MEDI'NOV 2020

Intégration de dispositifs IoT et médicaux dans une structure hospitalière : application de la famille de norme 80001-X

Philippe Augerat,
Gérant, SurgiQual Institute

9 septembre 2020

Présentation de la norme 80001-1 dans le contexte du projet SERENE IOT

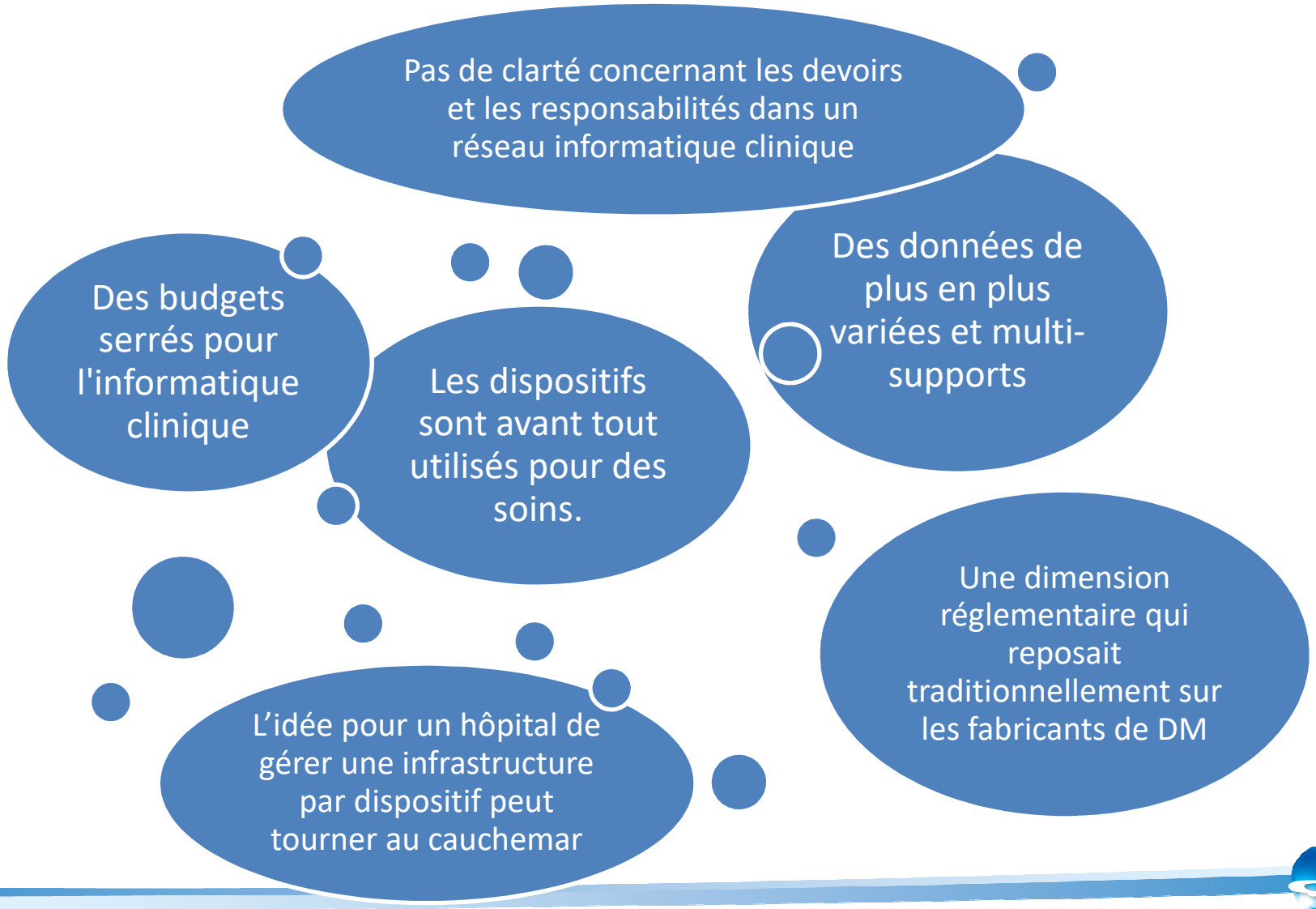
80001-1 : Application du **management du risque** aux réseaux des technologies de l'information contenant des dispositifs médicaux

IoT : Internet of Things

Motivations d'une infrastructure IOT

- L'accès aux données patients (et par extension le big data issu des IoT) combiné à l'analyse de ces données par l'IA sont vus comme un formidable accélérateur pour la médecine personnalisée comme pour la R&D à l'hôpital.
- Plus concrètement pour un hôpital, la connectivité des dispositifs peut permettre un gain de temps administratif, moins d'erreurs de saisie et une facilitation de la maintenance des dispositifs biomédicaux.

