



PRODUITS  
EQUIPEMENTS  
INDUSTRIELS

Nr. 11

**8 Rencontre avec**  
Patrick Kargol  
directeur  
de Kipp France

**14 Dossier spécial**  
Sécurité Industrielle  
et Cybersécurité

**16 Minalogic œuvre**  
pour la cybersécurité

**22 Le Wi-Fi 6 répond au**  
défi des usines  
intelligentes

**24 Focus**  
Equipements  
et Systèmes  
pour la Logistique

**26 L'IA générative**  
s'intègre dans  
les terminaux  
mobiles

## PROTÉGEZ VOS INFRASTRUCTURES INDUSTRIELLES

face aux cybermenaces grandissantes !

Page 14



**21** Grâce à la sécurité intégrée du matériel, la gamme Cosy+ de HMS Networks permet d'accéder, sans risque et à distance, aux machines reposant sur des automates pour réaliser des tâches de mise en service, de dépannage et de programmation en ligne.



@peifrance

TWITTEZ AVEC NOUS !  
DEVENEZ UN DE NOS  
FOLLOWERS !



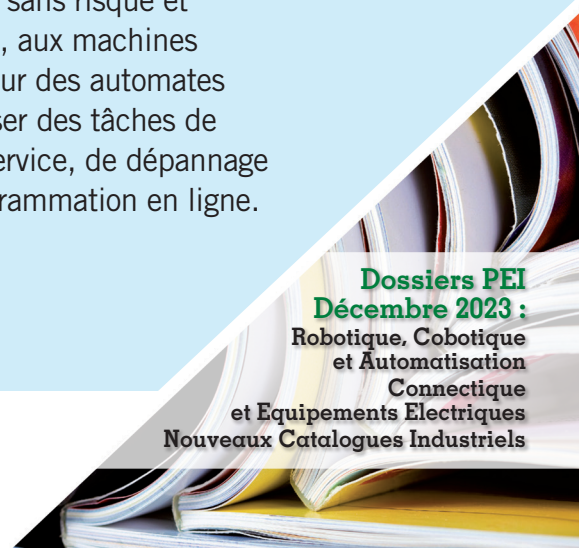
[www.pei-france.com](http://www.pei-france.com)

**Dossiers PEI**  
**Décembre 2023 :**

Robotique, Cobotique  
et Automatisation

Connectique

et Equipements Electriques  
Nouveaux Catalogues Industriels





**28 NOVEMBRE, 2023**  
**au Palais de la Bourse, Lyon**

**Conférences, Réseautage, Expositions,  
Déjeuner + Cocktail inclus**

## **L'INDUSTRIE 4.0 ET LES DERNIÈRES SOLUTIONS**

**OT SECURITY SYSTEMS & MANAGEMENT**

**IIOT, SCADA , ICS**

**LA CONVERGENCE ET L'EDGE COMPUTING**

**DATA CENTER ET SÉCURITÉ**

**APPLICATIONS DE LA TECHNOLOGIE BLOCKCHAIN POUR L'INDUSTRIE 4.0**

**LA CHAÎNE D'APPROVISIONNEMENT**

**En collaboration entre:**



**&**



**RESTEZ CONNECTÉ POUR NE PAS MANQUER L'ÉVÉNEMENT!**



120 Rue Jean Jaurès — 92300 Levallois-Perret  
Fax 01 47 56 20 20  
www.pei-france.com

#### RÉDACTION

Jacques Marouani  
tél. 06 65 29 96 84  
redaction@tim-europe.com

#### RÉGIE PUBLICITAIRE

Roxanne Akbulut  
tél. 06 52 31 41 56  
r.akbulut@tim-europe.com

M'fumu Tiya Mindombe  
tél. + 32 465 443 530  
m.mindombe@tim-europe.com

Représentants à l'étranger  
<https://media.tim-europe.com>

#### DIRECTEUR DE LA PUBLICATION

Orhan Erenberk  
o.erenberk@tim-europe.com

#### ADMINISTRATION DES VENTES/MAQUETTE

Francesca Lorini  
f.lorini@tim-europe.com

#### RESPONSABLE MARKETING

Marco Prinari  
m.prinari@tim-europe.com

#### WEB/NEWSLETTER

Carlo Cucchi  
c.cucchi@tim-europe.com



140 rue de Stalle - 3ème étage, 1180 Uccle,  
Bruxelles, Belgique

Numéro ISSN: 0999-4297  
Tirage de ce numéro: 25.000 exemplaires.  
Conception graphique: Design3, Milano, Italy  
Imprimé en Italie par Logo Srl - Padova  
© 2023 TIM Global Media BV



Jacques Marouani  
j.marouani@tim-europe.com

## La cybersécurité, un investissement à long terme

A l'heure où l'on ne cesse de parler de révolution digitale, d'usine 4.0, d'Internet des objets, d'intelligence artificielle, il est d'autant plus indispensable pour les entreprises de **protéger leurs infrastructures numériques**. Objectif : diminuer, voire éliminer, leur exposition à des cyberattaques toujours plus perfectionnées. Cela passe par la **sensibilisation à la cybersécurité de tout le personnel** connecté au système d'information. Un investissement à long terme qui aura pour effet de détourner l'attention de potentiels « hackers » car ces derniers s'attaqueront plus facilement aux systèmes d'information les plus mal protégés.

Il sera particulièrement efficace de s'informer sur la cybersécurité dans l'industrie, lors d'une **journée consacrée exclusivement à ce sujet, le 28 novembre, à Lyon**, où 300 entreprises sont attendues. Son nom : **Industrial CyberSec Forum, une manifestation dont PEI est partenaire.**

### Un projet européen porté par Minalogic

A cette occasion, nous publions un **Dossier Spécial Sécurité Industrielle et Cybersécurité**, détaillant les risques encourus, les moyens de s'en protéger et les actions à entreprendre pour se protéger efficacement. Prodware y dévoile un « **livre noir** » du « **hacker** » qui permet d'entrer dans la tête d'un cybercriminel pour mieux comprendre sa démarche et le neutraliser, Minalogic présente ses **actions de sensibilisation à travers le projet européen MinaSmart**, SoSafe revient sur son rapport qui indique que 46% des entreprises ont été victimes d'au moins une cyberattaque au cours des trois dernières années, et Intel présente son approche d'un écosystème ouvert afin de garantir que les opportunités de l'intelligence artificielle soient accessibles à tous, sans y sacrifier la sécurité des plates-formes et la protection de l'intégrité des données.

### Suivi des actifs, précis et économe en énergie

Autre thème essentiel pour l'industrie : les infrastructures logistiques. Nous abordons ce thème avec un **Focus Equipements et Systèmes pour la Logistique**. Y sont présentés un **service personnalisé d'approvisionnement en pièces détachées** développé par Antares Vision pour la société suisse Ferring, un système de suivi des actifs, précis et économe en énergie, basé sur un microcontrôleur Bluetooth Onsemi, et l'intégration de l'IA générative dans les terminaux mobiles et tablettes Zebra, en s'appuyant sur les solutions de Qualcomm.

*Jacques Marouani*

Rédacteur en chef

Abonnement  
numérique  
GRATUIT



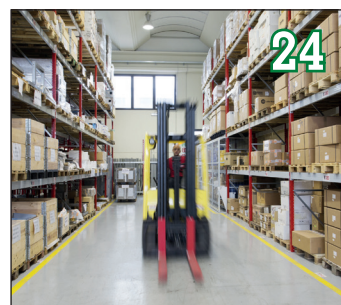
ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

[www.pei-france.com](http://www.pei-france.com)



- 5 Intel déploie la lithographie extrême ultraviolet pour la production en volume en Irlande
- 6 Circuits imprimés : Icape se développe aux Etats-Unis et en Allemagne
- 7 Le marché des moteurs ultra-basse tension devrait atteindre 6,5 milliards de dollars en 2027
- 8 Rencontre avec Patrick Kargol, directeur de Kipp France
- 10 Les câbles et chaînes porte-câbles d'Igus équipent la machinerie scénique des navires de croisière
- 12 Le blindage électromagnétique EMI pour les applications 5G gagne en efficacité
- 14 Dossier Spécial Sécurité Industrielle et Cybersécurité**  
Industrial CyberSec Forum le 28 novembre 2023 à Lyon
- 15 « Livre noir » du « hacker » : portrait d'un cybercriminel et guide de survie des entreprises
- 16 Toutes les entreprises doivent se sentir concernées par la cybersécurité
- 18 Près de la moitié des entreprises françaises auraient déjà été victimes de cyber-attaques
- 20 Accélérer la convergence de l'intelligence artificielle et de la sécurité
- 22 Wi-Fi 6 : répondre aux besoins changeants des usines intelligentes
- 24 Focus Equipements et Systèmes pour la Logistique**  
Un service personnalisé d'approvisionnement en pièces détachées
- 25 Un suivi des actifs précis et plus économe en énergie
- 26 L'IA générative s'intègre dans les terminaux mobiles
- 28 Une meilleure productivité pour les mesures dans les applications hygiéniques
- 29 Guidages linéaires pour un mouvement ultra-fluide
- 30 Index





## Intel déploie la lithographie extrême ultraviolette pour la production en volume en Irlande

Intel célèbre l'arrivée de sa technologie Intel 4, qui utilise la technologie de l'extrême ultraviolet (EUV), et la première utilisation de l'EUV dans la fabrication en grand volume (HVM) en Europe. Cette étape importante inaugure l'avenir de produits tels que les prochains processeurs Intel Core Ultra, qui ouvriront la voie aux PC avec IA, ainsi que les processeurs Intel Xeon de prochaine génération qui arriveront en 2024 et seront produits sur le nœud de fabrication Intel 3. La technologie EUV utilisée dans la production d'Intel 4 est largement adoptée dans les nœuds technologiques des semi-conducteurs de pointe qui alimentent les applications informatiques les plus exigeantes, telles que l'intelligence artificielle (IA), les réseaux mobiles avancés, la conduite autonome ou les nouvelles applications de centre de données et de cloud. L'ouverture de la Fab 34 d'Intel à Leixlip, en Irlande, combinée au projet d'installation de fabrication de tranches à Magdebourg, en Allemagne, et au projet d'installation d'assemblage et de test à Wrocław, en Pologne, contribuera à créer une chaîne de valeur de fabrication de semi-conducteurs de pointe de bout en bout, la première du genre, en Europe.



## Le fondeur X-Fab va bénéficier d'un financement européen pour ses innovations en semi-conducteurs

X-Fab Group, fondeur spécialisé dans la production de semi-conducteurs à signaux analogiques/mixtes, est sur le point de bénéficier d'importantes subventions européennes. Le financement, d'un montant total d'environ 80 M€, s'étendra sur trois usines.



Celle de Corbeil-Essonnes en France se spécialise dans les capteurs intelligents et les circuits de commande, les nouvelles architectures, la photonique et les technologies RF. Le site a récemment lancé sa production en 110 nm sur tranches de 200 mm, grâce à la technologie de pointe BCD-sur-SOI. Le site d'Erfurt en Allemagne travaille sur le développement d'une plateforme de fabrication unique et novatrice pour les systèmes de capteurs intégrés intelligents. X-Fab enrichit ainsi considérablement son offre technologique dans les domaines des systèmes de capteurs intelligents, de l'intégration 3D et de l'intégration de puces hétérogènes au moyen de l'impression par micro-transfert et contribue à élargir l'état de l'art international en matière de technologies d'intégration de systèmes et

d'assemblage avancé. Sur le site d'Itzehoe en Allemagne, X-Fab se concentrera sur le développement et la mise en œuvre de nouvelles méthodes de traitement des tranches en verre.

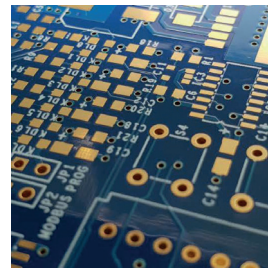
## Equans crée une entité spécifique pour aider ses clients dans leur transition digitale

Equans lance Equans Digital pour aider ses clients à développer leur performance à travers leur transition digitale. Elle rassemble l'ensemble des expertises des entités spécialisées dans les technologies de l'information et de la communication et le digital, soit 6000 collaborateurs, pour un chiffre d'affaires d'un milliard d'euros, dont la moitié en France. Le digital s'impose jour après jour comme un élément clé de la performance : performance des systèmes techniques (chaud, froid, IT) ; performance énergétique ; performance des process industriels, satisfaction pour les usagers finaux. Les spécialistes de Equans Digital s'appuient sur cinq expertises essentielles : audiovisuel et vidéo, robotique, automatisme, BIM, télécom et connectivité. Equans Digital intervient également dans des domaines transverses via une triple expertise de haut niveau : la cybersécurité, l'interopérabilité et les solutions applicatives. La cybersécurité est au cœur du digital. Il est indispensable de mesurer en temps réel les menaces et la vulnérabilité des systèmes pour mieux les protéger et garantir leur fonctionnalité.



## Circuits imprimés : Icape se développe aux Etats-Unis et en Allemagne

Icape, distributeur de circuits imprimés, a annoncé l'acquisition des actifs opérationnels des sociétés américaines PCB Solutions, Ustek et Nujay Technologies. Les trois sociétés sont spécialisées dans le négoce de circuits imprimés aux États-Unis depuis plus de vingt ans. PCB Solutions et Ustek Incorporated comptent également une activité de négoce de pièces techniques, représentant pour la première 10% de son activité et pour la seconde près de 30% de celle-ci. Au total, les trois sociétés couvrent les besoins d'un portefeuille de plus de 180 clients nord-américains, issus d'une importante variété d'industries, allant de la conception de matériel médical au secteur automobile. En 2022, ces trois sociétés ont généré un chiffre d'affaires annuel net cumulé de plus de 5 millions de dollars ainsi qu'une marge d'Ebitda supérieure à 10%. Par ailleurs, Icape a fait l'acquisition de 100% du capital de la société Princitec, fournisseur allemand à haute valeur ajoutée de circuits imprimés. Avec une base de 35 clients actifs principalement localisés en Allemagne, Princitec a généré en 2022 un chiffre d'affaires de 6,5 millions d'euros ainsi qu'une marge brute de l'ordre de 25,5%.



## Le Cetim référencé par la BPI pour les diagnostics d'éco-conception

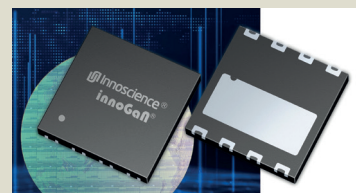
Le Cetim, institut technologique labellisé Carnot, a été référencé par la BPI (Banque publique d'investissement) sur les diagnostics d'éco-conception. Il fournit un accompagnement de 18 jours destiné aux entreprises de moins de 250 salariés et subventionné à hauteur de 60 à 70%. Fort de son expérience de près de deux décennies, le Cetim s'est forgé une expertise dans l'élaboration de méthodologies, d'outils et de normes visant à encourager les entreprises de l'industrie mécanique à adopter des pratiques d'éco-conception. Dans le cadre de ce



référencement, le Cetim propose un accompagnement structuré qui vise à identifier des leviers d'éco-conception au sein de l'entreprise en évaluant la performance environnementale de produits de référence et en cherchant des solutions viables. Une approche d'éco-conception en six étapes, basée sur une méthodologie normalisée (NF EN 16 524) qui permet de prendre en compte les enjeux environnementaux, de hiérarchiser les priorités et de concevoir ou reconcevoir les produits pour les rendre moins impactants sur l'environnement.

## Codico, distributeur d'Innoscence centré « conception intégrée »

Innoscence, société fondée pour créer un écosystème énergétique mondial basé sur des solutions électriques à hautes performances et à



faible coût au nitrure de gallium sur silicium (GaN-on-Si), a annoncé un accord de distribution avec Codico, couvrant tous les pays européens. Ce distributeur a été choisi pour accompagner les concepteurs du « début de leur parcours GaN, jusqu'à la production complète ». Codico est une entreprise dont le siège est près de Vienne en Autriche, avec des centres de compétence produits à Munich (Allemagne), Trévise (Italie) et Stockholm (Suède). Elle fournit un support technique depuis la phase de développement initiale jusqu'au produit final, pour une gamme de composants électroniques actifs, passifs et électromécaniques. « La plupart des clients n'en sont qu'au début de leur parcours avec les produits GaN. Par conséquent, même si les pièces sont robustes, fiables et faciles à utiliser, les concepteurs auront besoin de beaucoup d'assistance technique. Codico est en mesure de fournir l'expertise technique requise », a commenté Denis Marcon, directeur général d'Innoscence pour l'Europe.

