DeviceMed

Le magazine des fabricants de dispositifs médicaux

2

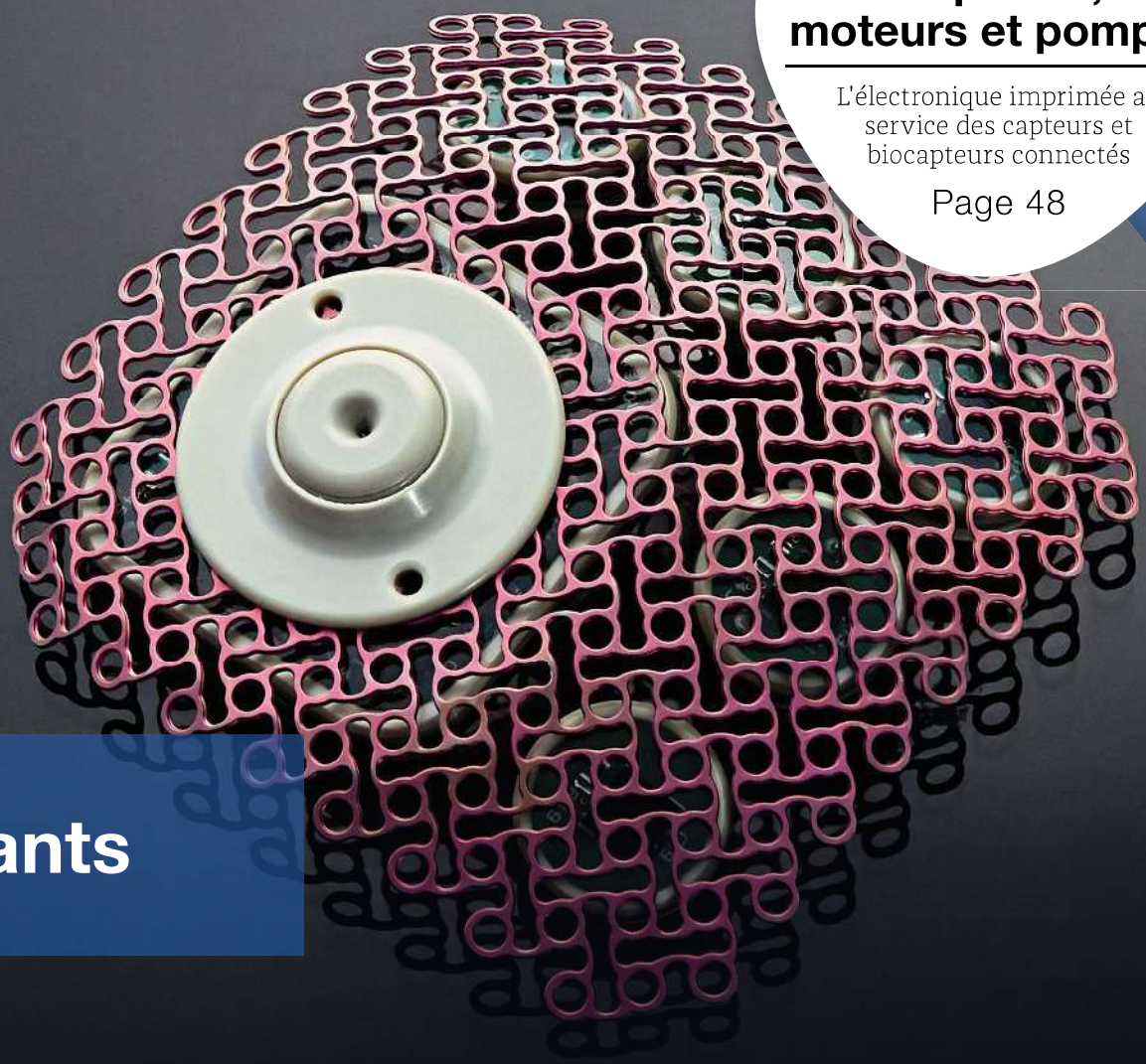
www.devicemed.fr
Année 18 | Mars/Avril 2025
ISSN 2198-3410
Euro 11,–

FOCUS

Capteurs, moteurs et pompes

L'électronique imprimée au service des capteurs et biocapteurs connectés

Page 48



DOSSIER

Implants

Page 14

Médi'Nov 2025 Avant-première

Cap sur l'innovation !