Avec de multiples contraintes



Réglementations pour infrastructure IoT

- Un environnement complet/certifié fournit par un fabricant de DM pour une revendication qu'il a identifié
  - **Risques gérés par ISO 14971** : le DM doit être utilisé dans les conditions documentées. L'utilisation du DM par le personnel médical est également soumise à certaines réglementations (formation, qualification).
- L'incorporation de DMs et autres composants multi-fabricants dans une infrastructure réseau sur mesure
  - **Risques gérés par l'IEC 80001-x** : l'hôpital (ou la structure responsable) doit alors prendre en charge les problèmes potentiels liés à l'incorporation des DMs au sein du réseau

Objectif de la série de normes 80001-x

- La norme doit permettre de traiter les points non traités de base par les fabricants car jugés potentiellement hors de leur contrôle
  - Les risques liées à l'incorporation des composants dans le réseau
  - L'inadéquation/indisponibilité potentielle des informations transmises de base par le fabriquant
  - La possibilité de performances altérées par la cohabitation des différents composants sur le réseau (exemple : contraintes de configuration)
  - Plus particulièrement l'interopérabilité des logiciels de dispositifs médicaux et d'autres applications logicielles
  - Certains contrôles de sécurité jugés absent sur les dispositifs médicaux
  - Le conflit entre contrôle strict des modifications d'un DM et réaction rapide en cas de problème de cybersécurité.

Diapositive 6

PA3

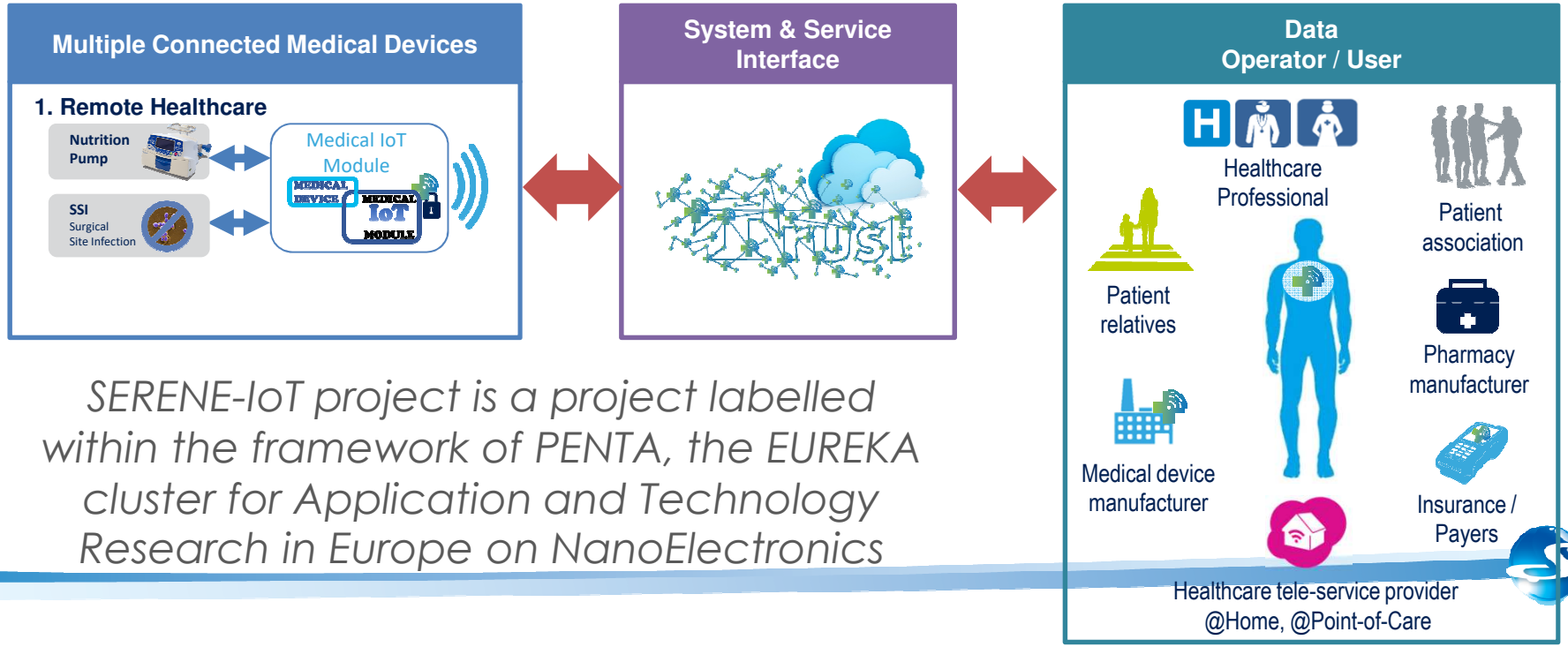
La norme peut permettre de combler l’écart d’usage
Utilisation prévue d'un dispositif médical : réaliser des images ou diagnostiquer un patient à l’instant t
Utilisation prévue d'un réseau informatique clinique : envoyer des commandes, envoyer des images, mais aussi surveiller un patient dans la durée, éviter les erreurs de saisie, etc !!!