## Travaux de recherche sur des pompes entraînées par moteur électrique

Vanzetti Engineering a lancé un projet avec l'École Polytechnique de Turin pour l'étude de pompes entraînées par un moteur électrique. Le projet est entièrement financé par Vanzetti Engineering dans le cadre d'une bourse de doctorale sur une durée de trois ans et a débuté en novembre 2022. Les applications de ces machines peuvent être multiples mais l'une des

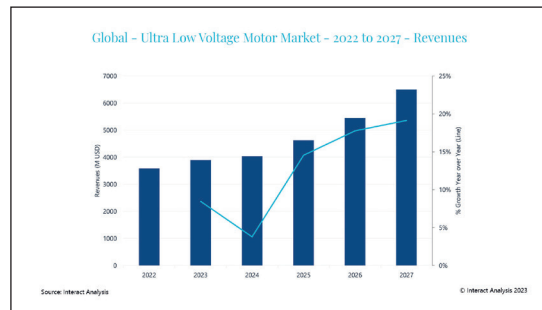


plus avancées sur le plan technologique est leur utilisation sur un lanceur spatial. Il s'agit d'un marché en pleine expansion, notamment après plusieurs lancements réussis par une entreprise américaine de renom dont les moteurs sont alimentés par cette même technologie. Dans un lanceur, les pompes ont pour tâche de pressuriser les propergols (par exemple LOX et GNL) en les amenant de la pression du réservoir à celle de la chambre de combustion, où ils réagissent en libérant l'énergie nécessaire pour générer la poussée qui permet à la fusée de décoller. Dans la configuration traditionnelle, les pompes sont entraînées par des turbines dédiées, mais des développements récents ont montré que, dans certains cas, celles-ci peuvent être remplacées par des moteurs électriques alimentés par batterie.



## Le marché des moteurs ultra-basse tension devrait atteindre 6,5 milliards de dollars en 2027

Le marché des moteurs ultra-basse tension devrait croître de 12,6% par an entre 2022 et 2027 pour atteindre près de 6,5 milliards de dollars, selon une étude de la de marché d'Interact Analysis. Ce marché est stimulé par la demande d'applications alimentées par batteries et par le besoin d'une plus grande flexibilité dans les processus de fabrication et de logistique. Trois acteurs principaux, Maxon, Ametek et MinebeaMitsumi, dominent actuellement le marché, mais le paysage est très fragmenté. Cela signifie que l'évolution de ce paysage dépend des solutions que les fournisseurs décident de développer dans de nombreux secteurs du marché, notamment les robots mobiles. Il existe également une tendance croissante vers les moteurs et entraînements intégrés, en particulier dans le segment de la robotique mobile, qui présente des opportunités pour différents fournisseurs d'émerger et de gagner des parts de marché. D'ici 2027, les moteurs intégrés devraient représenter 14% des moteurs utilisés dans les robots mobiles. Alors que le segment de la robotique mobile ne représente aujourd'hui que 3% des expéditions de moteurs, d'ici fin 2027, le secteur représentera 15,6% des expéditions totales du marché.



## Mitsubishi annonce une 2<sup>e</sup> usine de systèmes de contrôle d'automatisation industrielle au Japon

Mitsubishi Electric annonce un investissement supplémentaire de 42,5 milliards de yens, soit environ 275 millions d'euros, pour la construction d'une seconde unité de production destinée à la fabrication de systèmes de contrôle d'automatisation industrielle (Factory Automation) à Owariasahi City - préfecture d'Aichi - qui fait partie de son site industriel de Nagoya.



L'investissement initial, annoncé le 28 mars 2022, concernait une seule unité de production qui devait entrer en service en avril 2025. Ce projet est désormais complété par l'addition d'un deuxième bâtiment qui devra être opérationnel en avril 2027. Au total, l'investissement cumulé s'élève à 55,5 milliards de yens, soit environ 360 millions d'euros. Les deux unités de production seront étroitement intégrées pour rationaliser leurs opérations. En tant qu'usines de nouvelle génération, les communications 5G et l'IA seront utilisées, de même que la gestion avancée de la chaîne d'approvisionnement (SCM) et la gestion de la chaîne d'ingénierie (ECM) basées sur le concept «e-F@ctory» de Mitsubishi Electric. Les bénéfices attendus sont l'accélération de la productivité et l'amélioration de la qualité des cycles, la réduction des délais de livraison et une production de haute qualité et à haut rendement.

## Faulhaber réorganise son équipe de ventes mondiales

Afin de renforcer l'organisation des ventes à une époque où les marchés internationaux sont de plus en plus complexes, la société a décidé de remanier son équipe de ventes mondiales. Marcus Rimmel prend en charge le développement du marché mondial et est responsable du développement de nouvelles filières de vente et de nouvelles activités de développement commercial à l'échelle mondiale.

Dans ce contexte, Faulhaber veut se concentrer sur les grands comptes, les marchés cible et les régions à haut potentiel et investir dans le développement de savoir-faire spécialisé pour les secteurs du médical, de l'automatisation et de la robotique. Volker Sprenger qui gérait déjà les activités de vente et les grands clients en Allemagne, prend en charge les grands comptes au niveau mondial.

De plus, il continuera à renforcer la présence de Faulhaber en Amérique du Nord. Au vu de ses nombreuses années d'expérience de la gestion des relations avec les clients et déjà chef du service des activités de ventes mondiales, Mireille Deckers-Strobel assume désormais également la responsabilité des marchés de vente d'Europe, de Chine et d'Asie-Pacifique, ainsi que des clients directs partout dans le monde et du réseau de distribution.





# Rencontre avec Patrick Kargol, directeur de Kipp France

Patrick Kargol nous présente les activités de la société allemande Kipp, spécialisée dans les éléments de manœuvre et de serrage, les éléments standards mécaniques et les éléments de bridage pour machines à commande numérique 5 axes.

**Spécialisée dans les éléments de manœuvre et de serrage, la société Kipp est plus que centenaire. Pourriez-vous nous retracer son historique et nous préciser son savoir-faire ?**

**Patrick Kargol :** Kipp est une société familiale allemande fondée en 1919 qui a pris un virage industriel dans les années 1950 quand elle a inventé la manette indexable pour le serrage et l'ajustement de pièces sans outils. Basée à Sukz-am-Nekar, à 70 km de Stuttgart, elle dispose à son catalogue de plus de 65000 références d'éléments de manœuvre standards. Elle propose également la fabrication de pièces adaptées à des demandes spécifiques en termes de longueur ou de texture par exemple, qui sont dérivées de produits standards.

**En quelques chiffres clés, pouvez-vous nous situer aujourd'hui l'importance de Kipp : chiffre d'affaires, nombre de salariés, de filiales, de sites de production... ?**

**Patrick Kargol :** La société Kipp souhaite ne pas divulguer le montant de son chiffre d'affaires. Ce que je peux dire, c'est qu'elle emploie un peu moins de 500 personnes, dont 400 salariés, tous métiers confondus : finance, vente, production, logistique... Elle a 50 représentants à l'étranger et des sociétés dans 12 pays : Allemagne, France, Italie, Suisse, Autriche, Pays-Bas, Suède, République tchèque, Pologne, Turquie, Etats-Unis et Canada. La production et le centre logistique sont situés près du siège de la société.

**Kipp répond aux attentes et aux exigences de nombreuses industries, mais quelle est précisément l'étendue de son offre ? Pour quels grands types d'applications ?**

**Patrick Kargol :** Nos produits s'adressent aux fabricants de machines spéciales et à toute l'in-



*Patrick Kargol, directeur de Kipp France*

dustrie, depuis la petite start-up jusqu'aux très grands groupes. Notre gamme comprend des éléments de manœuvre et de serrage, des éléments standards mécaniques et des éléments de bridage pour machines à commande numérique 5 axes.

**Quelles sont les orientations de Kipp en matière d'innovation et dans quels domaines la société investit-elle ?**

**Patrick Kargol :** Nous suivons les évolutions de l'industrie 4.0 et nous avons par exemple mis au point un capteur d'état sans fil qui permet de vérifier le statut des produits : ouverts ou fermés. Outre nos dépenses en recherche et développement, nous avons réalisé d'importants investissements sur le site de production pour optimiser la fabrication en élargissant le parc machines, et dans le domaine de la logistique. Un centre logistique automatisé a été mis en place dès 2013 et nous en avons créé un autre l'année dernière qui a permis de doubler la capacité d'expéditions de la société.

**Quand la filiale française de Kipp a-t-elle été créée et comment opère-t-elle commercialement ?**

**Patrick Kargol :** La filiale française, basée à Vélizy-Villacoublay, près de Paris, a été créée il y a 20 ans, en juin 2003. C'est une entité commerciale qui compte 6 personnes. En plus des ventes directes via notre site Internet qui n'impose qu'un minimum de commande de 50 €, nous travaillons également avec des distributeurs. Notre chiffre d'affaires sur le marché français a pratiquement triplé au cours des dix dernières années.

**Comment analysez-vous le marché des éléments de manœuvre et de serrage en France en termes de développement et de concurrence, et quels sont vos objectifs à moyen terme sur le marché national ?**

**Patrick Kargol :** Nous avons plusieurs concurrents importants, fabricants ou distributeurs, établis notamment en Italie et en Allemagne. Le marché des éléments standards est difficile à chiffrer. Au cours de ces dernières années, nous avons connu une croissance dynamique due à un élan en faveur de l'amélioration des conditions de travail et à d'importants investissements en machines de production de la part des entreprises industrielles. La demande est particulièrement importante dans l'automobile, l'aéronautique et l'agroalimentaire qui sont des secteurs en forte croissance. Nous bénéficions de leur croissance et cela nous permet de nous développer à un rythme d'environ 10% par an, hors années Covid, durant lesquelles toute l'industrie a souffert.

►► 34203 sur [www.pei-france.com](http://www.pei-france.com)



## CAPTEURS DE NIVEAU RADAR CONNECTÉS AU CLOUD

pour la surveillance de niveaux à distance



**Automation24** propose les capteurs de niveau de Staal Instruments qui servent à surveiller les liquides dans les contenants et cours d'eau à ciel ouvert. Leur connexion au StaalCloud permet de collecter

et exploiter les données des appareils en temps réel. Un traceur GPS intégré fournit également des informations sur la position des substances en cours de transport. Les dispositifs de mesure de niveau radar de Staal Instruments sont conçus pour mesurer le niveau et le volume de liquides tels que l'eau, les produits chimiques et les huiles. Leur utilisation est surtout intéressante dans les applications où aucune infrastructure n'est disponible ou dans les cas où l'objet surveillé se déplace, notamment pour les cuves IBC ou les fûts en plastique. Après fixation à l'extérieur d'une cuve IBC, les volumes et niveaux peuvent être mesurés à travers la paroi en plastique. Outre des mesures de niveau et de volume, ces capteurs fournissent des informations fiables concernant la position des contenants IBC, souvent utilisés pour le déplacement des marchandises. Parmi les autres applications envisageables, on trouve la surveillance du niveau des canalisations d'eaux usées ou le monitoring des plans et cours d'eau à ciel ouvert. Ils permettent alors de détecter à temps les niveaux critiques et de prendre des mesures correctives.

►► 34207 sur [www.pei-france.com](http://www.pei-france.com)

## CAPTEUR DE TEMPÉRATURE POUR L'AUTOMATISATION INDUSTRIELLE

avec connecteur M12



La société britannique **Labfacility** propose un capteur de température pour l'automatisation industrielle avec un détecteur de thermomètre à résistance (RTD) à 4 fils Pt100 classe A, fonctionnant dans une plage de mesure de -75 à +250°C. Il est disponible dans une gaine en acier inoxydable 316 de 3 et 6 mm de diamètre avec

des longueurs standard de 100, 150, 200 et 250 mm. Il est fourni avec un corps simple ou avec des options à visser en filetage 1/4 BSPP, 1/2 BSPP et 1/4 et 1/2 NPT. Ce capteur est doté d'une connexion d'instrument codée M12 A à 4 broches, standard de l'industrie, adaptée aux applications de contrôle et d'automatisation des processus industriels et au remplacement des capteurs sur le terrain. Les principales applications sont l'automatisation, le remplacement sur site des capteurs, le contrôle des processus industriels, l'utilisation dans les usines pharmaceutiques et chimiques. Labfacility est le premier fabricant britannique de capteurs de température, de connecteurs de thermocouple et d'instruments de température associés et un revendeur de câbles de thermocouple.

►► 34208 sur [www.pei-france.com](http://www.pei-france.com)

## BOÎTIER DE TERRAIN SÉCURISÉ

adapté à plusieurs systèmes de bus de terrain



Le boîtier de terrain sécurisé SFB de **Schmersal**, qui pouvait déjà être intégré aux systèmes avec Profinet / Profisafe, est désormais également disponible pour les systèmes de bus EtherNet/IP avec CIP Safety et EtherCAT avec FSoE. L'avantage : le constructeur peut configurer les fonctions de sécurité d'une machine indépendamment du système de bus de terrain employé, car les trois variantes

couvrent les systèmes de commande les plus courants à l'échelle internationale. Le boîtier de terrain sécurisé de Schmersal permet de réaliser des solutions de sécurité flexibles et une installation rapide et sans erreur, et garantit une grande transparence des processus. Les interfaces d'appareillage universelles avec connecteurs M12 à 8 broches permettent le raccordement d'une multitude d'appareils de commutation de sécurité : dispositifs d'interverrouillage électroniques et électromécaniques, capteurs, boîtier de commande, rideaux lumineux ou interrupteurs. Il est possible de raccorder jusqu'à huit appareils de commutation de sécurité à un boîtier de terrain. Cela est nettement plus économique que l'équipement de chaque appareil avec une interface bus.

►► 34214 sur [www.pei-france.com](http://www.pei-france.com)

## PROGRAMMATEURS INTÉGRÉS ULTRA-RAPIDES

universels et polyvalents



Développés par le fabricant italien Algocraft, et distribués par **Cotelec** en France et en Afrique du Nord, les programmeurs intégrés de la série µISP sont des instruments professionnels ultra-rapides

dédiés à la programmation et au test des appareils. Basés sur la technologie propriétaire WriteNow, les 10 modèles de cette gamme ont la particularité de pouvoir fonctionner, soit connectés à un PC hôte grâce aux connexions incluses (RS-232, USB et LAN), soit en mode autonome. L'exécution du cycle de programmation en mode autonome peut être réalisée très simplement en appuyant sur le bouton Start ou via certaines lignes de contrôle TTL. Compatibles avec les luminaires, et bénéficiant d'une taille compacte et d'une extrême polyvalence, ces programmeurs offrent une intégration simple dans les environnements de production, les processus manuels et automatiques. Dotés d'un mode de protection et de cryptage des données, ces programmeurs sont fournis avec un interface utilisateur puissante et des utilitaires logiciels faciles à utiliser (WriteNow Project Generator) pour permettre à l'utilisateur de configurer et de contrôler aisément les instruments grâce à des procédures graphiques simples. Grâce à la technologie WriteNow, les programmeurs µISP permettent de réaliser une programmation à grande vitesse sans sacrifier la haute qualité et la flexibilité.

►► 34181 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

[www.pei-france.com](http://www.pei-france.com)

# Les câbles et chaînes porte-câbles d'Igus équipent la machinerie scénique des navires de croisière

L'ensemble des navires construits par les chantiers de l'Atlantique sont équipés de théâtres et d'équipements de loisirs conçus et installés par Videlio-HMS. Les câbles et chaînes porte-câbles sont fournis par Igus, choisis pour leur fiabilité et leur certification aux normes maritimes.

