants peuvent passer à l'identification des exigences de cybersécurité qui sont fortement liées à la classe de risque du dispositif et du tiers.

2. Exigences générales en matière de cybersécurité, Synthèse des standards UE, TGA et USA.

Pixee Medical commercialise ses dispositifs médicaux en Europe et même à l'international. Cela implique que, l'identification des exigences règlementaires applicables aux produits en matière de cybersécurité devra prendre en compte tous ces territoires. En Europe le nouveau règlement UE 2017/745 en son annexe 1 dans la section 17.2 rappelle que, les fabricants doivent développer les logiciels qui garantissent la sécurité de l'information durant le cycle de vie du produit[1]. C'est pour cette raison que le Medical Devices Coordination Group (MDCG) a publié le MDCG-16 V2019 qui reprend, analyse et détaille toutes les exigences/recommandations du règlement. Aux Etats unis, la FDA a mis sur pied deux guides à vocation d'aider les entreprises dans les activités de conformité. Le premier standard met en évidence les

attentes et le contenu du dossier de soumission pour l'approbation de la mise sur le marché[9]. Et le second initie et s'inscrit dans un processus d'amélioration continue des activités que prône l'ISO 13485 dans la version de 2016 ; il traite également toutes les activités de la surveillance après commercialisation[10]. Le laboratoire UL développe les standards qui prennent en considération les exigences Américaines, Canadiennes et Australiennes. Cependant, ils fournissent en plus aux déclarants/fabricants les recommandations sur les tests de reproductibilités, ils couvrent les tests de vulnérabilités, les logiciels malveillants et les faiblesses logicielles pour les Devices en réseau. La conformité aux exigences de la norme UL2900-1 fait la présomption de conformité aux Etats-Unis[16].

Toutes ces raisons permettent de prendre les normes de cybersécurité développées par le laboratoire UL comme le squelette sur lequel viendront se greffer les autres standards durant tout le cycle de vie des produits. Il s'agit notamment de l'UL 2900-1[2] et L-UL2900-2-1[11] qui traite respectivement la cybersécurité des logiciels pour les produits connectables[2] et les exigences particulières pour les composants connectables au réseau des systèmes de santé et de bien-être. Pendant les activités de stage, Deux supports d'enregistrements sont élaborés :

- Un document qui répertorie avec une référence toutes les exigences de cybersécurité issues des précédents standards, donne la provenance de l'exigence, ce qui permet pendant l'enregistrement en cas de doute ou de non compréhension de savoir où creuser davantage. Ce support contient également une colonne qui permet de définir si l'exigence est applicable ou pas. Ensuite une seconde partie permet de mettre en évidence et de donner le/les moyen(s) utilisé(s) pour se conformer à l'exigence (l'utilisation d'un nouveau standard, la mise à jour du dossier de conception ou de la documentation technique comme les spécifications fonctionnelles et techniques ou la rédaction de la CBOM…). La dernière colonne permet d'identifier la preuve de conformité par un nom et une caractéristique (Standard, Procédure, Instruction ou enregistrement).

pixee medical — Cybersecurity essential recommendations — KneePlus v1.3 — Form: ENR-CED-CERE index 1

Id	Cybersecurity Essential Recommendations	Standard references	Applicable / Non-applicable (A/NA)	Measures taken to answer to the requirement (standard, procedure applied…) or rationale for non-applicability	Records / Evidences
L1	Design the Device to Recover capabilities or services that were impaired due to a cybersecurity incident.	**FDA Premarket:** 3 **Health Canada:** 2.1.1 Table 1, Line 6	A	Specify this constraint in the technical specifications.	**[R01]** Technical specifications
L2	Implement design features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use.	**FDA Premarket:** V.B.1.a **Health Canada:** 2.1.1 Table 1, Line 6	A	Specify this constraint in the technical specifications.	**[R01]** Technical specifications
L3	Devices should be designed to permit routine security and antivirus scanning such that the safety and essential performance of the device is not impacted.	**FDA Premarket:** V.B.1.b	A	Specify this constraint in the technical specifications.	**[R01]** Technical specifications

Figure 8 : Enregistrement des recommandations essentielles de cybersécurité (Source : Auteur)

- Le second support est une annexe qui donne plus d'explications sur le principal support. On retrouve trois grandes parties :
- La référence complète des documents qui servent de preuve :

3. Records and evidences references

The following table lists the records and evidences to justify that the device meets the regulatory requirements.