La norme peut permettre de gérer des aspects très pratiques
La cybersécurité est la propriété d'un réseau et non d'un appareil.
Les clients ne veulent pas en ajoutant un antivirus, ou autre logiciel, annuler l'homologation du dispositif médical et créer leur propre DM.
Et cadrer le « non prévisible » . Exemple : les fabricants n'ont pas eu à prévoir/mitiger chaque virus à venir pour les dix prochaines années.
Philippe Augerat, 31/08/2020

Projet SERENE IOT

Infrastructure

- Connectivité d'une pompe à nutrition à l'aide d'un dongle et transfert des infos à un logiciel de l'hôpital.
- Connexion entre le dongle et le logiciel possible via plusieurs réseaux (LoRaWAN, BLE, GSM).



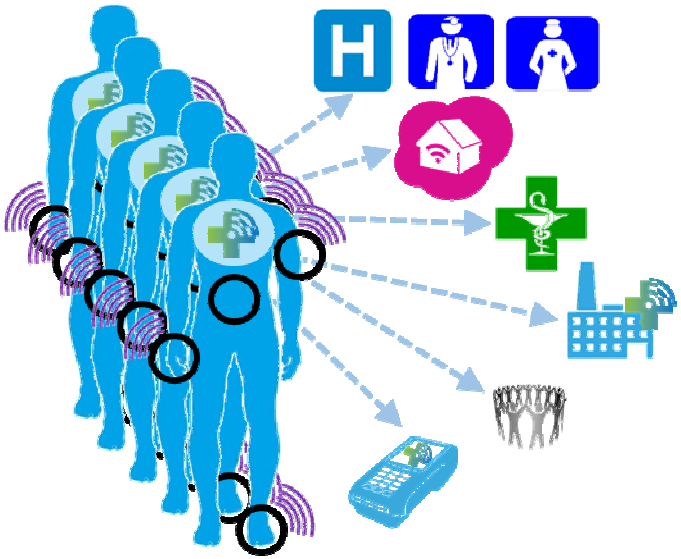
SERENE-IoT project is a project labelled within the framework of PENTA, the EUREKA cluster for Application and Technology Research in Europe on NanoElectronics

Usage ciblé pour le projet SERENE IOT

- Avec un large champ de revendications possibles pour la télémédecine
  - Déport d'information d'un DM
  - Maintenance de DMs
  - Suivi d'observance patient
  - Alertes/Surveillance
  - Décision d'intervention
- Et de multiples utilisateurs