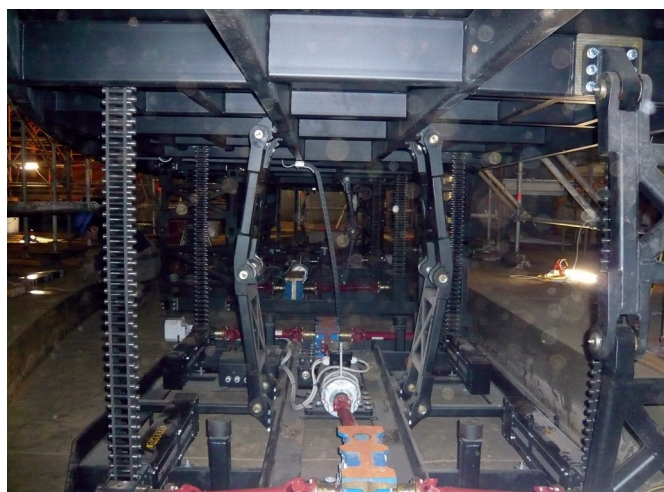
La société française Videlio, intégrateur et prestataire de services audiovisuels professionnels, n'apparaît pas aux yeux du public. Mais il se cache souvent derrière une salle de réunion et de visioconférence, un événement qui utilise écrans géants, écrans Led, vidéo projection, éclairage scénique, ou la salle de spectacle d'un navire de croisière. L'entreprise est organisée en trois unités qui couvrent les marchés de l'entreprise, de l'événementiel et de la croisière. Cette activité Cruise regroupe Videlio-HMS et Videlio-Funa et possède 100% du marché de la machinerie scénique pour navires en France. « Nous sommes spécialisés sur plusieurs systèmes installés à bord des navires de croisière, d'abord sur le système Entertainment, c'est-à-dire tous les équipements qui vont apporter de la distraction aux passagers : équipements audio, lumière, vidéo, explique Marco Baldin, directeur commercial chez Videlio-HMS. Ensuite sur la machinerie scénique, qui comprend notamment les ascenseurs. Enfin sur les systèmes pour la communication à bord du navire ».

## Un environnement en mouvement

Un navire de croisière présente plusieurs spécificités par rapport au domaine terrestre. C'est d'abord une petite ville qui regroupe jusqu'à neuf mille personnes et Videlio-HMS intervient sur différents types d'activités, avec plusieurs théâtres de tailles différentes. C'est ensuite un environnement en mouvement, avec des accélérations positives et des décélérations. Selon que l'on se trouve sur le haut ou dans le creux de la vague, les efforts à l'intérieur sont différents. Enfin, il y a pendant la construction de nombreux sous-traitants qui interviennent avec une forte co-activité, ce qui entraîne des contraintes supérieures à celles rencontrées dans un bâtiment terrestre car les endroits sont plus exigus ce qui oblige à établir des plannings extrêmement serrés et à mettre en place des méthodes et des process spécifiques pour pouvoir réaliser le montage de tous les équipements dans les délais impartis.

## La norme DNV GL, indispensable pour l'utilisation à bord

Un ascenseur de scène se présente sous la forme d'un plateau pouvant recevoir un certain nombre d'équipements, comme des haut-parleurs ou des projecteurs, ainsi que ceux liés à la sécurité de l'ascenseur lui-même. Il faut donc alimenter ces équipements par des câbles qui vont suivre la montée et la descente de l'ascenseur. Videlio-HMS a choisi les chaînes porte-câbles et les câbles Chainflex d'Igus, conçus pour les applications en mouvement. Ils sont résistants aux défaillances et bénéficient d'une



L'ascenseur montre ses dessous. Les câbles Chainflex Igus et leurs chaînes offrent de nouvelles possibilités, car Videlio n'est plus bridé par la longueur des câbles et peut imaginer de nouveaux effets.

garantie de 36 mois. Disponibles avec des gaines en différents matériaux, ils répondent aux exigences de la CEM et à celles de normes et directives telles qu'UL, CSA, VDE, EAC, CTP, Interbus et Profibus et sont disponibles avec des gaines en différents matériaux. Et il existe une gamme pour un usage maritime respectant la norme DNV GL, développée à la base pour les industries offshore.

L'ascenseur, fabriqué en Italie par Videlio-HMS arrive à Saint-Nazaire pré-assemblé à 90% et testé, mais non câblé. « Une fois embarqué à bord, nous réalisons le tirage de câbles pour mettre en liaison les armoires de puissance et de signaux et l'ascenseur, explique Marco Baldin. Le respect de la norme DNV GL est indispensable, mais il faut aussi des câbles suffisamment flexibles pour subir les mouvements sans dommages ».

Pour Videlio-HMS, les câbles Chainflex et leurs chaînes offrent de nouvelles possibilités par rapport aux enrouleurs utilisés auparavant, une technologie très différente et plus coûteuse. « Sur les ascenseurs, nous étions bridés par la longueur des câbles et nous devions trouver d'autres solutions pour les équipements qui ne pouvaient pas être installés sur un ascenseur ». Aujourd'hui, les sociétés de production qui créent les spec-







*La scène d'une salle de spectacle à bord des grands navires de croisière n'a rien à envier à celle d'un théâtre à terre. Et les produits Igus, qui respectent des normes maritimes, prennent en compte les contraintes dues au milieu.*

tacles à bord peuvent imaginer de nouveaux effets car elles ne sont plus bridées par l'impossibilité technique de véhiculer le signal ou la puissance en fonction du mouvement de l'ascenseur.

#### **Aucun problème technique en cinq ans d'utilisation 365 jours sur 365**

Le tirage de câbles dans un bateau suit des règles extrêmement strictes établies par le chantier naval qui établit un routage précis. Les câbles doivent suivre un chemin prédéfini qui tient compte de ces règles, en premier lieu de sécurité concernant l'isolation coupe-feu. Mais quand Videlio commence à travailler sur un projet, les longueurs nécessaires ne sont pas connues avec exactitude et les câbles ne seront glissés dans les chaînes porte-câbles qu'au dernier moment. « Nous avons étudié d'autres possibilités, comme le pré-équipement de l'ascenseur avec les câbles et leurs chaînes porte-câbles montés prêts à être connectés à des boîtes de jonction, explique Marco Baldin. Mais cela ajouterait un risque supplémentaire de faux contact au niveau des borniers que nous serions obligés d'ajouter. Dans la mesure du possible, nous utilisons des câbles ininterrompus de l'armoire de contrôle jusqu'à l'équipement. Chaque jonction est une source potentielle d'erreur ». Quel que soit la demande du client, Igus s'adapte, avec une offre allant du câble en touret jusqu'au câble confectionné avec les connecteurs et placé dans une chaîne porte-câbles pour faire du plug and play.

Utilisés depuis 2018, les câbles Chainflex DNV GL ont servi pour équiper au moins six paquebots fabriqués par les chantiers de l'Atlantique pour les croisiéristes MSC, Royal Caribbean Cruises et Celebrity Cruises, sans jamais rencontrer le moindre problème. Une fiabilité très importante pour des navires en fonction 365 jours par an, avec souvent deux spectacles chaque jour. « Cette fiabilité est très importante pour des raisons de sécurité car certains câbles véhiculent des données liées à l'appareil, comme pour des raisons économiques, précise Marco Baldin. Envoyer un technicien par avion lors d'une escale coûterait très cher ».

Ce dernier apprécie également la qualité du service d'Igus, pour les conseils, les informations sur les nouveaux produits, et la flexibilité d'Igus « capable de nous dépanner de quelques mètres de câble si nous avons un souci sur une longueur. Nous apprécions qu'Igus ne se contente pas de nous vendre le produit, puis d'attendre la prochaine commande. Les équipes sont toujours présentes pour répondre à nos demandes ».

►► 34206 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

Vous voulez surveiller les process de base de manière simple et fiable.

# SIMPLICITE + EFFICACITE

Grâce à notre expérience et nos connaissances techniques, nous avons développé des produits faciles à sélectionner, à installer et à entretenir.

Répondez à vos besoins dans les applications de base avec les produits de notre Sélection Fondamentale



**Liquipoint FTW23**  
Détecteur de niveau pour liquides dans l'industrie agroalimentaire

[fr.endress.com/ftw23](http://fr.endress.com/ftw23)



**Cerabar PMP23**  
Capteur de pression hygiénique avec cellule métallique

[fr.endress.com/pmp23](http://fr.endress.com/pmp23)



**Picomag**  
Débitmètre électromagnétique pour liquides conducteurs

[fr.endress.com/dma](http://fr.endress.com/dma)

Vous souhaitez en savoir plus ?  
[www.fr.endress.com/fundamental](http://www.fr.endress.com/fundamental)

►► 34200 sur [www.pei-france.com](http://www.pei-france.com)

**Endress+Hauser**

People for Process Automation

# Le blindage électromagnétique EMI pour les applications 5G gagne en efficacité

David Inman, responsable des services tests et applications chez Parker Chomerics, présente une gamme de plastiques conducteurs destinés à fournir un blindage électromagnétique EMI efficace dans les applications 5G.

Pour fournir un blindage électromagnétique EMI efficace pour les applications 5G qui évite suffisamment les perturbations et les interférences avec les appareils électroniques et les composants individuels, la science des matériaux doit réaliser des avancées importantes. La gamme Premier de types de plastiques conducteurs mise au point par Parker Chomerics et destinée à être utilisée dans les solutions de blindage électromagnétique EMI 5G constitue une formidable avancée.

Chaque type de plastique conducteur spécifique est une synthèse d'alliages de polymères thermoplastiques PC/ABS et de charges conductrices conçues pour offrir des performances électriques, mécaniques et physiques équilibrées. La technologie des charges conductrices utilise des fibres de carbone nickelé comme produit de remplissage de base, mélangé à de la poudre de nickel-graphite pour offrir des niveaux de performance élevés. Chaque matériau de remplissage possède des propriétés uniques qui aident les fabricants d'équipements et d'appareils électroniques à satisfaire aux exigences CEM du marché mondial de la 5G.

## Tests approfondis

Toute la gamme de produits Premier a été soumise au préalable à des tests approfondis concernant les caractéristiques relatives au blindage électronique EMI, en appliquant notamment les normes industrielles ASTM-D4935 et IEEE-STD-299 sur des bandes de fréquences s'étendant de 30 MHz à 40 GHz. Il existe cependant un besoin croissant de matériaux capables d'assurer un blindage électromagnétique EMI aux fréquences plus élevées qui sont propres à la 5G. Ces tests ouvraient donc une nouvelle voie. Les nouveaux tests nécessitent souvent d'utiliser



de nouvelles méthodes et de nouveaux équipements, ce qui a poussé Parker Chomerics à développer une enceinte unique de test de l'efficacité du blindage haute fréquence, connue sous le nom de « Mini Box ». Ce type de configuration test IEEE-STD-299 à petite échelle évalue l'efficacité du blindage à des fréquences allant jusqu'à 115 GHz.

Les échantillons de test moulés « de charge » et « de référence » Premier possédaient un diamètre de 133 mm. L'un des principaux avantages de cette taille d'échantillon est que le même diamètre convient aux tests permettant de s'assurer de la conformité aux normes ASTM D4935 et IEEE-STD-299 en utilisant la chambre de test principale de Parker Chomerics ou Mini Box. Un seul échantillon de test suffit par conséquent pour la collecte des données de test de 30 MHz à 110 GHz.

Un montage coaxial spécialement conçu pour tester des matériaux homogènes au-dessus d'une plage de fréquences de 30 MHz à 1,5 GHz a été utilisé dans le cadre des tests ASTM D4935. En termes de configuration, un échantillon de test était placé entre les deux moitiés du montage de test. À l'aide d'un analyseur de spectre classique, le premier test a été réalisé

*La gamme Premier de Parker Chomerics est un mélange d'alliages de polymères thermoplastiques PC/ABS et de charges conductrices.*

avec le disque de « référence », tandis que le second test d'efficacité du blindage a été réalisé sur l'échantillon de test de « charge ».

## Une efficacité de blindage impressionnante

Deux configurations différentes ont été utilisées pour les tests IEEE STD 299. Tout d'abord, la chambre principale a testé l'échantillon à des fréquences comprises entre 800 MHz et 40 GHz. Cette chambre est une enceinte en acier entièrement soudée qui mesure 3,7 x 6 m avec deux sections et une paroi commune dotée d'une trappe de visite sur laquelle l'échantillon de test a été placé. Un côté de la chambre de test contient l'équipement de test et l'antenne de transmission, tandis que l'autre côté contient l'équipement et l'antenne de réception.

La Mini Box a ensuite testé les fréquences de 50 MHz à 110 GHz à l'aide d'un analyseur de réseau Keysight N5225A. Deux mesures du coefficient de transmission ont été effectuées, l'une avec le matériel en place sur la Mini Box et l'autre sans rien entre les deux antennes (référence ouverte IEEE-STD-299).

Les résultats montrent une efficacité de blindage impressionnante pour tous les plastiques conducteurs Premier. Les fabricants et les utilisateurs finaux peuvent se fier à ces données, car Parker Chomerics met au point des montages et des méthodes de test d'efficacité du blindage de manière à reproduire le produit de revêtement conducteur utilisé dans les applications réelles.

►► 34213 sur [www.pei-france.com](http://www.pei-france.com)





## BOÎTIERS DE DISTRIBUTION DE PUISSANCE

pour les architectures 48V



**Würth Elektronik ICS**, fabricant de solutions de distribution de puissance pour les véhicules dits "Off-Road" et les véhicules commerciaux, propose ses boîtiers de distribution de puissance Redline Power Boxes en architecture 48V. Ils sont

adaptables à des applications spécifiques, intégrés dans des boîtiers standards, et économiques car nécessitant des temps de développement courts. Les systèmes 48 V représentent une alternative intéressante, tant d'un point de vue technique qu'économique, à la technologie 12/24 V et aux installations haute tension complexes. Dans le domaine de l'électromobilité, ils offrent aux concepteurs et fabricants une plus grande liberté en ce qui concerne l'intégration de consommateurs électriques puissants. Pour ce type de boîtiers, Würth Elektronik a notamment utilisé des composants adaptés à la plage de tension 48 V, tels que des connecteurs, des fusibles et des relais. La conception modulaire, la gamme de boîtiers standardisés disponibles et le circuit imprimé configurable permettent de réaliser des projets personnalisés et de réduire considérablement les délais et les coûts de développement. La conception des boîtiers vise également à simplifier l'installation et la maintenance sur le véhicule. Würth Elektronik ICS propose actuellement trois versions de boîtiers 48V : la Mini, la Twin et la 6F.

►► 34212 sur [www.pei-france.com](http://www.pei-france.com)

## CIRCUITS INTÉGRÉS DE SURVEILLANCE DE LA TEMPÉRATURE

dans les appareils électroniques



**Toshiba Electronics Europe** a considérablement élargi sa gamme de circuits intégrés de détection de surchauffe Thermoflagger avec la sortie de six autres composants, portant le total à huit. Ces dispositifs,

combinés à des thermistances à coefficient thermique positif (« positive thermal coefficient », PTC), sont destinés à détecter les augmentations de température dans les appareils électroniques. La sécurité étant primordiale dans de nombreuses applications, les circuits intégrés de détection de surchauffe Thermoflagger surveillent les températures internes pour s'assurer que les systèmes fonctionnent comme prévu, garantissant ainsi la sécurité. Les applications typiques comprennent les appareils mobiles, les appareils électroménagers, les équipements industriels et bien d'autres. Un signal Flag (PTCGOOD) très utile est disponible en version push-pull ou open-drain avec l'option de verrouillage (ou non). Ils peuvent fonctionner à une température ambiante comprise entre -40°C et +125°C. Ils fonctionnent à partir d'une tension d'alimentation (VDD) comprise entre 1,7 V et 5,5 V et présentent une faible consommation de courant aussi basse que 1,8  $\mu$ A (typ.). Toshiba a collaboré avec Murata qui recommande désormais les circuits intégrés Thermoflagger pour leur utilisation avec ses thermistances PTC.