Reference ID	Document name	Document reference	Document index	Comments
R01	Technical specifications	SW001-KNEE_PLUS-CDCT-001	10	
R02	Verification-technique	SW001-KNEE_PLUS-PTVT-001		
R03	Quick guide	SW001-KNEE_PLUS-DOAC-001	3	
R04	Standard operating procedure - Software Installation	SW001-KNEE_PLUS-SOPP-010	4	
R05	Tableau de configuration	SW001-KNEE_PLUS-TCFG-004	5	
R06	Software Safety Class	SW001-KNEE_PLUS-CDSL-001	5	
R07	Track Plus unitary test plan	SW001-KNEE_PLUS-PTST-016	1	
R08	Unitary-Tests-Plan	SW001-KNEE_PLUS-PTST-005	9	
R09	Test Plan Integration	SW001-KNEE_PLUS-PTST-004	10	
R10	Cybersecurity traceability matrix			
R11	Bill of materials			

Figure 9 : Liste des preuves documentaire créer ou mise à jour (Source : Auteur)

- Les éléments du système de management de la qualité :

4. QMS procedures and instructions references

The following table lists the QMS procedures and instructions followed to meet the regulatory requirements.

Reference ID	Document name	Document reference	Document index	Comments
Q01	Récupération des preuves médicaux légales	INS - instruction	1	
Q02	Gestion des vulnérabilités connues	PRD - Procedure	1	
Q03	Gestion des clés de chiffrement	INS - instruction	1	
Q04	Procédure de conception et développement informatique	PRD-CED-001	4	

Figure 10 : Amendement documentaire du SMQ(Source : Auteur)

- La liste des standards applicables : C'est le socle de toute la démarche de conformité.

5. Standard versions

The following table lists the standards followed to meet the regulatory requirements.

Reference ID	Document name	Document reference (including version or eventual amendment)	Comments
S01	Information security - Authenticated encryption	ISO/IEC 19772:2020	
S02	Information technology - Security techniques - Digital signature schemes giving message recovery	ISO/IEC 9796 (all parts)	
S03	IT Security techniques - Digital signatures with appendix	ISO/IEC 14888 (all parts)	
S04	Information technology - Security techniques - Cryptographic techniques based on elliptic curves	ISO/IEC 15946-1:2016	
S05	Information technology - Security techniques - Encryption algorithms	ISO/IEC 18033 (all parts)	
S06	Security Requirements for Cryptographic Modules	NIST FIPS 140-3:2019	
S07	Medical devices - Application of risk management to medical devices	NF EN ISO 14971: 2019	
S08	Principles for Medical Device Security - Risk Management	AAMI TIR 57: 2016	
S09	Medical device software - Software life cycle processes	IEC/ISO 62304:2015	
S10	IT Security techniques - Security techniques - Hash-functions	ISO/IEC 10118 (all parts)	

Figure 11 : Plan qualité de cybersécurité (Source : Auteur)

Les documents avec la référence marquée en jaune sont des documents qui n'existent pas dans le SMQ. La référence est attribuée au moment de la création.

Les exigences et recommandations de cybersécurité sont essentiellement basées sur :

- La documentation du produit, des processus et de l'utilisation prévue.
- Les contrôles de sécurité (sécurisé par la conception)

- La gestion des risques liés à la sécurité informatique
- Les tests de vulnérabilités, d'exploitation et de faiblesse
- L'organisation de la société

Une fois toutes les exigences et les recommandations répertoriées et analysées, la seconde étape est l'analyse des risques. C'est le point central de tout le processus, car elle permet de juger si une recommandation est nécessairement appliquée ou pas. Elle permet de définir le rapport de proportion entre les risques et les efforts fournis.

3. Analyse des risques de sécurité informatique du produit

Dans le processus de gestion des risques des dispositifs médicaux La norme NF EN ISO 14971 : 2019 est une référence. Elle spécifie une procédure pour permettre d'identifier les phénomènes et situation dangereuses, d'analyser et évaluer les risques, de maitriser et surveiller l'efficacité de ces moyens de maitrise[17]. C'est sur ce standard que repose la base du processus de gestion de risque au sein de Pixee Medical.

C'est une norme internationale qui traite tous les risques. Son caractère généraliste va la rendre moins adaptée pour les risques liés à une spécialisation bien spécifique. C'est pour cette raison qu'une multitude de standard ont été développés pour traiter de manière précise des thèmes particuliers, comme la cybersécurité et accompagner la 14971 dans cette procédure. Parmi les standards ou les méthodes développés pour traiter les vulnérabilités ou les menaces de cybersécurité nous avons :

- L'AAMI TIR 57 : Principes de sécurité des dispositifs médicaux – Gestion des risques
- La méthode EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité C'est une méthodologie simple proposé par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) conforme à la 27001. Elle permet d'analyser et traiter les menaces sur un produit ou une organisation.
- La CEI 80001-1 : Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux

La méthode EBIOS est la méthode choisie pour traiter les menaces et risques de sécurité informatique publiée par l'ANSSI (agence nationale de la sécurité et des systèmes d'informations). Elle synthétise plusieurs standards. La méthode a l'avantage d'être applicable à l'analyse des menaces de cybersécurité qui pèsent sur une organisation ou un produit. Elle s'articule autour de 5 grands axes.

- Le cadrage et socle de sécurité
- L'analyse des sources de risque
- La définition des scénarios stratégiques
- La mise en place des scénarios opérationnels
- Le traitement du risque

Le cadrage et socle de sécurité

Les principales activités de cette phase sont :

- Définir les objectifs de l'étude :
- Identifier les participants, le rôle et les responsabilités.
- Définir le cadre temporel du processus.
- Lister l'ensemble des missions.