http://serene.minalogic.net/

https://twitter.com/SereneIoT



Device & Service Use Cases

Contraintes de la série 80001-x

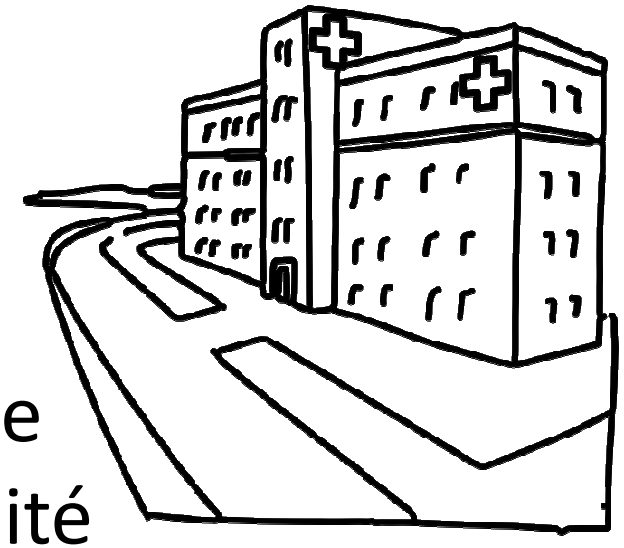
- Elles pèsent en premier lieu sur la structure gérant l'infrastructure (dite organisme responsable), ici l'hôpital qui a pour responsabilité
  - de réaliser un dossier de gestion des risques,
  - de récupérer la documentation de tous les éléments de l'infrastructure,
  - de maîtriser les composants et les intervenants de l'infrastructure pendant tout le cycle de mise en place et utilisation de celle-ci.
- La norme pèse indirectement sur les autres intervenants (fabricants de DM ou non) qui doivent mettre à disposition leur documentation et impacter la maîtrise des risques.

Inconvénients apparents de la série 80001-x

- Cela ressemble à une usine à gaz propre à générer formations, consulting et travail sans fin
  - Part 2-1 - Step-by-step risk management of medical IT-networks - Practical applications and examples
  - Part 2-2 !! Guidance for the disclosure and communication of medical device security needs, risks and controls
  - Part 2-3 - Guidance for wireless networks
  - Part 2-4 - General implementation guidance for Healthcare Delivery Organizations
  - Part 2-5 !! Application guidance: Guidance on distributed alarm systems
  - Part 2-6 - Application guidance - Guidance for responsibility agreements,
  - Part 2-7 - Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
  - Part 2-8 - Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
  - Part 2-9 - Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities
- Mais plus vision positive : on est dans l'auto-évaluation de la conformité et dans des propositions de méthodes et de bon sens qui aident à cadrer les efforts des participants

Côté hôpital : un processus à implémenter

- Définition de responsabilités
- Implication des équipes informatiques et projet pour la description du réseau IT
- Implication de l'équipe juridique pour les accords de responsabilité
- Ecriture d'un plan de gestion des risques



Côté hôpital : la gestion des risques

- Toute la stratégie de l'organisme responsable pour le projet est décrite dans un plan
  - Responsabilités internes
  - Intervenants externes et accords de responsabilité
  - Description du réseau, des composants y compris l'utilisation définie et les bénéfices attendus
  - Exigences de surveillance
  - Critère d'acceptation des risques (la norme ne les définit pas) → s'inspirer du DM principal et donc de l'ISO 14971

Côté fabricant : documentation requise

- La documentation d'accompagnement que l'organisme responsable DOIT recueillir dépend du statut du fabricant, fabricant de DM ou autres fabricants de technologies de l'information
- En commun aux deux listes documentaires, mais avec des terminologies différentes, on trouve:
  - les exigences relatives au fonctionnement connecté des composants
  - les exigences relatives à la sécurité.
- En plus, il est demandé aux fabricants de DM :
  - Une liste de situations dangereuses lorsque l'infrastructure ne satisfait pas aux caractéristiques requises pour la connexion du DM à l'infrastructure.
  - Un document clé, le formulaire MDS2, qui standardise les infos du DM en matière de sécurité de dispositif médical.

MDS2

- **Manufacturer‘s Disclosure Statement on Medical Device Security**
- 23 thèmes de sécurité à documenter par le fabricant
- Passé de 41 questions à 216 questions fin 2019
- Les questions portent sur des sujets tels que :
  - Les types de données privées qui sont stockées sur l'appareil et la manière dont elles sont transmises
  - Le système d'exploitation de l'appareil, la version du système, la configuration et la connexion au réseau
  - Toutes les mesures de sécurité et capacités intégrées, comme le cryptage, la déconnexion automatique, la détection des logiciels malveillants, les verrous physiques, etc.
  - Capacités d'audit
  - Gestion de l'accès, caractéristiques d'authentification, exigences en matière d'autorisation

Côté fabricant : en pratique 1/2

- En pratique, l'organisme responsable peut se contenter de la documentation de base des fournisseurs
  - Pour la pompe, le MDS2 et les documents qui le complètent, la documentation produit, l'analyse de risques 14971 ou son résumé, un notice de cybersécurité, ont couvert les besoins
- L'organisme responsable peut décider que cela ne lui suffit pas et
  - demander au fabriquant une documentation complémentaire
  - demander au fabricant de participer à l'analyse de risques 80001-x.