►► 34215 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

## INTERFACE D'ALIMENTATION ET DE SIGNAL ROBUSTE

avec verrouillage rapide



**Binder**, fournisseur de connecteurs circulaires industriels, présente le Power Bayonet Connector PBC15. Sa taille correspond à un filetage M15. Ainsi, il comble le vide entre les conceptions M12 et M23 largement utilisées. Le

connecteur compact mais robuste convient particulièrement à l'alimentation électrique des moteurs triphasés ou des convertisseurs de fréquence. Il comporte 3 broches d'alimentation, par exemple pour alimenter les 3 phases sous tension d'un moteur triphasé, 2 broches supplémentaires pour la transmission du signal, ainsi qu'un contact de terre de protection. Le PBC15 est disponible chez Binder sous forme de connecteurs de câble femelles ou mâles à câbler, dans chaque cas en variante non blindée ou blindée. Grâce aux valeurs nominales de 630 V et 16 A pour l'interface d'alimentation, le connecteur circulaire convient à l'alimentation électrique de variateurs de petite et moyenne taille. Avec des valeurs nominales de 63 V et 10 A, les broches de signal peuvent être utilisées, par exemple, pour contrôler les freins ou pour interroger des paramètres de fonctionnement tels que les températures. Les applications typiques se situent dans les domaines de l'intralogistique, de l'automatisation des usines et des processus, ainsi que de l'ingénierie des machines.

►► 34217 sur [www.pei-france.com](http://www.pei-france.com)

## Technologie de fusion d'adhésif conçue pour l'industrie 4.0



### MICRON+ SERIES

Venez découvrir la solution la plus efficace pour votre ligne d'emballage

[www.meler.eu](http://www.meler.eu)

**MICRON**  
by meler

**prodpack**

21-22-23 NOVEMBRE 2023  
HALL 6 - EUREXPO LYON



Démonstrations en direct  
sur notre stand: E-110

►► 34000 sur [www.pei-france.com](http://www.pei-france.com)



# Industrial CyberSec Forum le 28 novembre 2023 à Lyon

Protégez vos infrastructures industrielles face aux cybermenaces grandissantes !

La fréquence et la sophistication des cyberattaques augmentent rapidement dans le contexte international. Et si l'on entend souvent parler de cybercriminalité dans le monde financier ou au niveau des États-nations, l'industrie représente également une cible de choix. Car tout est désormais interconnecté avec l'industrie 4.0 et la numérisation. Le processus de numérisation rapide dans les entreprises industrielles en plus d'un réseau de fournisseurs plus solide, a imposé des taux inquiétants de cyberattaques et une faible convergence des réseaux IT et OT.

## Statistiques inquiétantes sur l'état de la cyber-résilience

En ce qui concerne les cyberattaques, de nombreuses études internationales révèlent des statistiques inquiétantes sur l'état de la cyber-résilience des entreprises et des associations industrielles. Par exemple, en 2020, Fortinet (spécialiste des solutions et services en cybersécurité) a constaté que 58% des grandes entreprises industrielles ont été confrontées à une brèche de sécurité dans leurs systèmes OT au cours de l'année écoulée. De son côté, Kaspersky indique dans une étude de 2020 que 93% des entreprises estiment que leur stratégie de cybersécurité est insuffisante. De même, une étude de l'association professionnelle Agoria menée auprès de 77 entreprises manufacturières belges montre que 55% des répondants affirment n'utiliser ou n'envisager aucune norme relative à la cybersécurité OT. Enfin, l'étude indépendante du Ponemon Institute précise que 61% des entreprises affirment que des systèmes IoT obsolètes formaient le principal obstacle à la réduction des cyber-risques.



## La sécurité des réseaux industriels peut être renforcée

Toutefois, les professionnels de la cybersécurité affirment que la sécurité des réseaux industriels IT et OT peut être considérablement renforcée par l'intégration d'équipements tels que les automates programmables (PLC), les systèmes de contrôle industriel (ICS), l'internet industriel des objets (IIoT), les systèmes de contrôle et d'acquisition de données (Scada) et les systèmes de contrôle distribués (DCS).

Il est particulièrement important d'aborder la question de la cyber-résilience en France, étant donné que la région Auvergne-Rhône-Alpes est la deuxième région économique et industrielle du pays. Elle est dotée d'un fort potentiel économique, scientifique et technologique. Sa position stratégique au cœur de l'Europe lui confère un rôle de carrefour entre le nord et le sud du continent. Cette dynamique économique est renforcée par la présence de grande métropole telle que Lyon.

## Un événement incontournable

Pour cette raison, le 28 novembre 2023, le Palais de la Bourse à Lyon accueillera l'Industrial CyberSec Forum, manifestation dont PEI est parte-

naire. Un événement incontournable dédié à la protection des infrastructures industrielles dans un monde de plus en plus connecté. Les entreprises doivent faire face à des cybermenaces de plus en plus sophistiquées et fréquentes, et l'industrie 4.0 se trouve au cœur de ces enjeux. Au programme, des conférences passionnantes, des tables rondes, des rencontres d'affaires et des ateliers interactifs vous attendent pour vous permettre d'être à la pointe de la cybersécurité industrielle.

Apprenez des meilleurs experts du secteur, échangez avec vos pairs et trouvez des solutions adaptées à vos besoins. Votre participation à l'Industrial CyberSec Forum 2023 vous offrira une occasion unique de rencontre et de partage pour les spécialistes des technologies de l'information et de la communication, ainsi que pour les responsables de l'exploitation et de la sécurité des environnements industriels.

## Plus de 300 entreprises attendues

Plus de 300 entreprises sont attendues et seront représentées par les décideurs en charge des différents services des entreprises sensibilisés à la cybersécurité : responsables de la sécurité des systèmes d'information (RSSI), responsables « open innovation », directeurs des systèmes d'information (DSI), décideurs opérationnels, directeurs du marketing, directeurs techniques, responsables logistique, responsables des ressources, directeurs financiers, P-dg, directeur de la sécurité, professionnels du secteur numérique (Cloud / Datacenter, IoT et mobilité), directeurs du développement,...

Pour plus d'informations et pour vous inscrire à l'Industrial CyberSec Forum 2023, rendez-vous sur <https://industrial-cybersec.com/contact>.



# « Livre noir » du « hacker » : portrait d'un cybercriminel et guide de survie des entreprises

Le « livre noir » du « hacker » proposé en téléchargement par Prodware permet aux lecteurs d'entrer dans la tête d'un cybercriminel pour mieux comprendre sa démarche et la neutraliser.

Les dommages de la cybercriminalité équivalent à la 3<sup>e</sup> économie mondiale derrière les Etats-Unis et la Chine ! Pour les entreprises et les organisations, les attaques cyber sont parfois lourdes de conséquences. Au-delà des impacts directs (perte d'exploitation et d'activité, demande de rançon, etc.), les répercussions indirectes (dégradation de l'image de marque auprès des clients, des partenaires et des fournisseurs, dévalorisation boursière...) sont aussi très pénalisantes. Il n'est d'ailleurs pas rare qu'une cyberattaque soit suivie d'une faillite de l'entreprise dans les mois qui suivent.

## Les PME et ETI font partie des organisations les plus attaquées

Face à cette cybermenace omniprésente, toutes les entreprises ne sont pas égales : elles n'ont pas la même maturité cyber et l'équipe dirigeante n'a pas forcément pris la pleine mesure des risques. Alors que le nombre de rançongiciels recensés par l'ANSSI a atteint un très haut niveau ces dernières années, les PME et ETI font partie des organisations les plus attaquées. Si 86% des dirigeants se disent sensibles aux risques cyber, seulement 44 % des ETI font de la cybersécurité une priorité d'investissement. « 80% des chefs d'entreprise considèrent que leur entreprise est bien, voire tout à fait protégée... mais la réalité opérationnelle est bien plus nuancée ! » complète Cyril Duvivier, directeur de la sécurité et des pratiques cyber chez Prodware.

Le « livre noir » du « hacker », véritable guide de survie des entreprises, permet d'entrer dans le cerveau d'un « hacker », de mieux comprendre ses motivations et ses méthodes. Il évoque sa



vie quotidienne, son organisation, ses collègues, bref un monde pas si éloigné de celui de l'entreprise classique. Ainsi, familiarisé avec l'intimité des cybercriminels, il devient plus facile de prendre la mesure du risque et d'assurer sa cybersécurité.

## Portrait d'un hacker en 6 points

- L'organisation cybercriminelle : En tant que cybercriminel, il ne travaille pas seul. Il appartient à une organisation structurée et hiérarchisée comptant de nombreux « collaborateurs » spécialisés. Au sein de cet écosystème, chacun a sa mission avec un objectif commun : soutirer des informations et en tirer parti !
- La fiche de mission : le rôle du « hacker » est de réussir à pénétrer et à corrompre le système d'Information. Ses objectifs sont variés : obtenir une rançon, revendre des données à des tiers intéressés ou de directement des fonds.
- Le ciblage : comment va-t-il s'y prendre pour pénétrer le système d'information ? Tout simplement de la même manière qu'un cambrioleur : en scrutant l'infrastructure pour trouver une porte ouverte ou une fenêtre mal fermée. Et si l'infrastructure est suffisamment robuste pour éviter une compromission directe, il va

alors s'attaquer aux collaborateurs.

- L'attaque : Deux cas de figure se présentent : les bots automatiques scrutent nos Systèmes d'Information pour trouver des failles de sécurité que les hackers exploitent ensuite ; le « hacker » mène une analyse ciblée sur un « compte à potentiel ». Une fois que la brèche est trouvée, le cybercriminel prend tout simplement pied dans le système d'information de sa victime en vue de préparer la compromission.
- La compromission : confortablement installé chez sa victime, le « hacker » va pouvoir tirer parti de ses efforts. Selon les motivations qui l'ont poussé à agir, son plan d'action va différer : soit il détourne des fonds, soit il revend des informations sensibles ou personnelles au plus offrant sur le « dark web », soit il dépose un rançongiciel dans le système et exige une rançon pour fournir la clé de déchiffrement.
- L'extorsion : la plupart du temps, il se fait payer en cryptomonnaies sur le « dark web » : c'est anonyme, rapide et facile à utiliser. Pour la police, ces mouvements de fonds sont quasiment impossibles à suivre et les quelques traces laissées ne sont que temporaires. Sa monnaie préférée est le bitcoin. Selon Marsh, les bitcoins représentent d'ailleurs près de 98 % des paiements dans les cas d'extorsion par rançongiciel.

Le « livre noir » du « hacker » est téléchargeable sur ce lien : <https://www.prodwaregroup.com/fr-fr/documentation/livres-blancs/livre-noir-du-hacker/>.

► 34232 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

[www.pei-france.com](http://www.pei-france.com)

# Toutes les entreprises doivent se sentir concernées par la cybersécurité

**Antoine Camus, directeur cybersécurité et défense au sein de Minalogic, le pôle de compétitivité de la transformation numérique en Auvergne-Rhône-Alpes, nous présente les actions proposées au sein de ce pôle.**

## Quelles sont les actions récentes mises en place par Minalogic pour sensibiliser les entreprises à la cybersécurité ?

Nous avons entamé un grand nombre d'actions auprès des entreprises, notamment à travers de webinaires sur des thématiques et des secteurs d'activité verticaux pour que les entreprises réalisent comment la cybersécurité peut être adaptée à leur métier. En outre depuis juillet, Minalogic pilote le projet européen MinaSmart fédérant 13 partenaires (pôles, clusters et organismes de recherche) de la région pour un ensemble de 3000 adhérents. L'ambition de MinaSmart est d'accompagner les petites et moyennes entreprises traditionnelles de la région dans leur démarche de transformation numérique et leur faciliter l'accès aux solutions d'intelligence artificielle et de cybersécurité. Les entreprises pourront ainsi plus facilement sécuriser leurs systèmes d'information contre les risques d'attaques malveillantes qu'elles encourent, et de les accompagner pour trouver identifier des solutions simples, utiles et adaptées sur le marché. Notre principal travail, dans le cadre de ce projet, consiste à présenter les risques encourus par les entreprises et à les mettre en mouvement afin qu'elles adoptent une posture de cybersécurité dans le cadre d'une dynamique durable et pragmatique adaptée aux PME. Ce projet, baptisé MinaSmart financé à 50% par la Commission européenne, bénéficie d'un budget de 3,6 M€ sur une période de 3 ans. Il concerne toutes les entreprises de toutes tailles, tous les secteurs et toutes les filières métiers.

## En quoi le projet européen MinaSmart est-il novateur ?

Ce projet européen entre dans le cadre de la stratégie digitale mise en place par la

Commission européenne à travers les pôles européens d'innovation numérique (EDIH, « European Digital Innovation Hubs »). Ce sont des guichets qui aident les entreprises et les organisations du secteur public à relever les défis numériques et à devenir plus compétitives. Des EDIH ont été établis dans chacune des régions. Avec ce projet notre ambition est aussi de nouer des liens avec plusieurs structures en France spécialisées dans la cybersécurité. Nous avons déjà développé des collaborations étroites avec le pôle d'excellence cybersécurité de Bretagne afin de mettre en avant les compétences de nos PME régionales

## Par quelles démarches les entreprises doivent-elles commencer pour assurer la cybersécurité de leur système d'information ?

Nous proposons tout un parcours de sensibilisation et de résilience aux risques liés à la cybersécurité. Les entreprises doivent commencer par comprendre leur niveau de maturité initial au travers d'un premier diagnostic. Fortes de cette analyse, l'enjeu sera de constituer une feuille de route adaptée afin d'assurer durablement la sécurité économique de leurs actifs stratégiques. Le dirigeant joue un rôle clé lors de cette première étape car il doit être sponsor de ce projet d'entreprise et impliquer chaque collaborateur. Nous procédons en complément à des tests de pénétration pour évaluer la capacité d'entrer dans l'entreprise et nous proposons un plan de remédiation phasé avec un responsable de sécurité du système d'information externalisé. Certaines entreprises font parfois des audits, mais la grande majorité d'entre elles s'arrêtent là. Nous insistons sur



*Antoine Camus, directeur cybersécurité et défense au sein de Minalogic : « Nous insistons sur la nécessité de réaliser une action continue, pragmatique et adaptée aux PME ».*

la nécessité de réaliser une action continue, pragmatique et adaptée aux PME.

## Est-ce que nous assistons néanmoins à une prise de conscience de l'importance de la cybersécurité par les entreprises ?

Les entreprises sont de plus en plus conscientes des risques encourus à travers des témoignages de certaines d'entre elles qui ont subi des attaques. Elles ont conscience que les attaques sont massives, visant chaque entreprise sans distinction, les exposant toutes à devenir des victimes







*Minalogic apporte une réponse simple et efficace pour aider les adhérents du pôle (et plus largement les sociétés de la région Auvergne-Rhône-Alpes) à évaluer leur exposition aux risques.*

potentielles. La bonne nouvelle c'est qu'il y a des programmes adaptés pour chacun d'eux, et qu'il existe des aides. Cependant, cela ne bouge pas encore assez vite. Le regard porté sur la cybersécurité doit encore évoluer. Au-delà de la nécessaire protection, la sécurité économique aide les entreprises à se structurer, se différencier de la concurrence et conquérir de nouveaux marchés. Seules les entreprises impliquées dans cette démarche pourront postuler aux consultations et remporter des contrats. Deux réglementations européennes, la NIS 2 (Network and Information Systems Directive) et Dora (Digital Operational Resilience Act) imposeront de nouvelles exigences en matière de cybersécurité aux donneurs d'ordre, et par ricochet, à leurs sous-traitants, et si les PME sous-traitantes ne sont pas entrées dans cette démarche de cybersécurité, elles ne pourront plus répondre aux appels à projets. L'effort à fournir sera alors d'autant plus important qu'il n'aura pas été anticipé en amont.

#### Quel est le coût d'une démarche de cybersécurité et comment le diagnostic se déroule-t-il ?

Le coût dépend de l'état actuel dans lequel se trouve l'entreprise, de sa taille, des exigences de son secteur d'activité et de ses clients. Le diagnostic initial, à savoir l'établissement de la cartographie des risques, n'est pas très onéreux au regard des enjeux. Il revient entre 3000 et 5000 € et consiste en une analyse complète des procédures internes et externes ainsi qu'un examen des possibilités de pénétration. Toute PME qui a conscience du danger doit pouvoir se l'offrir. Il s'agit par exemple d'analyser l'or-

ganisation de l'entreprise concernant la gestion des données sur la base du référentiel ISO 27001, les systèmes de protection mises en place, les autorisations délivrées aux collaborateurs, les procédures de stockage des données, la facilité avec laquelle il est possible d'entrer dans l'entreprise... Les tests de pénétration utilisent les mêmes techniques que celles qui sont utilisées par les personnes malveillantes. Au total, plus de 130 points de contrôles sont vérifiés. Tous les détails de ce dispositif sont à retrouver sur le site de Minalogic(\*).