- Ensuite recensez les évènements redoutés : Identifier et caractériser les évènements de sécurité redoutés au niveau de l'entreprise et ou du produit. Tous les évènements redoutés sont retrouvés suite à la réponse à la question <<Que craint-on qu'il arrive ?>> Pour chaque événement redouté, il faudrait établir les impacts et la gravité sur l'organisation/produit. L'échelle de la gravité des impacts se fait suivant la grille suivante :

Echelle	Conséquences
G 4-critique	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G 3-Grave	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G 2-Significative	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G 1-Mineure	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Tableau 4 : Echelle de définition du niveau de gravité des événements redoutés (Source : [18])

Tous les événements doivent être consignés dans un tableau. Ils seront ensuite utilisés comme donnée pour la suite de l'analyse. Les différentes phases sont : la conception (**CO**), le développement (**DEV**), la production (**PROD**), le transport(**T**), l'utilisation (**U**), la maintenance (**M**) et la mise au rebut (**MR**).

Phase	Evénements redoutés	Impacts	Gravités
U	Utilisation de la plateforme d'exécution qualifiée a d'autres fins que celle prévue par la société.	- Impact sur le contenu/ disponibilité des données ou des fichiers. - Impact sur l'alignement de la prothèse	1

Tableau 5 : Synthèse de la table support pour l'enregistrement des événements redoutés (Source : Auteur)

Une fois tous les événements listés, le socle est défini par l'identification des standards supplémentaires, l'état actuel d'application, les écarts connus et leurs justifications.

Analyse des sources de risque

Cette étape permet d'identifier dans un premier temps la liste de tous les couples SR (source de risque) /OV (objectif visé). Elle relie chaque source de risque à un ou plusieurs objectifs visés. Pour chaque couple identifié la pertinence (Faible, Moyenne, Elevée) est évaluée en fonction de la motivation, les ressources et les activités de la source. Ensuite chaque couple SR/OV est évalué pour développer une cartographie de menace numérique du système. Pour parfaire à bien cet atelier, les questions suivantes peuvent être posées :

- Quelles sont les sources de risque susceptibles de porter atteinte aux missions de l'organisation ou à des intérêts supérieurs (sectoriels, étatiques, etc.) ?

- Quels peuvent être les objectifs visés par chaque source de risque en termes d'effets recherchés ?

Source de risque	Objectifs visés
Cyber-terroriste	Altérer le code source du logiciel avant la release de l'application

Tableau 6 : Table support pour l'identification des couples SR/OV (Source : Auteur)

Définition des scénarios stratégiques

L'écosystème est un paramètre essentiel dans l'analyse préliminaire des risques de sécurité. Il permet de retrouver toutes les parties prenantes depuis la conception jusqu'a la mise au rebut du produit. Pendant les attaques, le mode opératoire est d'exploiter les vulnérabilités des maillons faibles de l'environnement. Sécuriser son écosystème contre les vecteurs d'attaques pertinents est la première mesure à prendre. Pour cela une cartographie numérique de l'écosystème est établie pour permettre d'identifier déjà toutes les parties prenantes avec lesquelles le produit interagit directement ou indirectement, et pour sélectionner les parties prenantes critiques. Pour déterminer le niveau de menace la formule suivante est adoptée et peut être ajustée en fonction de l'étude :

*Équation 1 : Niveau de menace = (Dépendance * Pénétration) / (Maturité * Confiance)*

Où la dépendance, la pénétration, la maturité et la confiance sont définis sur une échelle de 1 à 4 comme mentionné dans l'annexe 2.

Scénario : Une source de risque identifié plus haut tentera d'attaquer la partie prenante de l'écosystème identifiée comme élément faible de la chaine pour conduire aux évènements redoutés qui laisseront les impacts identifiés au meilleur des cas.