Côté fabricant : en pratique 2/2

- Dans le cas précédent, il est proposé que l'organisme responsable signe un accord de responsabilité avec le fabriquant
  - Cadré par IEC 80001-2-6:2014 - "Part 2-6: Application guidance -- Guidance for responsibility agreements"
  - Pour le logiciel (qui n'est pas un DM), il a été notamment demandé au fabricant ses stratégies d'essai et les critères d'acceptation de ces essais.
- On est donc proche du travail d'un appel d'offre

L'analyse des risques 80001-1 : principes

- Très proche de l'ISO 14971
- Risques : patient ET confidentialité ET efficacité de l'organisation
- Situations dangereuses
  - Focalisées réseau, il ne s'agit pas de prendre en compte des risques propres à un DM hors de son usage en réseau (ex biocompatibilité) mais les situations dangereuses en lien avec celui-ci
  - Exemples : les problèmes de configuration incorrecte, non interopérabilité, cybersécurité
  - Avec liste de risques à adresser proposée dans IEC 80001-2-1:2012 annexe A

L'analyse des risques 80001-1 : cycle de vie

- La gestion des risques couvre toutes les étapes du cycle de vie de l'infrastructure :
  - incorporation d'un DM, suppression d'un Dm, reconfiguration d'un DM (exemple : affectation à un autre patient du dispositif), modification de l'infrastructure, upgrade d'un composant, surveillance, sauvegarde.
- On s'attend donc :
  - à des risques et des mesures de mitigation associés à chacune de ces étapes, a minima des tests de non régression.
  - à ce que l'organisme responsable intègre à son cadre qualité une procédure de gestion des risques ainsi qu'une procédure de contrôle des documents.

L’analyse des risques SERENE IOT (1/3)

- 22 risques identifiés comme non négligeables avant mitigation dont :
  - Loss of data/connectivity (4)
    - exemple : antenne LORA non fonctionnelle
  - Loss of function of medical device (9) :
    - exemple : système ne fonctionnant pas après upgrade d’un composant
    - Exemple : information patient non à jour
  - User errors (3) :
    - exemple : Erreur d’appairage entre le matériel et le patient
    - exemple : Usage des données dans un autre contexte clinique que celui prévu
  - Incorrect or inappropriate data exchange or interoperability (2)
  - Unauthorized access to data (4)

L'analyse des risques SERENE IOT (2/3)

- Parmi les mesures de risques :
  - 8 sont à implémenter par l'organisme responsable
  - 3 par le fabricant du dongle :
    - exemple : configuration sur la reprise des transferts de données en cas d'erreur de transfert
  - 2 par le fabricant du logiciel :
    - exemple : configuration de messages spécifiques au contexte de l'essai clinique
  - Les autres par des procédures ou accords commerciaux concernant plusieurs acteurs.

L’analyse des risques SERENE IOT (3/3)

- Pour les mesures de mitigation des risques spécifiques au CHU, il s’agit principalement :
  - De mettre en place des tests avant chaque mise ou remise en service de l’infrastructure.
  - D’apporter des éléments de redondance hardware
  - D’apporter des éléments de sauvegarde/restauration des données.
  - De mettre en place une activité de surveillance, s’appuyant sur des contrats

Conformité à la norme 80001

- La conformité est basée sur l'auto-évaluation
  - basée sur la présence des processus et des documents
- Pas de notion de classification de l'infrastructure
- Les normes (60601-1, 62304, etc) respectées par les composants comme leur usage prévu ne sont pas remis en cause PA4

Diapositive 22

PA4 Situation plus complexe si l'hopital développe lui même une partie du logiciel

Philippe Augerat, 03/09/2020

Bilan hôpital

- La mise en place d'une telle infrastructure conforme 80001-x demande certes un effort significatif de l'organisme responsable :
  - processus
  - documentation
  - ressources
- C'est à comparer avec l'aide au cadrage qu'elle apporte dans ce qui ressemble à un appel d'offre
  - définir les processus de suivi du projet en couvrant tous les risques
  - clarifier le « Network Intended Use »
  - demander aux fabricants la documentation adaptée