#### Quelles sont les principaux types d'attaques ?

Les possibilités d'attaques sont nombreuses et peuvent par exemple passer aussi bien par la messagerie, les objets connectés, le site internet... En revanche 80% des attaques sont effectuées via du phishing, d'où la nécessité de sensibiliser et former le personnel. Des attaques massives se produisent également sur les sites Internet les plus vulnérables, c'est-à-dire ceux qui ont été identifiés comme étant les plus vulnérables. Avec l'essor de l'IoT et des capteurs connectés, l'entreprise industrielle multiplie les points d'entrée qui sont autant de possibilités d'attaques. La technique la plus simple pour un hacker consiste à scanner toutes « les portes d'entrée » et de s'engouffrer dans l'entreprise via l'une d'elles. Enfin, les ransomwares se développent, avec des rançons adaptées à la surface financière de l'entreprise visée. Le seul moyen de s'en sortir est alors d'utiliser les sauvegardes et de tout réinstaller afin de restaurer le système d'information et de remettre en route la chaîne de production.

#### L'essor de l'intelligence artificielle accroît-il les menaces ?

Un outil tel que ChatGPT peut apprendre à une personne malveillante comment rédiger un mail d'attaque. Mais il peut aussi apprendre à un dirigeant comment se protéger.

#### Quelles sont les bases d'une protection contre les attaques ?

Avant tout du bon sens. Il est tout essentiel de ne pas télécharger de logiciels pirates, de faire en sorte que les logiciels utilisés soient à jour, de s'équiper de logiciels antivirus et antispham et de disposer d'un gestionnaire de mots de passe. Il faut enfin ne pas rester seul face à cette complexité grandissante. Les prestataires informatiques sont des alliés au quotidien et faire appel à un tiers de confiance pour établir un diagnostic permet d'établir un état des lieux fiable et objectif.

➔ 34221 sur [www.pei-france.com](http://www.pei-france.com)

(\*) <https://www.minalogic.com/services/developper-mon-business/protéger-votre-entreprise-et-votre-propre-intellectuelle-le-label-de-securite-economique/>

## LABFACILITY

[www.labfacility.fr](http://www.labfacility.fr)

### DÉTECTEURS RTD FILM PLAT

[sales@labfacility.com](mailto:sales@labfacility.com)

Disponible en  
classe A, B ou  
1/3 DIN



➔ 34193 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

[www.pei-france.com](http://www.pei-france.com)

# Près de la moitié des entreprises françaises auraient déjà été victimes de cyber-attaques

Le dernier rapport annuel « Human Risk Review », publié par SoSafe, indique que 46 % des entreprises en France ont été victimes d'au moins une cyberattaque au cours des trois dernières années.

Selon le dernier rapport annuel, « Human Risk Review » publié par SoSafe, qui propose des actions de sensibilisation à la cybersécurité, près de la moitié des entreprises en France (46 %) ont été victimes d'une cyberattaque au cours des trois dernières années, 21 % admettent même que ce fut le cas à plusieurs reprises. En revanche, seule une entreprise sur trois (30 %) se dit disposée à payer une rançon, un chiffre très bas en comparaison avec nos voisins européens : les Pays-Bas sont les plus susceptibles d'accepter de payer avec 46 % de ses entreprises concédant y avoir été contraintes, suivis par l'Allemagne (45 %), l'Autriche (43 %) et le Royaume-Uni (38 %).

Ce rapport, basé sur un sondage réalisé auprès de plus de 1 000 responsables de la sécurité des systèmes d'information (RSSI) de six pays européens (France, Allemagne, Grande-Bretagne, Autriche, Pays-Bas et Suisse), sur des entretiens d'experts et utilisant plus de 8,4 millions de données issues de la plateforme de sensibilisation à la cybersécurité de SoSafe, vise à établir un état des lieux des cybermenaces actuelles et évaluer la culture d'entreprise en matière de cybersécurité pour y faire face.

## Des cyberattaques de plus en plus diversifiées

L'étude révèle que 76 % des RSSI français interrogés sont stressés par le risque de cyberattaques. La plupart d'entre eux considèrent que les dernières innovations en matière d'intelligence artificielle (83%), la situation géopolitique actuelle (82%), et le travail hybride (77%) ne font qu'aggraver les risques de cybermenaces. Un répondant sur deux (49%) considère même que la menace va empirer au cours des douze prochains mois.

Les attaques par malware, en particulier, sont les plus dangereuses, selon 41% des répondants français. Les actes de piratage contre les chaînes d'approvisionnement sont également considérés comme un risque important pour 81% des RSSI. Ainsi, 18% des organisations interrogées ont déjà été victimes de ce type d'attaque et 81% reconnaissent que leur propre sécurité dépend des normes de sécurité de leurs partenaires. Les attaques par phishing restent une menace importante, renforcées par de nouvelles innovations en matière de manipulation émotionnelle. Ces attaques sont la deuxième menace la plus importante pour la cybersécurité des entreprises françaises : 35 % d'entre elles admettent en avoir déjà été victime. Selon 71% des RSSI français interrogés, les mails sont le moyen le plus utilisé par les cybercriminels pour tenter d'attaquer leurs organisations. Ainsi, pour 82% d'entre eux, ce type d'attaque et la manipulation émotionnelle des employés constituent un risque.



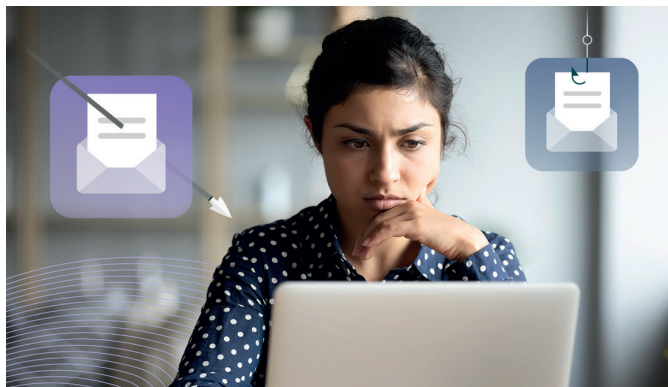
« Nous constatons que les entreprises prennent souvent des mesures, mais seulement à l'issue d'une attaque », précise Jean-Baptiste Roux, vice-président de Sosafe en charge du développement international.

## Une personne sur trois clique sur des pièces jointes ou des liens compromis

En outre, les données issues de la plateforme de sensibilisation SoSafe confirment que la menace est élevée : une personne sur trois (31%) clique sur des pièces jointes ou des liens compromis lorsqu'elles sont ciblées par une attaque via phishing. Les mails malveillants qui ont comme objets « Voiture endommagée » ou « Invitation à l'équipe » sont les plus susceptibles d'inciter les destinataires à les ouvrir, cliquer ou même saisir des informations personnelles sur un autre site web. Par ailleurs, les employés semblent particulièrement sensibles aux tactiques d'ingénierie sociale qui déclenchent des émotions fortes, telles que la pression (24%), l'autorité (28%) ou les appels financiers (18%).

« La méthode des attaques par phishing reste la plus utilisée par les cybercriminels car elle est la plus performante sur le plan humain. Le





fait que, selon nos données, une personne sur trois tombe dans le piège d'un mail de phishing, peut s'expliquer par les possibilités illimitées de personnalisation de ce type d'email. Bien souvent, les destinataires n'y sont pas préparés. Les cybercriminels sont maintenant en mesure d'utiliser des informations personnelles pertinentes collectées sur les réseaux sociaux, de rebondir et d'instrumentaliser l'actualité afin de déclencher des émotions fortes ou encore d'utiliser l'IA pour imiter des images, des vidéos ou encore des voix. Pour les personnes malveillantes souhaitant mettre au point de nouvelles stratégies et mener à bien ce type d'attaques, cette créativité est désormais devenue la norme » précise Niklas Hellemann, P-dg et fondateur de SoSafe.

#### La sensibilisation à la cybersécurité est devenue un enjeu prioritaire

Plus de deux tiers des RSSI en France (69%) estiment qu'au sein de leurs équipes, le niveau de conscience face aux risques est élevé. De surcroît, 68 % estiment que les investissements dans ce domaine sur les dix-huit prochains mois vont augmenter. Le développement d'une culture de la cybersécurité est ainsi une priorité pour 94% des entreprises, encouragé par le fait que les équipes dirigeantes y accordent une plus grande importance, selon 66% des personnes interrogées.

« Le fait que les entreprises sont de plus en plus conscientes de la nécessité d'investir dans la sensibilisation aux risques cyber, et que cette prise de conscience ait également atteint la direction de l'entreprise, représente une évolution positive. Toutefois, nos données comportementales actuelles démontrent qu'il reste encore beaucoup à faire : environ 31% des personnes cliquent sur des mails de phishing, et 52% d'entre elles divulguent même des données confidentielles. Ainsi, même si les employés comprennent mieux qu'avant l'importance de la cybersécurité, il reste encore du travail afin que les bons comportements perdurent sur le long terme. Il est donc nécessaire de renforcer l'autodéfense numérique des entreprises pour lutter contre la cybercriminalité. » ajoute Niklas Hellemann.

« Nous constatons que les entreprises prennent souvent des mesures, mais seulement à l'issue d'une attaque. Or, les dégâts s'avèrent déjà importants et difficiles à réparer lorsque le mal est fait. La prévention est de loin la meilleure solution. Heureusement, la réglementation va de plus en plus nous aider à sensibiliser les dirigeants d'entreprises. Le référentiel 27001 et la directive européenne NIS 2 imposent la mise en place d'actions de sensibilisation à la cybersécurité et l'obligation de se conformer à cette directive est prévue dès le 17 octobre 2024 », précise Jean-Baptiste Roux, vice-président de Sosafe en charge du développement international.

► 34222 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

## ROUTEURS CELLULAIRES SÉCURISÉS

pour renforcer la sécurité des réseaux d'infrastructure critiques



**Moxa** présente le routeur OnCell G4302-LTE4 qui vient compléter sa gamme de routeurs cellulaires sécurisés. Ces équipements intègrent un logiciel de sécurité conforme aux normes CEI 62443-4-2, qui optimise les performances et

accélère la correction des vulnérabilités. Leur respect des certifications sans fil mondiales permet en outre des communications sécurisées pour diverses applications industrielles. Intégré au routeur OnCell G4302-LTE4, le logiciel MXsecurity offre des fonctionnalités centralisées de sécurité et de gestion des réseaux permettant de configurer et de surveiller les équipements à distance. Les alertes et notifications en temps réel accélèrent l'identification et la résolution des problèmes. La conformité à la norme CEI 62443-4-2 et les fonctionnalités avancées comme le démarrage sécurisé, le réseau privé virtuel (VPN) et la traduction des adresses réseau (NAT) protègent les données et les réseaux contre les cybermenaces. Grâce à la redondance WAN intégrée et à la technologie GuaranLink, le routeur OnCell G4302-LTE4 permet de rétablir rapidement la connexion, limitant ainsi les périodes d'indisponibilité et les interruptions de l'activité. Avec sa fiabilité adaptée aux besoins de l'industrie, il convient aux zones dangereuses.

► 34223 sur [www.pei-france.com](http://www.pei-france.com)

## SOLUTION DE SENSIBILISATION À LA CYBERSÉCURITÉ

avec une approche dédiée à l'industrie



**Conscio Technologies**, éditeur du logiciel « Sensiwave », propose une solution complète en matière de sensibilisation cybersécurité et accompagne les RSSI, DSI et DPO dans la mise en œuvre de leur stratégie de sensibilisation en ligne. La société met en usage une démarche de « sensibilisation

impliquante » qui se traduit par la mise en œuvre de 12 techniques de psychologie de la persuasion et de l'engagement, appliquées à la sensibilisation cybersécurité. Elle a développé une approche sectorielle qui consiste à proposer des contenus adaptés aux différents secteurs identifiés : santé, collectivités territoriales, industrie et vente au détail. La sécurité des systèmes industriels est devenue un véritable enjeu. Par conséquent, grâce à son approche dédiée au secteur de l'industrie, Conscio Technologies propose des contenus adaptés et co-construits avec des DSI et des ingénieurs production du secteur. Des vidéos explicatives, riches et complètes sont mises à disposition pour les automaticiens. Le contenu des opérateurs est plus spécifique avec des vidéos interactives au format court (micro-learning) et ludiques avec des mises en situation d'un risque.

► 34230 sur [www.pei-france.com](http://www.pei-france.com)



# Accélérer la convergence de l'intelligence artificielle et de la sécurité

Intel présente une approche définie par logiciel et accélérée par le silicium, fondée sur l'ouverture, le choix, la confiance et la sécurité.

Au cours de la deuxième journée d'Intel Innovation, en septembre 2023, Greg Lavender, directeur technique d'Intel, a présenté un aperçu détaillé de la manière dont la philosophie de l'écosystème ouvert d'Intel, axée sur les développeurs, fonctionne pour garantir que les opportunités de l'intelligence artificielle (IA) soient accessibles à tous. Les développeurs désireux d'exploiter l'IA sont confrontés à des défis qui entravent le déploiement à grande échelle de solutions pour le client et la périphérie, le centre de données et l'informatique en nuage. Intel s'engage à relever ces défis avec une approche large, définie par le logiciel et accélérée par le silicium, fondée sur l'ouverture, le choix, la confiance et la sécurité.

## Faciliter le déploiement de l'IA grâce à la confiance et à la sécurité

Greg Lavender a souligné l'engagement d'Intel en matière de sécurité de bout en bout, ce qui inclut l'Intel Transparent Supply Chain pour la vérification de l'intégrité du matériel et des microprogrammes, et la garantie d'un calcul confidentiel pour aider à protéger les données sensibles dans la mémoire. Aujourd'hui, Intel renforce la sécurité de ses plates-formes et la protection de l'intégrité des données avec plusieurs outils et services, dont la disponibilité générale d'un nouveau service d'attestation.

Ce service est le premier d'un portefeuille de logiciels et de services de sécurité appelé Intel Trust Authority. Il offre une évaluation unifiée et indépendante de l'intégrité de l'environnement d'exécution de confiance et de l'application des politiques, ainsi que des enregistrements d'audit, et il peut être utilisé partout où l'informatique confidentielle Intel est déployée, y compris multi-cloud, hybride, sur site et à la



Greg Lavender, directeur technique d'Intel, a souligné l'engagement d'Intel en matière de sécurité de bout en bout.

périphérie. Intel Trust Authority deviendra également une capacité intégrale pour permettre l'IA confidentielle, en aidant à garantir la fiabilité des environnements informatiques confidentiels dans lesquels la propriété intellectuelle et les données sensibles sont traitées dans des applications d'apprentissage automatique.

## Un écosystème ouvert

Des organisations du monde entier utilisent l'IA pour accélérer les découvertes scientifiques, transformer les entreprises et améliorer les services aux consommateurs. Cependant, l'application pratique des solutions d'IA est limitée par des défis difficiles à surmonter pour les entreprises, qu'il s'agisse d'un manque d'expertise interne et de ressources insuffisantes pour gérer correctement le pipeline de l'IA (y compris la préparation et la modélisation des données) ou de plates-formes propriétaires coûteuses dont la maintenance est longue et coûteuse.

Intel collabore avec les principaux fournisseurs de logiciels Red Hat, Canonical et SUSE pour

fournir des distributions optimisées pour Intel de leurs logiciels d'entreprise afin de garantir des performances optimisées pour les dernières architectures Intel. Greg Lavender a été rejoint par Gunnar Hellekson, vice-président et directeur général de l'activité Red Hat Enterprise Linux, pour annoncer une collaboration élargie qui verra Intel contribuer au support en amont de l'écosystème Red Hat Enterprise Linux (RHEL) à l'aide de CentOS Stream. Intel continue également de contribuer aux outils et cadres d'apprentissage automatique et d'IA, notamment PyTorch et TensorFlow.

