GIMELEC

Nous décuplons les énergies

Guide pédagogique Cybersécurité OT

Un guide proposé par le Club Cyber-OT du GIMELEC

Version 2 - Mars 2023

GIMELEC CYBER OT

le club des offreurs pour la cybersécurité industrielle

Edito du Président

Le Club Cyber-OT s'est donné comme ambition de fédérer les offreurs en cybersécurité OT en France. En effet, la cybersécurité est un maillon essentiel et stratégique des systèmes digitaux qui font aussi bien l'industrie, les villes et les bâtiments, et les adhérents du GIMELEC portent ces offres technologiques et électronumériques garantes de la compétitivité et de la sécurité de leurs utilisateurs.

Le digital est constitué de deux univers interconnectés, mais aux enjeux différents. Le monde des systèmes d'information ou IT (pour Information Technologies), qui permet de digitaliser des processus et traite essentiellement de la donnée, est le plus connu de ces univers. Son pendant est le monde de l'informatique industrielle ou OT (pour Operating Technologies), il regroupe **les systèmes digitaux qui pilotent des processus physiques**, tels que les lignes d'assemblage dans les usines, les protections des réseaux électriques, le pilotage des réseaux d'eau, le contrôle des ventilations dans les bâtiments ou encore les feux rouges dans la ville.

L'évolution du monde qui nous entoure se structure autour des fondamentaux que sont l'électrification et la digitalisation. **Cette tendance de fond promet de gagner en productivité**, mais est également un gage d'efficacité pour réduire l'empreinte carbone des activités humaines en gardant la capacité de produire et d'innover. **Il est désormais impossible d'envisager la productivité sans digital, et son corollaire, le digital sans cybersécurité, y compris dans toutes les applications industrielles et urbaines !**

Yann Bourjault, Président Club Cyber-OT
Directeur cybersécurité et transformation digitale - Schneider Electric

Le Club Cyber OT se consacre aux positions et travaux permettant de **faire progresser la cybersécurité industrielle (OT) en France et en Europe** afin de sécuriser les technologies #electronumériques conçues, fabriquées et vendues en grande partie par les membres du GIMELEC. L'objectif est de permettre d'assurer la pérennité des apports du digital dans les économies modernes. Pour cela, renforcer la coopération entre clients et fournisseurs est un enjeu clé, comme le soulignait le rapport « Cybersécurité : avis de tempête » de l'Institut Montaigne. Afin de structurer cette coopération, les fournisseurs doivent se rassembler pour être représentés et collaborer avec les associations d'utilisateurs et les instances législatives et régulatoires.

Les enjeux sont critiques, il s'agit en effet de mettre en lumière le domaine de la cybersécurité OT pour faire face aux menaces grandissantes dans un domaine resté relativement épargné jusqu'en 2018, mais qui voit les risques augmenter rapidement. Des efforts importants sont à faire pour organiser les entreprises et financer cette ambition, mais aussi pour préciser la façon dont la cybersécurité pourra, demain, se combiner avec pragmatisme et sans accros avec les exigences du monde industriel.

Pour les offreurs de solutions cyber-OT, **la plupart des grands enjeux de développement sont communs** : de la prise en compte des exigences régulatoires et normatives aux efforts de pédagogie, en passant par la coordination événementielle. Chaque entreprise libère ainsi du temps pour développer individuellement sa propre différentiation.

Qu'est-ce que le Club Cyber-OT du GIMELEC ?

- Le GIMELEC est une association professionnelle, **porte parole des industriels de l'électronumérique et de l'automatisme**. Ses 200 membres développent des solutions pour les **transitions énergétiques, industrielles et numériques sur le marché français**, avec plus de 16 milliards de chiffre d'affaires.

- Le Club Cyber-OT du GIMELEC est un Club regroupant un collectif d'entreprises et d'organismes de recherches, actifs dans le domaine de la **cybersécurité des systèmes industriels et urbains**, communément appelée **Cyber OT**. Le collectif vise une action en faveur des solutions sécurisées et participants à une maitrise de la souveraineté numérique française et européenne.

- Créé en 2020, successeur du Cluster ECC4iU, **le Club rassemble désormais une trentaine d'entreprises phare du secteur,** couvrant l'ensemble des offres du secteurs : conseil et audit, matériels, installation et maintenance.

- **L'action du Club est structurée sur 5 axes fondamentaux au service du développement de la Cyber-OT :**

Accompagner la prise de maturité du secteur

en communicant sur l'importance de la cyber pour accompagner les gains de compétitivité du digital.

Développer des partenariats

pour co-construire les pratiques de cyber-OT dans tous les secteurs concernés, avec les acteurs métier déjà en place.

Appuyer le développement des offres de formations nécessaires

en sensibilisant sur les besoins de formation croisée entre cybersécurité et connaissance du monde industriel.

Coconstruire le cadre règlementaire, normatif et de certification

en facilitant les échanges et l'émergence de consensus au niveau français puis européen.