Bilan fabricants

- Pour les autres acteurs, cela demande plus de transparence et de détails
  - de rendre public à l'organisme responsable des informations habituellement non fournies mais existants
  - Exemples : analyse de risques (ou son résumé), notice de cybersécurité, stratégie d'essai, résultat d'essai
- Avec un travail additionnel minimal
  - L'obligation des fabricants de DM vis-à-vis de la norme IEC 80001 de fournir le formulaire MDS2
  - Sous réserve d'avoir anticipé la connectivité

Présentation de SurgiQual Institute (SQI)

12 ans d'accompagnement de nos clients

Développement logiciel sous assurance qualité

Conformité réglementaire des dispositifs médicaux

- Plus de 130 clients
- 54% de start-ups
- 35% en local
- Reconnaissance de nos compétences et de nos méthodologies (certifiées ISO 13485)
- 24 personnes

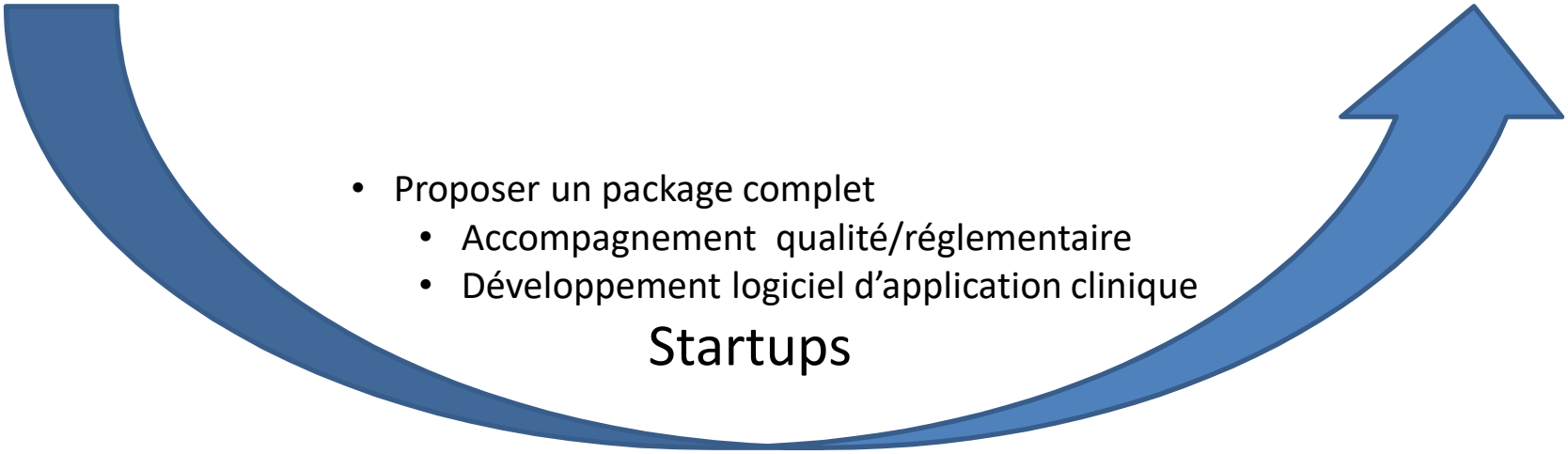
La volonté de développer des offres uniques

Institutionnels

- Gérer comme fabricant les aspects conformité d'un essai clinique de dispositif médical non marqué CE

Industriels

- Développer des outils numériques pour le bloc opératoire
- Développer des plateformes logicielles cloud pour la médecine personnalisée



- Proposer un package complet
  - Accompagnement qualité/réglementaire
  - Développement logiciel d'application clinique

Startups

7 experts qualité et affaires réglementaires

15 experts du développement logiciel

Avec de belles réussites

- http://www.sinnovial.com/fr/technosinnotest/
- https://www.youtube.com/watch?v=Qa6s5m3WKn0
- https://www.magia-diagnostics.com/
- https://lnkd.in/dENdUuh
- https://www.medicalps.eu/2020/01/28/innover-en-toute-securite-avec-surgiqual-institute-le-cas-decole-du-projet-brain-computer-interface/

Merci !