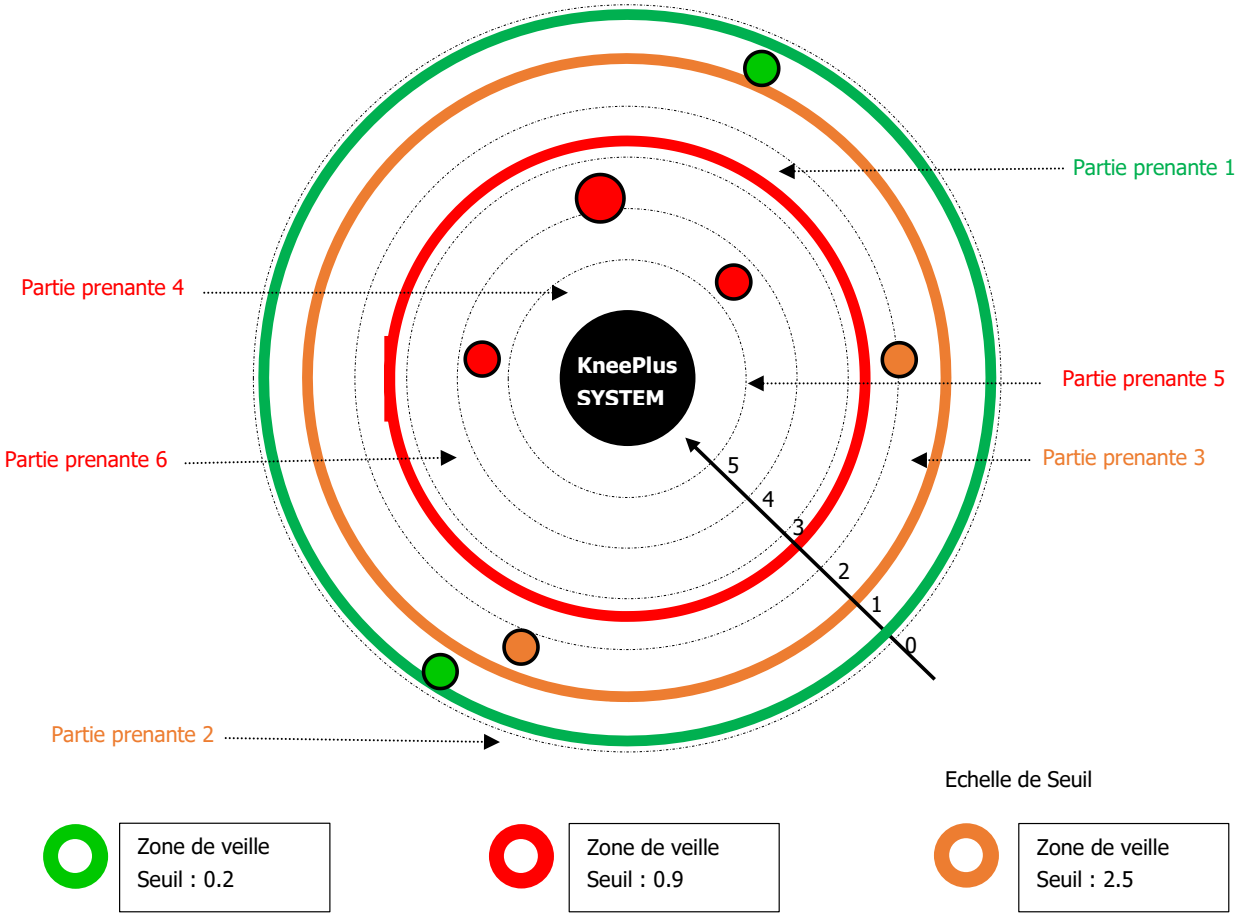

Figure 12 : Cartographie des menaces numérique d'un système (Source : Auteur inspiré de [18])

A partir des éléments précédemment établis (Evènement redoutés, Couple source de risque / objectif visé et la cartographie numérique) les scénarios stratégiques sont bâtis. Pour chaque couple source de risque/objectif visé jugé pertinent le(s) chemin(s) d'attaque(s) est/sont identifié(s) de manière stratégique est/sont détecté(s) à partir de la cartographie de menace numérique du système ; Puis la gravité de ce triplet est déterminée. Les résultats sont répertoriés dans la table suivante :

Source de risque	Objectifs visés	Chemin d'attaque stratégique	Gravité

Tableau 7 : Exemple de table support pour le triplet SR/OV et chemin d'attaque (Source : Auteur)

Mise en place des scénarios opérationnel et traitement des risques

Pour chacun des scénarios stratégiques précédemment établis, des scénarios stratégiques sont mis en place et structurés selon une séquence d'attaque. Ensuite, leur vraisemblance générale est évaluée, mais avant cela la vraisemblance élémentaire de chaque scénario est faite.

La vraisemblance dépend de la faisabilité ou de la probabilité de réussite d'une attaque. Elle est définie selon la grille suivante :

Echelle	Description
V 4- quasi certain	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G 3-très vraisemblable	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G 2- vraisemblable	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G 1-peu vraisemblable	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Tableau 8 : Echelle de vraisemblance des scénarios opérationnels(Source : Auteur inspiré de [18])

Lorsque les scénarios opérationnels sont définis, La synthèse de toute l'analyse est effectuée dans une matrice d'analyse des anomalies et des risques. Dans cette matrice on retrouve ;

- Le code de l'attaque : il permet d'identifier de manière unique une attaque
- La description de l'attaque
- L'évènement que peut apporter cette attaque
- Le préjudice ou l'impact porté au patient ou son environnement
- La vraisemblance de l'attaque
- La sévérité des dommages que porte la conséquence
- Le risque qui est une combinaison entre la vraisemblance de l'attaque et la sévérité de l'impact de cette attaque.
- Les mesures qui représentent toutes les actions mises en place pour réduire autant que possible la vraisemblance de l'attaque ou la sévérité de l'impact.
- Le code de la mesure qui représente l'identifiant unique attribué à chaque attaque afin de l'insérer dans la matrice de traçabilité.