## Protéger les modèles d'IA contre l'altération, la manipulation et le vol

Alors que le monde s'appuie de plus en plus sur l'IA pour résoudre des problèmes vastes et complexes et obtenir de véritables résultats commerciaux, il est de plus en plus nécessaire de protéger les modèles d'IA, les données et les plateformes sur lesquelles ils s'exécutent contre l'altération, la manipulation et le vol. Le chiffrement entièrement homomorphe (FHE) permet d'effectuer des calculs directement sur des données chiffrées, même si les mises en œuvre pratiques sont limitées par la complexité des calculs et la surcharge. Intel a déclaré qu'elle prévoyait de développer un circuit intégré spécifique à l'application (Asic) afin de réduire le surcoût de performance d'un million de fois associé à une approche FHE uniquement logicielle. En outre, l'entreprise lancera la version bêta d'une boîte à outils logicielle pour l'informatique cryptée, qui permettra aux chercheurs, aux développeurs et aux communautés d'utilisateurs d'apprendre et d'expérimenter le codage FHE.

►► 34225 sur [www.pei-france.com](http://www.pei-france.com)



## MICROCONTRÔLEUR 32 BITS

intégrant un module de sécurité matériel



Pour permettre aux concepteurs d'intégrer facilement la sécurité dans leurs applications,

**Microchip** annonce une famille de microcontrôleurs PIC32CZ CA 32 bits avec un processeur

Arm Cortex-M7 300 MHz, un module de sécurité matérielle (HSM) intégré et une large gamme d'options de connectivité et de mémoire Flash pour une flexibilité accrue. La famille de microcontrôleurs PIC32CZ CA comprend le PIC32CZ CA90 avec un HSM ou le PIC32CZ CA80 sans HSM intégré. Le HSM du PIC32CZ CA90 est une solution monolithique qui offre une sécurité avancée pour les applications industrielles et grand public. Le HSM fonctionne comme un sous-système sécurisé avec un microcontrôleur séparé intégré qui exécute le micrologiciel et les fonctionnalités de sécurité, notamment le boot sécurisé par hardware, le stockage des clés, l'accélération cryptographique, un véritable générateur de nombres aléatoires. Les microcontrôleurs PIC32CZ CA peuvent être configurés à l'aide d'une large gamme d'options de connectivité, notamment USART/UART, I2C, SPI, CAN FD, USB haut débit et Gigabit Ethernet. L'option Ethernet comprend le pontage audio-vidéo (AVB) et le protocole PTP (Precision Time Protocol) basés sur la norme IEEE 1588. Ces produits sont évolutifs avec 2, 4 ou 8 Mo de mémoire Flash intégrée, 1 Mo de mémoire SRAM et de code de correction d'erreur (ECC) pour atténuer la corruption des données.

►► 34227 sur [www.pei-france.com](http://www.pei-france.com)

## PASSERELLES INDUSTRIELLES D'ACCÈS À DISTANCE SÉCURISÉ

par Ethernet, Wi-Fi ou liaison cellulaire



Grâce à la sécurité intégrée du matériel, la gamme Cosy+ de **HMS Networks** permet d'accéder sans risque et à distance aux machines reposant sur des automates pour réaliser des tâches de mise en service, de dépannage et de programmation en ligne. Avec la version Wireless de Cosy+, les utilisateurs peuvent se connecter à leurs machines par Ethernet, Wi-Fi ou liaison cellulaire en fonction de la situation industrielle. L'accès à distance sécurisé garantit une prise en charge efficace et durable des machines. L'accès à distance aux passerelles Ewon Cosy+ s'effectue via Talk2M, premier service cloud industriel indépendant au monde avec plus de 400 000 passerelles Ewon connectées. Faisant

suite au lancement de la version Ethernet de Cosy+ l'année dernière, Cosy+ Wireless répond à la demande croissante d'accès sans fil sécurisé aux machines. Cette demande est stimulée par la nécessité d'accroître la productivité tout en préservant la sécurité et la durabilité des opérations.

►► 34224 sur [www.pei-france.com](http://www.pei-france.com)

## SOLUTION DE DÉTECTION ET DE SURVEILLANCE DES MENACES

pour l'Internet des objets



**CrowdStrike**, spécialiste de la protection des postes de travail et des applications sur le cloud, de l'identité et des données, dévoile CrowdStrike Falcon Insight for IoT, solution EDR/XDR pour les applications

XIoT (Internet étendu des objets). Disponible via la plateforme CrowdStrike Falcon, elle offre les capacités reconnues de protection, de détection et de réponse de CrowdStrike aux IoT, OT, appareils médicaux, IoT industriel et appareils connectés à tous les niveaux de l'entreprise. Ainsi, les clients sont désormais en mesure de sécuriser leur organisation avec la même plateforme prenant en compte l'XIoT, les terminaux informatiques, les applications cloud natives, les identités et les données. La convergence de l'IT-OT conduit les équipes chargées de la sécurité et de la prévention à sécuriser les systèmes d'infrastructures critiques. Cependant, les solutions de sécurité IT traditionnelles ne sont pas compatibles avec les actifs XIoT, manquent de contexte pour une prévention et une détection efficaces des menaces, et perturbent les opérations. En collectant et en exploitant le contexte spécifique des actifs pour conduire une politique de prévention des menaces XIoT sur mesure et une détection de haute-fidélité, CrowdStrike Falcon Insight for IoT permet une transformation numérique des systèmes opérationnels OT sécurisée et atténue les menaces critiques.

►► 34226 sur [www.pei-france.com](http://www.pei-france.com)



Avec le **VISOR® Robotic**, votre robot pourra tout faire :

Pick & Place  
Localisation 3D pour AGV  
Contrôle d'assemblage  
Lecteur de code

►► 34202 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

[www.pei-france.com](http://www.pei-france.com)

# Wi-Fi 6 : répondre aux besoins changeants des usines intelligentes

**Pelle Svensson, responsable du développement, en charge des produits radio courte portée chez u-blox explique la manière dont le Wi-Fi continue d'évoluer pour rester à la hauteur du défi posé par les usines intelligentes.**

Lorsque le Wi-Fi a été déployé pour la première fois dans les usines connectées, sa tâche était simple : faire en sorte que quelques appareils communiquent entre eux. Aujourd'hui, la situation est complètement différente. Il y a à peine dix ans, l'usine intelligente ressemblait à une place vide. Aujourd'hui, elle ressemble davantage à un marché animé. Le lieu est le même, mais le contexte a radicalement changé. Comme sur un marché bruyant, l'environnement est fort encombré par les ondes et les appareils doivent se donner beaucoup de mal pour se faire entendre.

Heureusement, les technologies sans fil ont continué à évoluer pour répondre aux besoins de plus en plus exigeants des marchés qu'elles desservent. Et le Wi-Fi ne fait pas exception. La numérisation croissante des usines et les nouveaux cas d'utilisation augmentent les demandes en Wi-Fi, la technologie sans fil qui achemine environ 45% du trafic IP mondial et 60 à 80% du trafic sans fil.

## Le Wi-Fi a beaucoup évolué

Le Wi-Fi a beaucoup évolué depuis l'époque où, il y a seulement deux décennies, il ne dépassait pas les 54 Mbps. En 2009, le Wi-Fi 4, ou IEEE 802.11n comme on l'appelait à l'époque, a permis une augmentation considérable du débit, avec l'introduction de la bande 5 GHz dans IEEE 802.11a et des débits de données plus élevés dans les deux bandes. La rétrocompatibilité des points d'accès Wi-Fi 4 avec les appareils dotés d'anciennes versions de Wi-Fi a contribué à stimuler l'adoption de cette technologie.

En 2013, le Wi-Fi 5, ou IEEE 802.11ac, a permis d'améliorer encore les performances, avec un débit maximal de 6,8 Gbit/s, et un fonctionnement limité à la bande 5 GHz. Plus récemment,

le Wi-Fi 6 a poursuivi l'augmentation des performances sur tous les fronts, en particulier sa capacité à gérer plus efficacement plus de trafic provenant d'un plus grand nombre de clients. C'est pourquoi il est parfois également appelé High-Efficiency Wireless (HEW).

Les avancées innovantes apportées par le Wi-Fi 6 répondent aux exigences actuelles en termes de débit élevé (près de 10 Gbit/s), tout en offrant des performances fiables à longue portée, une faible latence, une consommation d'énergie minimale, la coexistence et un transfert rapide.

## Les attentes de l'industrie en matière de Wi-Fi

Chaque version de la norme Wi-Fi ayant permis d'atteindre de nouveaux sommets en termes de performances, la technologie a trouvé sa place dans des applications de plus en plus sophistiquées et exigeantes. Dans le même temps, la demande en termes d'améliorations de la norme n'a cessé de croître pour répondre aux besoins émergents en matière de communication sans fil, tels ceux qui sont devenus courants dans les déploiements industriels.

La haute disponibilité est primordiale dans les usines où les temps d'arrêt se traduisent directement par une perte de revenus. Dans les environnements RF encombrés, cela inclut la robustesse face aux interférences provenant des autres appareils, ainsi qu'un débit élevé, permettant de raccourcir les temps de transmission et de libérer rapidement de la bande passante après chaque communication. Garantir l'évolutivité - la capacité de connecter des clients supplémentaires au réseau sans avoir à ajouter de points d'accès - est majeure car le Wi-Fi offre une connectivité réseau à un nombre sans cesse croissant d'appareils.

Des temps de réponse rapides sont essentiels



*Pelle Svensson, responsable du développement, en charge des produits radio courte portée chez u-blox.*

pour les systèmes d'automatisation industrielle utilisés, par exemple, pour orchestrer des processus dans les chaînes de production complexes. Comme de plus en plus d'appareils mobiles, des robots aux outils électriques intelligents, sont connectés au réseau, la fluidité itinérante (« seamless roaming ») gagne en importance pour éviter de longues tentatives de reconnexion lorsque l'appareil entre dans la zone couverte par un nouveau point d'accès. De plus, pour simplifier les opérations et maintenir des faibles coûts, il est important que la mise en service et la maintenance soient faciles.

## Avantages du Wi-Fi 6

Si le Wi-Fi 4 offrait un « haut débit » et que le Wi-Fi 5 apportait un « très haut débit », le Wi-Fi 6, dont la première version est sortie en 2018,







était axé sur la « haute efficacité ». Le saut de 6,8 Gbit/s à 9,6 Gbit/s peut être moins spectaculaire que certaines augmentations d'ordre de grandeur lors des versions précédentes. Mais là où le Wi-Fi 6 brille vraiment, c'est dans son utilisation plus efficace de la bande passante disponible, qui permet d'accueillir plus de clients par point d'accès sans dégrader les performances du réseau.

Une série d'innovations technologiques a été déterminante pour gérer efficacement plus de clients :

- L'accès multiple par répartition orthogonale de la fréquence multi-utilisateurs (Multi-user orthogonal frequency division multiple access, MU-OFDMA), est une technique utilisée pour découper la bande passante disponible en unités de ressources de tailles variables, ce qui donne aux points d'accès la souplesse nécessaire pour desservir simultanément plusieurs clients avec les ressources dont ils ont précisément besoin. MU-OFDMA quadruple le nombre de clients qu'un nombre donné de points d'accès peut gérer.
- La technologie Multi-user multiple input multiple output (MU-MIMO), permet aux points d'accès de diriger simultanément des flux de données uniques vers plusieurs clients, à la fois en liaison montante et en liaison descendante.
- La modulation d'amplitude en quadrature 1024 (1024 QAM) permet d'encoder plus d'informations sur chaque symbole. Le Wi-Fi 6 peut regrouper 10 bits par symbole, soit une capacité 25 % supérieure à celle du Wi-Fi 5, qui utilisait 256 QAM.
- De plus, la coloration BSS (basic service set)

permet de s'assurer que les canaux de « couleur différente » n'interféreront pas les uns avec les autres.

- Enfin, le temps de réveil de cible (« target wake time », TWT) permet aux appareils d'économiser les batteries et d'augmenter l'autonomie.

#### Exploiter le spectre 6 GHz avec le Wi-Fi 6E

Pour surmonter la principale limitation des ressources, à savoir le spectre disponible, les agences de régulation telles que la FCC américaine ont ouvert la bande 6 GHz aux communications Wi-Fi sans licence, doublant (ou plus dans certains cas) la quantité de spectre précédemment disponible sur les bandes 2,4 et 5 GHz combinées. Les points d'accès et les terminaux capables d'utiliser les 1200 MHz du nouveau spectre seront étiquetés Wi-Fi 6E.

Les avantages de la bande 6 GHz incluent la proximité de la bande 5 GHz, déjà largement utilisée, ainsi qu'une abondance de canaux sans chevauchement et dont la taille est variable. Et parce que le nouveau spectre est encore largement inexploité, les appareils n'auront pas à faire face à de précédents clients encombrant les ondes.

Le Wi-Fi est devenu un pilier des usines intelligentes, la technologie sans fil de prédilection, souvent complétée par la technologie Bluetooth, ainsi que des technologies de communication cellulaire propriétaires ou non. Le Wi-Fi 6 renforcera probablement sa position grâce aux nombreuses nouvelles fonctionnalités énumérées ci-dessus.

➔ 34211 sur [www.pei-france.com](http://www.pei-france.com)

## OUR SOLUTION. YOUR SUCCESS.

Une grande expertise pour  
chaque application.



- ▶ Haute efficacité énergétique
- ▶ Réduction des émissions de CO<sub>2</sub>
- ▶ Découvrez votre potentiel d'économies

**NORD**  
DRIVESYSTEMS

NORD Réducteurs  
Tel +33 1 49 63 01 89  
[france@nord.com](mailto:france@nord.com) | [www.nord.com](http://www.nord.com)

➔ 33945 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

# Un service personnalisé d'approvisionnement en pièces détachées

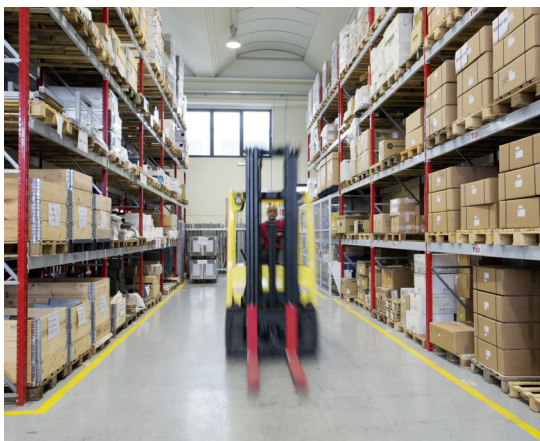
**Antares Vision fournit à la société suisse Ferring, spécialiste de la médecine reproductive, un système d'approvisionnement en pièces détachées pour augmenter l'efficacité de son processus de production.**

Née en 2015, la collaboration se développe entre Ferring Pharmaceuticals, spécialiste de la médecine reproductive, santé maternelle et domaines spécifiques de la gastro-entérologie et de l'urologie, et Antares Vision Group, partenaire technologique dans la numérisation des produits et des chaînes d'approvisionnement, à la pointe de la traçabilité, de l'inspection et de la gestion intégrée des données.

Après une première approche suite à l'entrée en vigueur de la réglementation sur la sérialisation, le groupe Ferring utilise actuellement les solutions d'Antares Vision Group sur 23 lignes dans différentes usines en Suisse, États-Unis, Chine, République tchèque, Israël, Écosse et Indonésie.

## Des délais d'approvisionnement réduits de 90%

Grâce à la collaboration avec Antares Vision Group, le groupe Ferring a fortement réduit les délais d'approvisionnement en pièces détachées. Avec des processus de chaîne d'approvisionnement intégrés, la disponibilité de la quantité minimale en stock est toujours garantie et les opérations de maintenance ont augmenté en efficacité. « Pour les pièces détachées, les délais d'approvisionnement sont réduits de 90%. C'est l'un des principaux avantages de notre collaboration avec Antares Vision Group entamée en 2015 ! », déclare Fernando Monteiro, directeur des technologies opérationnelles chez Ferring Pharmaceuticals Group. « Nous avons traversé des périodes difficiles dans un monde de sérialisation en pleine croissance. Les réglementations ont évolué au fil des années et ont eu un impact sur notre planification de la production, la rendant parfois plus complexe », ajoute-t-il.



## Des pièces de rechange de Ferring sont stockées chez Antares Vision en Italie

Ferring Pharmaceuticals et Antares Vision Group ont développé conjointement des solutions personnalisées pour améliorer les opérations de maintenance.