Page 30

DM d'administration de médicaments

Système d'essais pour auto-injecteurs selon la norme ISO 11608

Page 52

SPÉCIAL

DM connectés et E-Santé

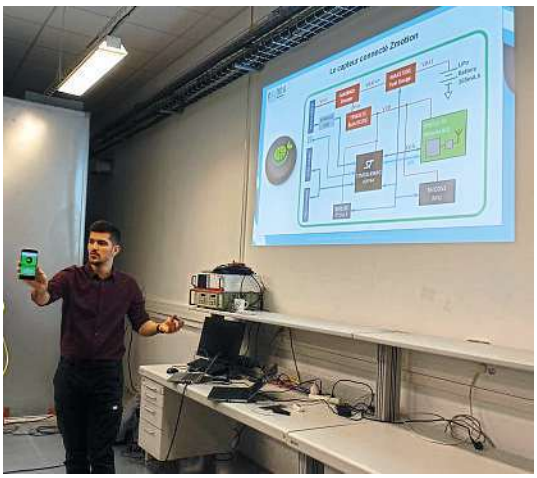
Communiquer en Li-Fi : une idée lumineuse pour le secteur médical ?

Page 40

VOGEL COMMUNICATIONS GROUP

Sécuriser les dispositifs médicaux connectés : le rôle essentiel du pentest

Face aux risques de cyberattaques, les pentests sont devenus incontournables pour les fabricants de dispositifs médicaux connectés. Mais de quoi s'agit-il ? C'est une question à laquelle sait répondre Mickaël Seignobos d'Esynov, qui donnera une conférence sur le sujet à Medi'Nov 2025.



Source : Esynov

Esynov propose une formation dédiée à la cybersécurité des DM, qui peut être donnée en entreprise, avec adaptation personnalisée.

Qu'il s'agisse de pompes à insuline, de pacemakers, de moniteurs de signes vitaux ou encore d'équipements de laboratoire, les dispositifs médicaux connectés sont des cibles privilégiées de cyberattaques.

« L'interconnexion croissante de ces dispositifs avec les réseaux, que ce soit à domicile ou en milieu hospitalier, amplifie les menaces, un dispositif vulnérable pouvant servir de point d'entrée dans le réseau », explique Mickaël Seignobos, Expert Cybersécurité Produit pour Esynov. Et une faille peut avoir des conséquences dramatiques : vol de données de santé, modification des paramètres d'un appareil, interruption de fonctionnement critique, perte de secrets industriels (Propriété Intellectuelle), etc.

Une exigence réglementaire en Europe et aux États-Unis

Face à ces menaces réelles, les autorités imposent désormais des règles strictes en cybersécurité. En Europe et aux États-Unis, la réalisation de tests d'intrusion (pentests) par un tiers est devenue une exigence normative (ex. guidance FDA "Cybersecurity in Medical Devices" du 27 septembre 2023).

« Les entreprises qui ignorent ces obligations s'exposent à de fortes sanctions économiques, et en particulier à un refus d'autorisation de mise sur le marché », précise Mickaël Seignobos, « Sans parler des dommages sur l'image de marque de l'entreprise ».

À plus haut niveau, pour être conforme au Cyber Resilience Act qui s'applique aux produits intégrant des éléments numériques, les industriels doivent :

- intégrer la cybersécurité dès la conception (principe de "security by design"),
- assurer la mise à jour et la correction des failles de sécurité durant le cycle de vie du produit,
- notifier les autorités en cas de faille de sécurité critique,
- et évaluer les risques.

Le pentest fait partie intégrante de ce processus de démonstration et de documentation de la sécurité dans le cadre d'une conformité aux normes européennes et internationales.

Déroulement d'un pentest sur un DM

Un test d'intrusion suit une méthodologie rigoureuse adaptée aux systèmes embarqués, réalisée par un ingénieur spécialisé, indépendant des équipes de développement :

- cartographie des composants : identification des interfaces (Wi-Fi, Bluetooth, ports USB, API cloud...),
- analyse des menaces : recherche des vulnérabilités connues (CVE) et spécifiques à l'architecture du dispositif,
- attaques simulées : exploitation des failles détectées (injection de code, attaques sur le firmware, interception de données),
- évaluation des impacts : analyse des conséquences potentielles (prise de contrôle, altération de données, interruption),
- recommandations et corrections : rapport détaillé avec mesures correctives,
- nouveau test après correction (optionnel) : vérification que les vulnérabilités ont bien été éliminées.

Ces éléments soulignent pour les industriels la nécessité d'intégrer la cybersécurité dès la conception du DM et tout au long de son cycle de vie, en mobilisant des spécialistes et partenaires de confiance pour se former et réaliser les pentests. *eg*

Stand 29
www.esynov.fr

DeviceMed

INFO

La plateforme technologique Esynov est une association indépendante d'une vingtaine d'experts, qui s'appuient sur l'expertise académique de Grenoble INP - Esisar, et sur près de 30 ans de collaboration avec les industriels pour promouvoir les bonnes pratiques en R&D et pré-industrialisation de systèmes embarqués. La mission d'Esynov est de répondre aux besoins des industriels sur les thématiques CEM, RF et Cybersécurité produit, par de la formation et du conseil en phase de conception et R&D, de préqualification produit et de pentest.