Code	Description de l'attaques	Sources	Evènements	Impact	Vraisemblance	Sévérité	Risk	Mesures	Code mesure	Probabilité résiduelle	Sévérité résiduelle	Risque	Nouveaux évènements prédictibles
AT001													
AT002													
AT003													
AT004													
AT005													
AT006													

Tableau 9 : Matrice d'analyse des attaques et des risques de cybersécurité (Source : Auteur)

4. Mise en place des exigences règlementaires et rédaction de la documentation associée

L'ensemble des enregistrements rédigés durant sur cette procédure sont :

- L'analyse des risques de sécurité informatique

- La classification du dispositif médical en fonction des risques de cybersécurité

- la Cybersecurity Bills Of Materials (CBOM)

- **Les spécifications techniques (Design Secure) basées sur l'analyse des risques**

- Les plans de test avec les laboratoires externes

- L'enregistrement de l'organisme dans un ISAO

L'ISAO est une politique mise en place par les Etats Unis permettant aux fabricants de dispositifs médicaux de s'aider mutuellement entre eux en partageant chacun les vulnérabilités et les solutions entreprises pour pallier à ces attaques.

Inscrire La société comme un membre actif de L'ISAO (Information's Sharing and Analyzing Organization) en partageant les vulnérabilités, les menaces, les informations et les communications clients qui ont un impact sur ses propres dispositifs médicaux.

- **La surveillance**

C'est l'insertion dans le processus de surveillance après commercialisation, d'une procédure de gestion des vulnérabilités et des menaces qui permet d'analyser, d'évaluer et, si nécessaire, de déterminer des mesures de contrôle des risques ou de compensation pour les vulnérabilités identifiées, sur la base du système de surveillance établi dans le SMQ (système de management de la qualité de l'entreprise).

- Le plan périodique sur les activités de cybersécurité

L'entreprise doit rédiger un rapport périodique sur les événements de cybersécurité à l'origine d'un changement (chaque 3 ans) et le fournir aux autorités compétentes, en mentionnant la description de la vulnérabilité ou de la menace à l'origine du changement y compris la manière dont l'entreprise a pris connaissance de la vulnérabilité. Le rapport contient aussi un résumé des conclusions de l'évaluation des risques de l'entreprise, la description de(s) modifications apportées et la justification de(s) changements. De plus, la référence de chaque dispositif impacté doit être renseignée par son identifiant unique (UDI). Les communications et les informations échangées entre Pixee Medical, ses clients et ses fournisseurs sont également citées. Chaque vulnérabilité porte la date et le nom de ISAO dans lequel il a été signalé.

IV. Résultats Obtenus, Perspectives, Apport du stage et difficultés rencontrés

A- Résultats Obtenus

Au bout de 4 mois de stage le projet de mise en conformité de la société vis-à-vis des exigences de cybersécurité se déroule avec succès.

Afin d'évaluer l'avancement des missions axés sur la cybersécurité, Une autoévaluation a été faite le 22 juin 2021 pour avoir une idée claire du travail effectué.