D'une part, de nombreux sites de Ferring utilisent les mêmes composants - cela est préférable car disposer de pièces de rechange différentes pour chaque site serait extrêmement coûteux. D'autre part, la pénurie de stocks mettrait en péril la continuité des activités. Aussi, Antares Vision Group et Ferring ont mis en place une liste de pièces de rechange capables de couvrir les besoins des différentes usines impliquées. Ces composants sont stockés au siège d'Antares Vision Group en Italie et peuvent être expédiés dans le monde entier à tout moment ! Grâce à cet accord international solide et à la collaboration étroite entre les deux entreprises, Ferring Pharmaceuticals a pu répondre aux demandes spécifiques et garantir à chaque fois le respect des normes réglementaires de chaque pays desservi.

## Un « jumeau » des lignes de production dans les bureaux et les laboratoires

Ferring Pharmaceuticals a également pu augmenter le niveau d'efficacité du processus de production pendant les opérations de maintenance ordinaires en augmentant la disponibilité des pièces de rechange et en adoptant une solution pour les tests et les qualifications qui permet de maintenir la continuité opérationnelle aux niveaux les plus élevés, même en cas de nouvelles versions et de mises à jour du logiciel.

Et pour faciliter les essais et la qualification, une solution a également été mise au point. Cette solution combine le matériel

et le logiciel et reproduit la fonctionnalité des lignes de production de Ferring. Ce système peut simuler des opérations dans des environnements autres que la production, comme les bureaux et les laboratoires, ce qui rend la validation plus accessible. Fonctionnant hors ligne et sans matériel d'emballage réel, il permet de réaliser des tests complets, sans perturber les délais de production réels !

« Notre collaboration avec Ferring Pharmaceuticals a évolué depuis le début en fonction des besoins et des exigences du client. En prêtant attention aux développements réglementaires et en approfondissant la connaissance des processus des différents sites de Ferring, nous avons été en mesure d'améliorer l'efficacité de la production et de la maintenance, avec une réduction drastique des délais d'approvisionnement en pièces détachées et avec un système qui teste les mises à jour logicielles, excluant le risque d'arrêt de la ligne », conclut Mattia Assanelli, Directeur des services d'Antares Vision Group.

►► 34228 sur [www.pei-france.com](http://www.pei-france.com)



# Un suivi des actifs précis et plus économe en énergie

En partenariat avec Unikie et CoreHW, Onsemi fournit un système permettant de développer facilement des solutions de suivi des actifs pour les entrepôts, les magasins de détail et d'autres bâtiments.

Onsemi, spécialiste des technologies intelligentes d'alimentation et de détection, a lancé un système de positionnement de bout en bout qui permet le développement plus simple et plus rapide de solutions de suivi d'actifs, plus précises, plus rentables et plus économes en énergie. Le système est basé sur le microcontrôleur RSL15 d'Onsemi, le microcontrôleur Bluetooth 5.2 à plus faible consommation de l'industrie, et intègre des algorithmes logiciels et des composants fournis par Unikie et CoreHW.

La solution Bluetooth faible énergie (Bluetooth LE) permet d'utiliser des balises pour suivre des objets ou des personnes avec une précision inférieure au mètre dans des espaces fermés définis tels que des entrepôts, des magasins ou d'autres bâtiments. Il peut s'adapter à de grands volumes d'objets suivis en termes de performances et de coût, tout en réduisant les efforts de développement et les délais de mise sur le marché. Avec plusieurs nouvelles fonctionnalités avancées, le microcontrôleur RSL15

est idéal pour diverses applications d'automatisation industrielle, comme le suivi des actifs, la vente au détail intelligente et les nœuds de périphériques IoT.

## Précision, efficacité énergétique et sécurité

Il cumule plusieurs avantages :

- la précision : il prend en charge une portée plus longue, des transmissions de données plus élevées et une localisation suivant l'angle d'arrivée (« Angle of Arrival », AoA) et l'angle de départ (« Angle of Departure », AoD).
- l'efficacité énergétique : la fonction de détection intelligente innovante d'Onsemi permet au processeur Arm Cortex-M33 de rester en veille profonde tout en continuant à surveiller les interfaces des capteurs.
- la sécurité : le RSL15 est conçu avec les technologies Arm TrustZone et Arm CryptoCell-312 pour établir la sécurité d'un dispositif et pour protéger l'authenticité, l'intégrité et la confidentialité du code et des données. Certifiée

PSA Niveau 1, cette conception renforce les mesures de sécurité déjà proposées dans le protocole Bluetooth pour garantir l'assurance à la fois au niveau des données et des applications.

## Calcul des positions en temps réel

Unikie, une société d'ingénierie pionnière axée sur la création d'espaces intelligents, a développé des algorithmes et des composants logiciels pour calculer les positions en temps réel d'une balise Bluetooth LE, en utilisant les valeurs IQ des signaux reçus.

CoreHW, une société de semi-conducteurs fabriqués développant des technologies de circuits intégrés fournit des kits de développement Bluetooth pour la localisation basée sur l'angle d'arrivée (AoA) à une gamme d'industries, leur permettant de tirer parti de systèmes de localisation intérieure pour améliorer les applications basées sur la localisation.

►► 34236 sur [www.pei-france.com](http://www.pei-france.com)

# WAGO



## WAGO ENERGY DATA MANAGEMENT

L'efficacité c'est aussi simple que ça !

Avec l'application Wago Energy Data Management, vous disposez d'une solution globale pour la gestion de vos données énergétiques

- Enregistrement
- Sauvegarde
- Visualisation
- Surveillance

►► 33837 sur [www.pei-france.com](http://www.pei-france.com)



Pour en savoir +



# L'IA générative s'intègre dans les terminaux mobiles

L'IA générative, alliée aux terminaux mobiles Zebra, offre aux entreprises plus de confidentialité, de sécurité, de capacité et de réduction de coûts.

Zebra Technologies, l'un des principaux fournisseurs de solutions digitales permettant aux entreprises de connecter les données, les actifs et les personnes de façon intelligente, a développé avec succès un grand modèle de langage (LLM) d'intelligence artificielle générative (IA générative). Celui-ci fonctionne sur les terminaux mobiles et les tablettes Zebra, et ne nécessite aucune connectivité au cloud. Cette avancée permet aux partenaires et aux clients de Zebra de réaliser des gains de productivité significatifs qui façonneront l'avenir du travail dans de nombreux secteurs comme la vente au détail, les entrepôts, la logistique, le tourisme, les loisirs et l'événementiel, ou encore la santé. Exécutés sur des terminaux mobiles, les grands modèles de langage d'IA générative peuvent renforcer les potentiels des équipes terrain afin de mieux servir les clients finaux.

## Une confidentialité et une sécurité renforcées

Alliée aux terminaux mobiles, l'IA offre une personnalisation supplémentaire ainsi qu'une

confidentialité et une sécurité renforcées, les données restant sur le terminal mobile. Elle permet également d'accélérer les performances et de réduire les coûts, les moteurs de recherche cloud basés sur l'IA générative pouvant s'avérer coûteux. Un livre blanc publié par Qualcomm Technologies suggère en effet qu'une requête basée sur l'IA générative coûterait dix fois plus qu'avec une méthode de recherche traditionnelle. En supprimant la nécessité d'utiliser le cloud, il est ainsi possible de réduire les coûts.

« Les terminaux mobiles Zebra sont de puissantes plateformes avec des logiciels et des modèles d'IA de pointe qui bénéficient de l'apport de notre vaste écosystème de partenaires pour résoudre les défis des clients et leur apporter de la valeur ajoutée », a déclaré Tom Bianculli, directeur de la technologie, chez Zebra Technologies. « Nous appliquons l'IA générative aux terminaux mobiles, ainsi qu'à d'autres domaines de spécialisation Zebra tels que l'IA vocale, la vision par ordinateur et les logiciels de vision industrielle alimentés par le deep learning, ou

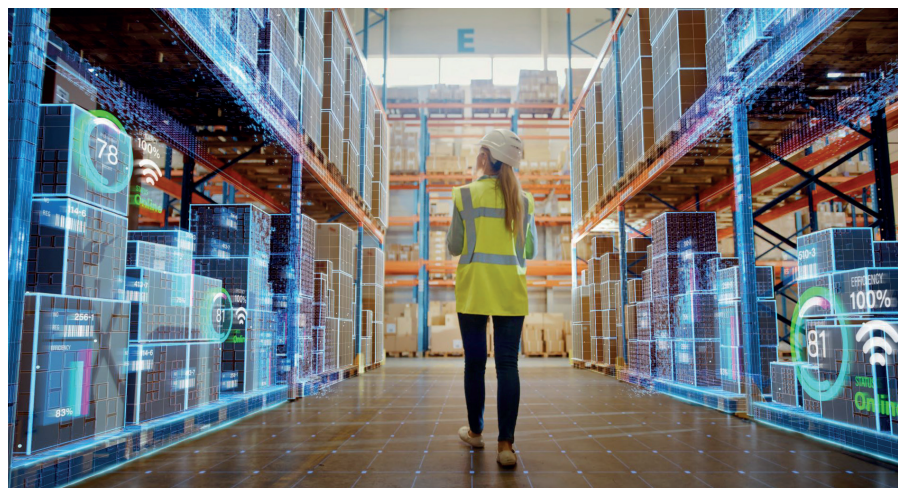


« Les terminaux mobiles Zebra sont de puissantes plateformes avec des logiciels et des modèles d'IA de pointe », a déclaré Tom Bianculli, directeur de la technologie, chez Zebra Technologies.

encore les logiciels de gestion des tâches et du workflow utilisant l'IA orchestrée ».

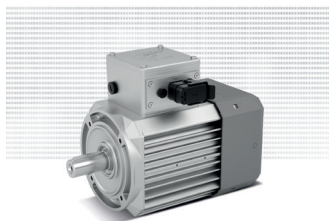
Les terminaux mobiles TC53/TC58 et TC73/TC78, ainsi que la gamme de tablettes ET6x de Zebra, équipés de processeurs Qualcomm Technologies (et des solutions de visibilité des actifs et d'automatisation intelligente de Zebra), offrent de meilleures informations décisionnelles, analyses et recommandations qui favorisent la résolution des problèmes, la planification et la créativité. Les équipes terrain peuvent utiliser un modèle de terminal portatif de petite taille, même dans les environnements isolés, urbains ou souterrains ne disposant pas d'une connectivité cloud.

►► 34234 sur [www.pei-france.com](http://www.pei-france.com)



## SYSTÈME D'ENTRAÎNEMENT À HAUT RENDEMENT

pour les systèmes de convoyage



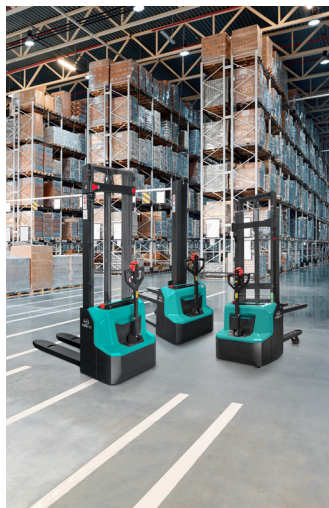
Une charge maximale de 35 kg par mètre est considérée comme une valeur par défaut réaliste pour la plupart des centres de distribution de colis. Quelles sont cependant les performances qu'un système d'entraînement doit fournir pour

supporter cette charge maximale dans la durée ? Cette question est une source de préoccupation pour les prestataires logistiques. Les systèmes d'entraînement à haut rendement énergétique ne contribuent pas seulement à réduire les coûts ; chaque baisse de la consommation d'énergie se traduit également par une diminution des émissions de CO<sub>2</sub>. Les experts de **Nord Drivesystems** conseillent aux clients les solutions d'entraînement les plus appropriées. Le moteur synchrone IE5 à haut rendement de Nord Drivesystems constitue la base de nombreuses solutions d'entraînement et dépasse même la classe de rendement IE5 la plus élevée. Nord Drivesystems le propose sous forme de moteur autonome ou de solution système intégrée. Avec le motoréducteur DuoDrive, le moteur est intégré dans un réducteur à engrenages cylindriques, et pour effets des économies d'énergie ainsi qu'une interface et un espace d'installation réduits. Dans le système d'entraînement LogiDrive, la configuration est complétée par un variateur de fréquence décentralisé afin de simplifier le câblage.

►► 34229 sur [www.pei-france.com](http://www.pei-france.com)

## GERBEURS COMPACTS

pour les entrepôts aux allées étroites



**Baoli** lance une gamme de gerbeurs très compacts, la série KBS 12, trouvant sa place dans la quasi-totalité des entrepôts, particulièrement là où l'espace est compté. Les batteries lithium-ion sans entretien les rendent également très souples et faciles d'utilisation. Avec une capacité de charge de 1,2 t pour une hauteur de levée de 3600 mm, ces gerbeurs peuvent être utilisés pour une grande variété d'applications. Ils sont déclinés en trois modèles : KBS 12, KBSI 12 et KBSM 12. Le KBS 12 est disponible en version mât

simplex et télescopique. Son châssis est équipé de 4 points d'appui afin d'assurer une stabilité maximale du gerbeur. Les fourches sont disponibles avec une largeur totale de 570 ou 685 mm. Le KBSI 12 dispose d'une levée initiale actionnable d'une pression sur un bouton. Il est idéal pour les applications nécessitant une plus grande garde au sol et une maniabilité optimisée sur sol légèrement irrégulier. Le KBSM 12 est doté d'un mât poutre, ou mono-mât, dont la position centrale offre un meilleur contrôle visuel sur les bras de fourche.

►► 34079 sur [www.pei-france.com](http://www.pei-france.com)

## SOLUTIONS DE DÉTECTION

pour les robots mobiles et les véhicules autonomes



**Sick** présente les capteurs multiScan et la caméra 3D safeVisionary2 qui améliorent significativement l'efficacité des véhicules autonomes et des robots mobiles. Les capteurs Lidar 3D multiScan 100 assurent aux robots mobiles une vue

panoramique à 360° en 3D. En raison des 690000 points de mesure, le multiScan100 atteint une précision de pointe grâce à laquelle rien ne lui échappe dans son environnement. Avec sa forme compacte d'environ 10 cm et la prise en charge d'interfaces industrielles, il est très facile à intégrer. La première variante, le multiScan136, fournit des données de mesures 3D pouvant être utilisées pour une localisation autonome précise de véhicules ainsi qu'une cartographie simultanée de l'environnement. De plus, grâce aux capteurs Lidar 3D, il est possible de détecter des bords ou des obstacles en 3D. Sick propose également la caméra 3D safeVisionary2. Pendant un transport, elle surveille le trajet en 3D, c'est-à-dire l'espace au-dessus du plan de balayage du scrutateur laser de sécurité installé sur le véhicule. Les objets qui franchissent ce champ 3D, par exemple un crochet de grue ou des palettes ou des objets dépassant des étagères, sont détectés avec fiabilité. La même chose s'applique à la protection des côtés lors des manœuvres de véhicules autonomes et de robots mobiles pendant les procédés de chargement et de déchargement.

►► 34233 sur [www.pei-france.com](http://www.pei-france.com)

## PALETTE PLASTIQUE ROBUSTE

pour la logistique



La palette SF1000 PES de **Smart-Flow** de dimensions 1000 x 1200 x 150 répond parfaitement aux besoins des entreprises qui recherchent un produit à la fois ergonomique et fiable,

pouvant être utilisé aussi bien en rack que sur convoyeur, pour leur logistique interne ou à l'export. Conçue d'un seul bloc, la palette plastique SF1000 PES est extrêmement robuste. Cette palette medium est dotée de 3 ou 5 semelles, selon les versions, afin de garantir une parfaite répartition du poids. En matière de charge, elle peut supporter 1250kg en dynamique et jusqu'à 500 kg en rack. A noter qu'elle peut être renforcée à l'aide de 3 barres métalliques dans le sens 1200 et une barre dans le sens 1000, permettant de passer à 1650kg en charge dynamique et de doubler sa charge en rack à 1 tonne. La structure de la palette a été repensée avec une forme moins ajourée pour offrir encore plus de résistance. Quant au plateau, son design a été étudié pour équilibrer parfaitement le transfert de force de l'ensemble, entre le plateau supérieur et les pieds. Smart-Flow a également ajouté des rebords extérieurs en option de 7 mm ou 22 mm pour assurer une parfaite tenue du chargement. Et pour une pérennité à toute épreuve, la forme de ses plots a été arrondie afin d'éviter les risques de casse pouvant être causés par les coups de fourche répétés des engins de manutention.

