

Fiche de missions technologiques – Digitalisation de la chaîne de valeurs : confiance numérique

📍 France

« Confiance Numérique as a Service » pour l'Industrie du Futur au travers de la mise en place de structures certifiées au plus haut niveau autour de la privacy (ou protection des données personnelles), la sécurité physique des personnes et la cybersécurité.

1. Confiance numérique

La numérisation des processus de l'usine et des sites industriels exige de mettre en place des « boucliers éthiques, technologiques et numériques de protection » des personnes, des infrastructures, des infostructures et des données au coeur-même de l'environnement cyber-physique.

Ces « boucliers de protection de l'entreprise, de l'usine et des sites industriels connectés » concernent :

- la sécurisation des données personnelles (« Privacy ») ;
- la sécurité physique et la santé des personnes ;
- la cybersécurité (la prévention contre les attaques) ;
- l'anticipation des risques et résilience.

1.2.1 Enjeux industriels

- Garantir « l'intégrité et la sûreté de fonctionnement » de la ligne de fabrication, de la station, des sites industriels en général et des machines, véhicules, outils, « accessoires », équipements informatiques de support en particulier ;
- Garantir la sécurité physique et la santé des opérateurs et acteurs humains en interaction quasi-permanente avec des réseaux d'objets et robots connectés ;
- Se conformer aux législations en vigueur concernant la protection des données personnelles émanant des opérateurs et acteurs humains de l'Industrie du Futur.

Il conviendra de décliner ces enjeux pour :

- Assurer la « résilience » de toutes les infrastructures et infostructures en cas d'incidents, de « crise » ou suite à des « attaques » ;
- Garantir « l'intégrité et la véracité de tous les flux de données » issus des différents réseaux d'objets intelligents (systèmes de contrôle industriel, réseaux électriques, réseaux de surveillance, réseaux de supervision, etc.) ;
- Mettre en place un dispositif d'anticipation des risques de toute nature, tant vis-à-vis des personnes, que des infrastructures, infostructures et des données.

1.2.2 Enjeux transformationnels et sociétaux

La sécurité numérique se métamorphose et vit un changement d'échelle faisant naître de nouveaux paradigmes sociétaux et sémantiques pour :

- Placer l'humain au cœur et développer une culture de la « politique et des processus » de sécurité, de « privacy » et de cybersécurité au sein de l'entreprise, de l'usine et des sites industriels connectés (notamment par la mise en place des codes de bonnes pratiques au sein des personnels tant pour la sécurité physique que pour la cybersécurité) ;
- Intégrer dans les « business models » des entreprises, usines et sites industriels connectés les coûts (rédhitoires) consécutifs à des défaillances, voire des manques en termes de sécurité des personnes et de cybersécurité (par exemple, coûts liés à la « fuite » d'informations sensibles, au piratage sous la forme d'une prise de contrôle par des agents malveillants de machines, outils et véhicules, rançonnage, etc.) ;
- Introduire des niveaux de certification en termes de sécurité des personnes en interactions avec des réseaux d'objets / robots / machines intelligents, de « privacy », et enfin de cybersécurité des entreprises, des usines et sites industriels connectés ;
- Créer des nouveaux modèles d'assurance des entreprises, usines et sites industriels connectés, notamment ceux pilotés par les usages in situ.

1.2.3 Verrous technologiques

La chaîne de sécurité repose sur différents verrous technologiques tels que :

- L'hétérogénéité des systèmes, infrastructures, infostructures dont il faut garantir l'intégrité (réseaux de serveurs informatiques, d'énergie, de surveillance, de contrôle, etc...) ;
- La complexité, la taille et le passage à l'échelle des systèmes, infrastructures, infostructures dont il faut garantir l'intégrité ;
- L'agilité en « temps réel », face à la grande « vitesse » d'évolution et de changement des conditions et de l'environnement opératoires, a fortiori sur des sites industriels très exposés, mais également dans l'entreprise et les usines ;
- Modélisation, simulation et visualisation des flux dynamiques de « points faibles en sécurité physique et en cybersécurité » d'une chaîne de production, d'une usine et d'un site connectés ;
- L'optimisation des paradigmes de cryptographie end-to-end ou en local (on the device) en fonction des besoins et du compromis « privacy-cybersécurité » ;
- La vérification de propriétés de flots d'information et de sécurité d'exécution

des composants logiciels coeur de système.

1.2.4 Verrous sociétaux

Malgré la forte attente en terme de nos sociétés en termes de sécurité, des verrous sociétaux demeurent comme :

- Chaîne de responsabilité civile dans des sinistres impliquant ou causés par des objets, robots, véhicule connectés et autonomes ;
- Définition et mise en place de « métriques » de diagnostic, d'analyse et de prédiction des risques inhérents à la sécurité physique des personnes et à la cybersécurité (métriques susceptibles d'être normalisées et partagées par les producteurs, clients, assureurs, investisseurs, etc.) ;
- Définition et mise en place de « métriques » de confidentialité des données personnelles ;
- Appartenance des données émanant d'un opérateur sur une chaîne de fabrication, collectées au travers de dispositifs « connectés » ;
- Définition des compromis à obtenir entre la protection des données personnelles et la « sécurisation » des entreprises, usines et sites ;
- Questions sociologiques et juridiques relatives à la place du comportement et de l'erreur humaine dans la boucle de cybersécurité en cas de faille ou fuite.



Leviers

Nouveaux modèles économiques et sociétaux. Stratégies et alliances. - Relations Clients / Fournisseurs intégrés - Usines et lignes / Ilots connectés, pilotés et optimisés - Nouvelle approche de l'homme au travail. Organisation et management innovants. - Technologies de production avancées. - Objets connectés et internet industriel.



Filières

Aéronautique - Agro-industrie - Automobile - Biens de consommation - Biotechnologie - Bois - Chimie et Matériaux - Construction et génie civil - Déchets et recyclage - Eco-industries - Efficacité énergétique - Électronique - Énergies renouvelables - Espace - Ferroviaire - Industries et technologies de santé - Industries extractives et de première transformation - Mécanique - Mode et Luxe - Naval - Nucléaire



Technologies

Digitalisation de la chaîne de valeurs