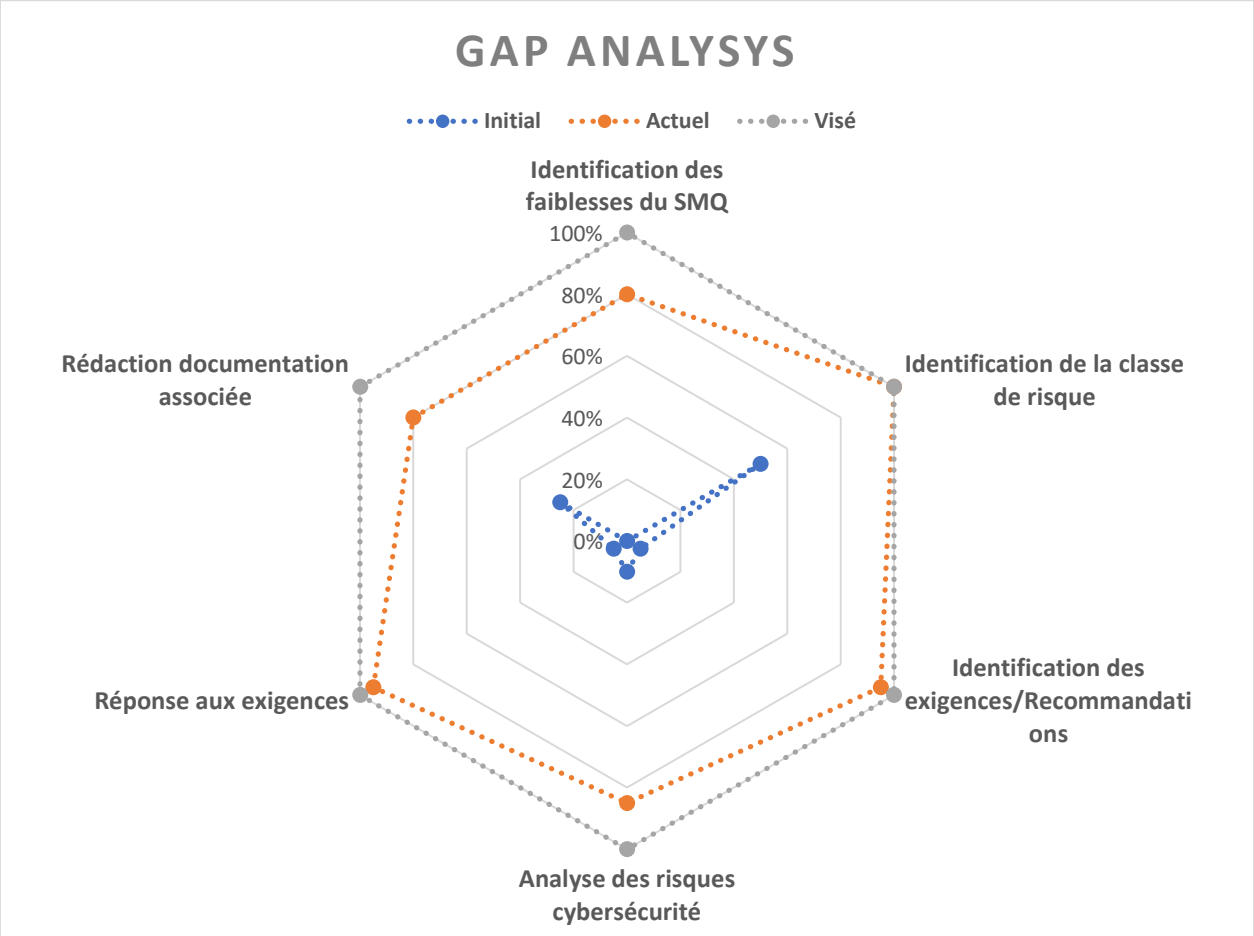

Figure 13 : Résultats des écarts entre l'état initial des travaux, l'état actuel et l'objectif visé (Source : Auteur)

Les résultats du diagramme montrent les évolutions et toutes les tâches réalisées en lien avec la cybersécurité. A cette date le pourcentage global d'avancement des taches est de 80%.

Notamment, il reste encore quelques actions à clôturer/réaliser sur :

- La procédure de gestion de la cybersécurité.
- Le rapport de cybersécurité.
- La définition des mesures de maitrise de risque de cybersécurité.

B- Perspectives

Une fois les process de cybersécurité totalement implantés au sein du système de management de la qualité de la société et la rédaction de la documentation technique terminée, l'organisme fera une soumission de commercialisation de la version (1.3.4) du logiciel auprès de la FDA afin de recevoir une autorisation de sa mise sur le marché Américain. L'Australie et l'Europe suivront par la suite.

C- Apport du stage

Le stage dans les locaux de Pixee Medical a été très enrichissant et bénéfique. L'environnement de travail, la qualité du personnel et les missions réalisées ont permis une améliorer sur le plan professionnel et personnel.

Sur le plan Professionnel : La gestion du projet d'insertion d'une procédure de gestion des activités de cybersécurité ont permis :

- ✓ Amélioration de la capacité à gérer un projet.
- ✓ Recherche, analyse, interprétation et mise en application des textes règlementaires.
- ✓ Planification et animation des réunions de travail.
- ✓ Communication en milieu professionnel.
- ✓ Travail en équipe.
- ✓ Amélioration des connaissances et des compétences techniques sur la cybersécurité, l'orthopédie et le développement logiciel.
- ✓ Familiarisation avec la réglementation Américaine et Australienne.

Sur le plan personnel, cela a permis de renforcer et développer l'esprit d'équipe, la force de proposition et d'analyse, la gestion du temps, l'adaptabilité et la confiance en soi.

De plus le projet m'a amené à discuter avec des personnes au disciplines variées.

D- Difficultés Rencontrées

La première difficulté rencontrée en stage fut le changement des missions de stage. Initialement, le travail devait être tournées vers la rédaction de la documentation technique (Classification, Description, Gestion des risques, Evaluation préclinique et clinique) du logiciel Shoulder, Une temporisation a été faite pour décider sur quel projet je travaillerai prochainement. J'ai travaillé finalement sur le projet de cybersécurité du logiciel KneePlus et de l'organisme en général.

La seconde difficulté rencontrée est qu'une semaine après le début du stage, le tuteur de stage a été infecté par le COVID, et de ce fait a dû passer près de 03 semaines de congés maladie. Pendant cette période, il a fallu établir un nouveau planning pour une meilleure gestion du temps. Cette période a donc été consacrée à une revue de la documentation de l'entreprise, ce qui a plutôt été bénéfique par la suite.

Pour avoir passé la première partie des classes à 70% à distance, avec une culture française différentes de celle du Cameroun, un souci de communication extraprofessionnelle avec l'équipe était présent, mais il s'améliore un peu plus chaque jour.