►► 34027 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023

[www.pei-france.com](http://www.pei-france.com)

# Une meilleure productivité pour les mesures dans les applications hygiéniques

La gamme de produits compacts d'Endress+Hauser permet d'accroître la productivité, est facile à utiliser et offre une flexibilité optimale en production.

Endress+Hauser présente une gamme de produits au design compact destinée aux applications hygiéniques. Cette gamme permet d'accroître la productivité, est facile à utiliser et offre une flexibilité optimale en production. Elle convient parfaitement aux industries des sciences de la vie, de l'agroalimentaire et des boissons. Elle couvre trois principes : la mesure de pression, la détection de niveau et la mesure de niveau continu.

La conception entièrement hygiénique des produits et la classe de protection IP69 permettent un nettoyage efficace. Les capteurs en inox sont entièrement soudés et peuvent rester en place pendant les process de nettoyage et de stérilisation des installations. Cela permet de gagner du temps et de simplifier les procédures de nettoyage. L'écran tactile intuitif permet de modifier les réglages directement sur l'appareil.

## Des performances optimales pour chaque application

Pour la mesure de la pression, le modèle Cerabar PMP43 séduit par une large gamme de variantes de capteurs avec des raccords process entièrement soudés et hygiéniques, utilisés

dans les industries agroalimentaires, des boissons et des sciences de la vie. Le modèle Liquiphant FTL43 permet de détecter des niveaux dans tous les liquides grâce à la technologie par lame vibrante éprouvée. Un des avantages majeurs est la large gamme d'applications sans adaptation nécessaire aux différents milieux. Pour une mesure de niveau fiable et sans contact, Endress+Hauser présente le capteur radar Micropilot FMR43. L'appareil garantit une mesure fiable même dans des conditions de process turbulentes ou changeant rapidement. Les besoins des industries hygiéniques en matière de cuves plus petites ont également été pris en compte lors du développement des nouveaux appareils. En plus de la technologie éprouvée des radars 80 GHz, un raccord process de 1/2 pouce peut être sélectionné avec l'option de fréquence 180 GHz, ce qui permet une utilisation dans les cuves de process les plus petites.

## La maintenance prédictive permet d'éviter les arrêts de process

La gamme de produits compacts augmente la productivité des process de production. La fonction de vérification développée par Endress+Hauser avec Heartbeat Technology y contribue largement. Elle fournit des informations de diagnostic et de surveillance fiables. La surveillance constante du process permet de détecter à un stade précoce les anomalies telles que la formation de mousse ou un colmatage sur l'antenne de l'appareil. Cela permet une maintenance prédictive et réduit le risque d'arrêt de l'usine. Les vérifications de l'appa-

reil sont effectuées en moins de trois minutes, sans démontage ni interruption du process.

Les cycles d'étalonnage du Micropilot FMR43 peuvent être considérablement allongés grâce à Heartbeat Technology avec l'indice de précision radar (RAI). Cette technologie permet de vérifier que la précision de l'instrument reste dans les limites tolérées sans interrompre le process. En effet, le RAI évalue la précision de la mesure de référence au cours d'une vérification traçable conformément à la norme ISO 9001, afin d'analyser les éventuelles dérives de la mesure par rapport à l'appareil tel qu'il a été fabriqué. De cette manière, les opérateurs de production maîtrisent toujours la précision des appareils de mesure.

## Facilité d'utilisation grâce à l'assistance numérique

L'ensemble de la gamme utilise une interface utilisateur identique pour toutes les technologies. L'installation, la mise en service et l'utilisation des appareils sont ainsi plus faciles et plus intuitives que jamais. De nombreux assistants numériques guident les utilisateurs lors de la mise en service et du paramétrage. Cela permet de gagner un temps précieux et d'éviter les erreurs systématiques. Toutes les analyses, les contrôles, la maintenance et les vérifications de fonctionnement peuvent être confortablement effectués à distance via un smartphone ou une tablette à l'aide de la technologie Bluetooth et de l'application SmartBlue d'Endress+Hauser. De plus, les appareils peuvent également être intégrés dans des systèmes d'automatisme ou des outils logiciels pour le paramétrage et le contrôle via une connexion IO-Link.

► 34235 sur [www.pei-france.com](http://www.pei-france.com)







# Guidages linéaires pour un mouvement ultra-fluide

La technologie NSK de mouvement ultra-fluide développée pour les guidages linéaires très prisés à usage général série NH/NS, constitue une première mondiale.

Grâce à l'utilisation d'éléments roulants élastiques, la technologie brevetée NSK de mouvement ultra-fluide produit un profil de frottement dynamique très homogène, idéal pour les matériels d'inspection et de mesure de haute précision. Les caractéristiques de faible frottement et de fluidité de mouvement des guidages linéaires en font un atout précieux pour tous types de systèmes nécessitant un contrôle de mouvement performant. C'est pourquoi les guidages linéaires NH/NS sont utilisés dans un large éventail d'applications : équipements de fabrication de semi-conducteurs et d'écrans LCD, équipements de fabrication automobile, robots convoyeurs, matériels d'inspection et de mesure et machines-outils notamment.

Aujourd'hui, les équipements utilisés dans ces applications sont de plus en plus sophistiqués. En particulier, les matériels d'inspection et de mesure les plus récents exigent davantage de fluidité et de précision de mouvement et placent de fortes attentes sur les guidages linéaires.

## Éléments roulants élastiques

Dans cette optique, NSK a entrepris de dévelop-



Guidages linéaires NSK série NH/NS dotés d'une technologie de mouvement ultra-fluide.

per sa technologie de mouvement ultra-fluide en optimisant la forme du chemin de circulation des billes et en faisant appel à des éléments roulants élastiques pour supprimer les « micro-stutters » irréguliers (brefs bégaiements ou secousses lors du mouvement provoqués par des fluctuations localisées du frottement). Ces éléments réduisent l'effet de collision des billes entre elles dans les sections incurvées du chemin de circulation des billes, afin d'empêcher toute augmentation du frottement et, par conséquent, d'obtenir un mouvement extrêmement fluide.

## Pour les applications nécessitant un fonctionnement vertical

Outre les matériels d'inspection et de mesure, les guidages linéaires NSK dotés de la technologie de mouvement ultra-fluide conviennent aux applications nécessitant un fonctionnement vertical et aux autres positions de montage où les caractéristiques opérationnelles ont tendance à se détériorer. En outre, ces guidages linéaires innovants sont interchangeables dimensionnellement avec la série standard NH/NS de NSK, facilitant ainsi le remplacement des unités actuellement en service sans aucune modification de conception. La technologie ultra-fluide de NSK est disponible pour les guidages linéaires séries NH 15, 20 et 25, ainsi que pour les modèles NS 15, 20, 25 et 30. Au total, NSK peut fournir 28 variantes, dont différentes longueurs et différents types de glissières. Ces guidages linéaires sont compatibles avec un large choix d'options, telles que l'unité de lubrification NSK K1-L, les configurations acier inoxydable et les traitements de surface spéciaux.

➔ 34166 sur [www.pei-france.com](http://www.pei-france.com)



ABONNEMENT NUMÉRIQUE GRATUIT

N° 11 - NOVEMBRE 2023



## PLUS DE SECURITE POUR VOS MACHINES

Avec notre solution Industrie 4.0: le bus SD de Schmersal

- Montage en série de jusqu'à 31 interrupteurs de sécurité distincts
- Réduction des coûts de câblage
- Transmission des données de diagnostic
- Messages rapides et détaillés en cas de défauts
- Facilite la maintenance prédictive de votre installation

[www.schmersal.fr](http://www.schmersal.fr)



34 123 sur [www.pei-france.com](http://www.pei-france.com)



**SCHMERSAL**  
THE DNA OF SAFETY

**PROF NET**

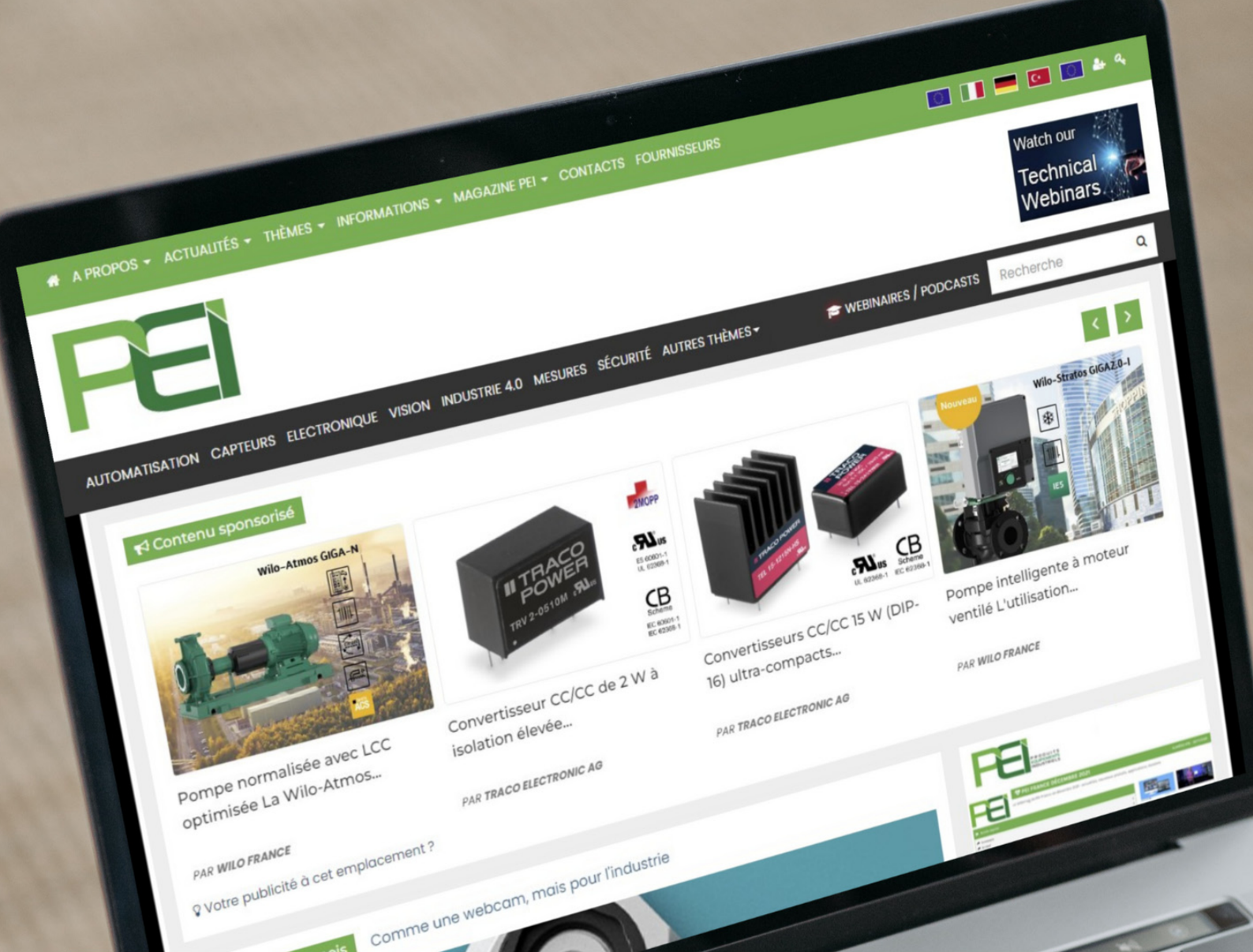
EtherNet/IP  
EtherCAT  
CANopen  
OPC UA

# Sociétés présentes dans ce numéro

Annonces en vert

<b>A</b>	ANTARES VISION	24					
	AUTOMATION24	9					
<b>B</b>	BAOLI	27					
	BINDER	13					
<b>C</b>	CHOMERICS	12					
	CONSCIO TECHNOLOGIES	19					
	COTELEC	9					
	CROWDSTRIKE	21					
<b>E</b>	ENDRESS+HAUSER	11, 28					
<b>F</b>	FOCKE MELER GLUING SOLUTIONS	13					
<b>H</b>	HMS INDUSTRIAL NETWORKS	21					
<b>I</b>	ICFS SHOW	2					
	IGUS	10					
	INTEL	20					
<b>K</b>	KIPP	8					
<b>L</b>	LABFACILITY	9, 17					
<b>M</b>	MICROCHIP	21					
	MINALOGIC	16					
	MOXA	19					
<b>N</b>	NORD REDUCTEURS	23, 27					
	NSK	29					
<b>O</b>	ONSEMI	25					
<b>P</b>	PRODWARE	15					
<b>S</b>	SCHMERSAL	9, 29					
	SENSOPART	21					
	SICK	27					
	SMART-FLOW	27					
	SOSAFE	18					
<b>T</b>	TOSHIBA ELECTRONICS	13					
<b>U</b>	U-BLOX	22					
<b>W</b>	WAGO CONTACT	25					
	WÜRTH ELEKTRONIK	13					
<b>Z</b>	ZEBRA TECHNOLOGIES	26					



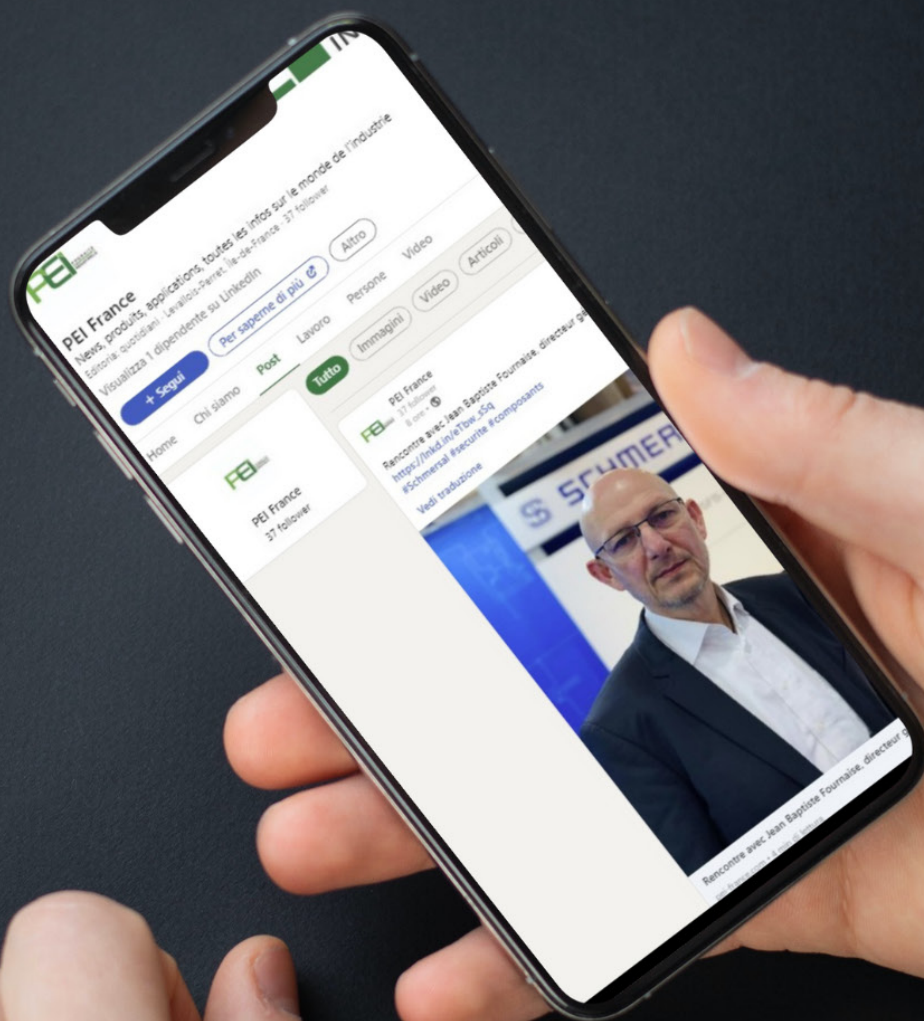


# WWW.PEI-FRANCE.COM

- | Temps de chargement rapide
- | Réactivité
- | Contenus pertinents
- | Webinars et podcasts à la demande
- | Formulaire de demande de renseignements clair
- | Intégration du fil d'actualités Twitter







**SUIVEZ**  
**PEI FRANCE**  
**SUR LINKEDIN**