Conclusion

Aux Etats Unis le président de la république a signé le 12 Mai 2021 un décret destiné à renforcer les ressources de cybersécurité[19] au niveau de la FDA et du NIST. Cela démontre à quel point les incidents de cybersécurité sont de plus en plus grandissants dans les centres de santé, les hôpitaux et la société toute entière. La santé et la sécurité des patients se retrouvent exposées à des vulnérabilités et aux attaques au vu également de l'utilisation croissante des appareils sans fil, connectés à internet, à un réseau ou des supports portables. Pour pallier à cela, La règlementation est un levier fort sur lequel les autorités ont décidé de s'appuyer pour consolider la résilience des dispositifs médicaux. Mais pas que, il faut aussi mobiliser les ressources sur le plan technique et managérial.

C'est dans cet élan que ce projet se positionne pour contribuer aux activités de l'industrie médicale dans l'identification des problèmes liés à la cybersécurité qu'ils doivent aborder dans le cycle de vie du dispositif, de la conception à l'utilisation en passant par le développement et la production. De plus, il faut tout de même prendre en compte la rédaction de la documentation nécessaire pour la demande de commercialisation aux Etats Unis et en Europe. Tout cela dans le but de mettre sur le marché un dispositif médical digne de confiance pour le patient.

Les résultats de ce travail ont été insérés dans le système de management de qualité de l'entreprise. Ils sont utilisés pour la rédaction de la documentation technique de KneePlus. Et aujourd'hui, ils sont préparés pour être utilisés sur le second projet de l'entreprise ShoulderPlan en cours de développement.

Annexes

Annexe 1 : Description des différents groupes de classe de dispositifs médicaux australien.

	Description
Groupe A	Ce groupe comprend les dispositifs médicaux qui contiennent : - Un médicament qui agit sur le patient pour fournir un effet secondaire en plus de l'objectif principal du dispositif (comme les stents recouverts de médicaments), ceci n'inclut pas les dispositifs dont l'objectif principal est de délivrer un médicament (comme les seringues ou les pompes à perfusion) - Les matériaux d'origine animale non viables, sauf si le dispositif est uniquement destiné à entrer en contact avec une peau intacte. Il est possible de citer comme exemples les pansements avec du collagène et les valves cardiaques avec des feuillets de tissu animal Tout matériau d'origine microbienne ou recombinante, comme l'acide hyaluronique ou les protéines recombinantes.
Groupe B	Ce groupe comprend les dispositifs médicaux qui sont : - Des implants mammaires - Implants de remplacement de l'articulation du genou, de la hanche ou de l'épaule - Destinés à la contraception ou à la prévention des maladies sexuellement transmissibles et qui sont implantables ou invasifs pour une utilisation à long terme - Les dispositifs médicaux implantables actifs - Les accessoires implantables des dispositifs médicaux implantables actifs - Dispositifs actifs destinés à contrôler, surveiller ou influencer directement les performances d'un dispositif médical implantable actif
Groupe C	Ce groupe comprend les dispositifs médicaux qui sont : - Les poches de sang, y compris celles qui contiennent un anticoagulant - Les dispositifs médicaux auxiliaires destinés à être utilisés dans la chirurgie de remplacement des articulations - Destinés à désinfecter, nettoyer, rincer ou hydrater les lentilles de contact - Destinés à la désinfection d'un autre dispositif médical - Destinés à la contraception ou à la prévention des maladies sexuellement transmissibles et qui ne sont pas implantables ou invasifs pour une utilisation à long terme
Groupe D	Ce groupe comprend les dispositifs médicaux qui : -Enregistrent des images de patients (par une méthode qui repose sur une énergie située en dehors du spectre visible), où - Sont des modèles anatomiques (physiques ou virtuels), où - Sont des logiciels, programmables ou programmés et utilisés pour générer un modèle anatomique virtuel - Sont également destinés à être utilisés pour l'un ou l'autre des éléments suivants, ou les deux : Le diagnostic ou le suivi d'une maladie, d'une blessure ou d'un handicap L'étude de l'anatomie ou d'un processus physiologique.

Groupe E	Ce groupe comprend les dispositifs qui : - Sont destinés à être utilisés uniquement pour nettoyer un autre dispositif médical (autre que des lentilles de contact) par une action physique. - Sont destinés à l'exportation uniquement - Contiennent des matières d'origine animale non viables, sont destinés à entrer en contact uniquement avec une peau intacte et ne sont pas fournis stériles.

Annexe 2 : Métrique de cotation des critères d'évaluation du niveau de menace.

	DÉPENDANCE	**PÉNÉTRATION**	**MATURITÉ**	**CONFIANCE**
1	Relation non nécessaire aux fonctions stratégiques	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	Relation utile Aux fonctions Stratégiques	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode Réactif	Les intentions de la partie prenante sont considérées comme neutres.
3	Relation indispensable mais non exclusive.	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Relation indispensable et unique (pas de substitution possible à court terme)	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation.	La partie prenante met en œuvre une politique de management du risque. La politiqusse est intégrée et se réalise de manière proactive	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée

Bibliographie

[1] « RÈGLEMENT (UE) 2017/ 745 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 5 avril 2017 - relatif aux dispositifs médicaux, modifiant la directive 2001/ 83/ CE, le règlement (CE) no 178/ 2002 et le règlement (CE) no 1223/ 2009 et abrogeant les directives du Conseil 90/ 385/ CEE et 93/ 42/ CEE », p. 175.

[2] « UL Standard | UL 2900-1 : Software Cybersecurity for Network-Connectable Products, Part1: General Requirements». https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL2900-1 (consulté le juin 06, 2021).

[3] « Knee+ | Navigation en Réalité Augmentéepour l'arthroplastie totale du genou », Pixee Medical. https://www.pixee-medical.com/knee/ (consulté le juin 06, 2021).

[4] Pixee Medical, « Documentations Techniques, Device description ».

[5] O. of the Commissioner, « What We Do », FDA, mars 11, 2018. https://www.fda.gov/aboutfda/what-we-do (consulté le mai 02, 2021).

[6] Y. Pesqueux, Planifier, agir, contrôler : voilà la recette du progrès continu ». La Découverte, 2008. Consulté le: juin 27, 2021. [En ligne]. Disponible sur: https://www.cairn.info/petit-breviaire-desidees-recues-en-management--9782707160140-page-40.htm?try_download=1

[7] « norme NF EN ISO 13485- Dispositifs médicaux - Systèmes de management de la qualité - Exigences à des fins réglementaires », Ed. Afnor, Paris, www.afnor.org, avr. 30, 2016. [En ligne]. Disponible sur: https://sagaweb-afnor-org.ezproxy.utc.fr/fr-FR/sw/consultation/ notice/1416630?recordfromsearch=True

[8] Foods and Drugs Administration (FDA), « Quality System (QS) Regulation/Medical Device Good Manufacturing Practices », FDA, mars 17, 2021. https://www.fda.gov/medical-devices/postmarket-requirementsdevices/quality-system-qs-regulationmedical-device-good-manufacturing-practices (consulté le juin 06, 2021).

[9] Foods and Drugs Administration (FDA), « Content of Premarket Submissions for Management of Cybersecurity in Medical Devices », U.S. Food and Drug Administration, mai 14, 2019. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarketsubmissions-management-cybersecurity-medical-devices (consulté le juin 06, 2021).

[10] Foods and Drugs Administration (FDA), « Postmarket Management of Cybersecurity in Medical Devices », U.S. Food and Drug Administration, juill. 03, 2019. https://www.fda.gov/regulatory-information/search-fdaguidance-documents/postmarket-management-cybersecurity-medical-devices (consulté le juin 06, 2021).

[11] « UL Standard | UL 2900-2-1 : Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems ». https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL2900-2-1 (consulté le juin 06, 2021).

[12] Medical Device Coordination Group Document, « MDCG 2019-16 Guidance on Cybersecurity for medical devices ». Consulté le: juin 06, 2021. [En ligne]. Disponible sur: https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_cybersecurity_en.pdf

[13] « DIRECTIVE 93/42/CEE DU CONSEIL du 14 juin 1993 relative aux dispositifs médicaux ». Consulté le: juin 06, 2021. [En ligne].
Disponible sur: https://eur-lex.europa.eu/legalcontent/FR/TXT/PDF/?uri=CELEX:31993L0042&from=DE

[14] Foods and Drugs Administration (FDA), « Classify Your Medical Device », FDA, oct. 22, 2020. https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device (consulté le juin 13, 2021).

[15] Foods and Drugs Administration (FDA), « Product Classification ». https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpcd/classification.cfm (consulté le juin 13, 2021).

[16] Underwriters Laboratories UL, « U.S. FDA Recognizes UL 2900-2-1 for Use in Premarket Reviews », https://www.ul.com/news/us-fda-recognizes-ul-2900-2-1-use-premarket-reviews (consulté le juin 06, 2021).

[17] « Norme NF EN ISO 14971 - Dispositifs médicaux - Application de la gestion des risques aux dispositifs médicaux », Ed. Afnor, Paris, www.afnor.org, déc. 18, 2019. [En ligne]. Disponible sur: https://sagaweb-afnor-org.ezproxy.utc.fr/fr-FR/sw/consultation/notice/1535096?recordfromsearch=True

[18] Agence nationale de la sécurité des systèmes d'information ANSSI, « guide-methode-ebios-risk-Manager ». Consulté le: juin 19, 2021. [En ligne]. Disponible sur: https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

[19] A. Jonniaux, « États-Unis : Joe Biden signe en urgence un décret sur la cybersécurité », Journal du Geek, mai 14, 2021. https://www.journaldugeek.com/2021/05/14/etats-unis-joe-biden-signe-enurgence-un-decret-sur-la-cybersecurite/ (consulté le juin 20, 2021).