Suivre la conjoncture du marché

en permettant aux membres de croiser leur vision des dynamiques et des caractéristiques du marchés et des enjeux associés.

GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

32 entreprises spécialisées en cyber-OT !

- ABB France - B&R Automation
- Advens
- Alstef
- Automatique&Industrie
- Agilicom
- Axians (VINCI Energies)
- CEA (Leti & List)
- EKIUM
- Eiffage Energies Systèmes
- Fortinet
- Framatome
- HITACHI Energy France
- GE Grid Solutions
- ICE
- KOHLER-SOREEL
- KYRON
- NOZOMI Networks
- Phoenix Contact
- Rockwell Automation
- Sauter
- Schneider Electric
- SCLE SFE
- Seclab
- SICAME Group
- Siemens
- Socomec Group
- SPIE
- Stormshield
- Systerel
- Wallix
- Weidmuller

Avec la collaboration

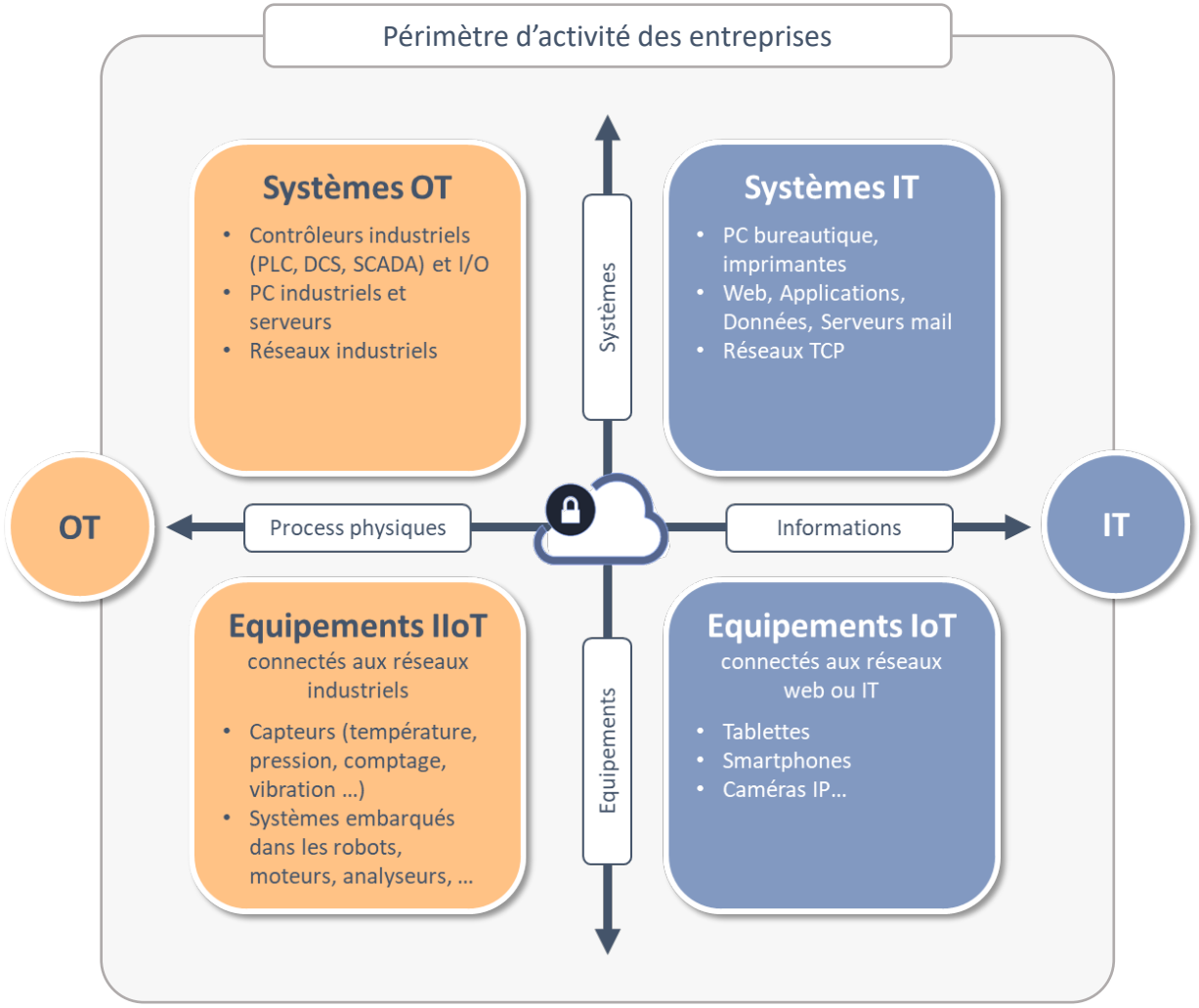
Qu’est-ce l’OT par rapport à l’IT, l’IoT et l’IiOT ?

Définitions :

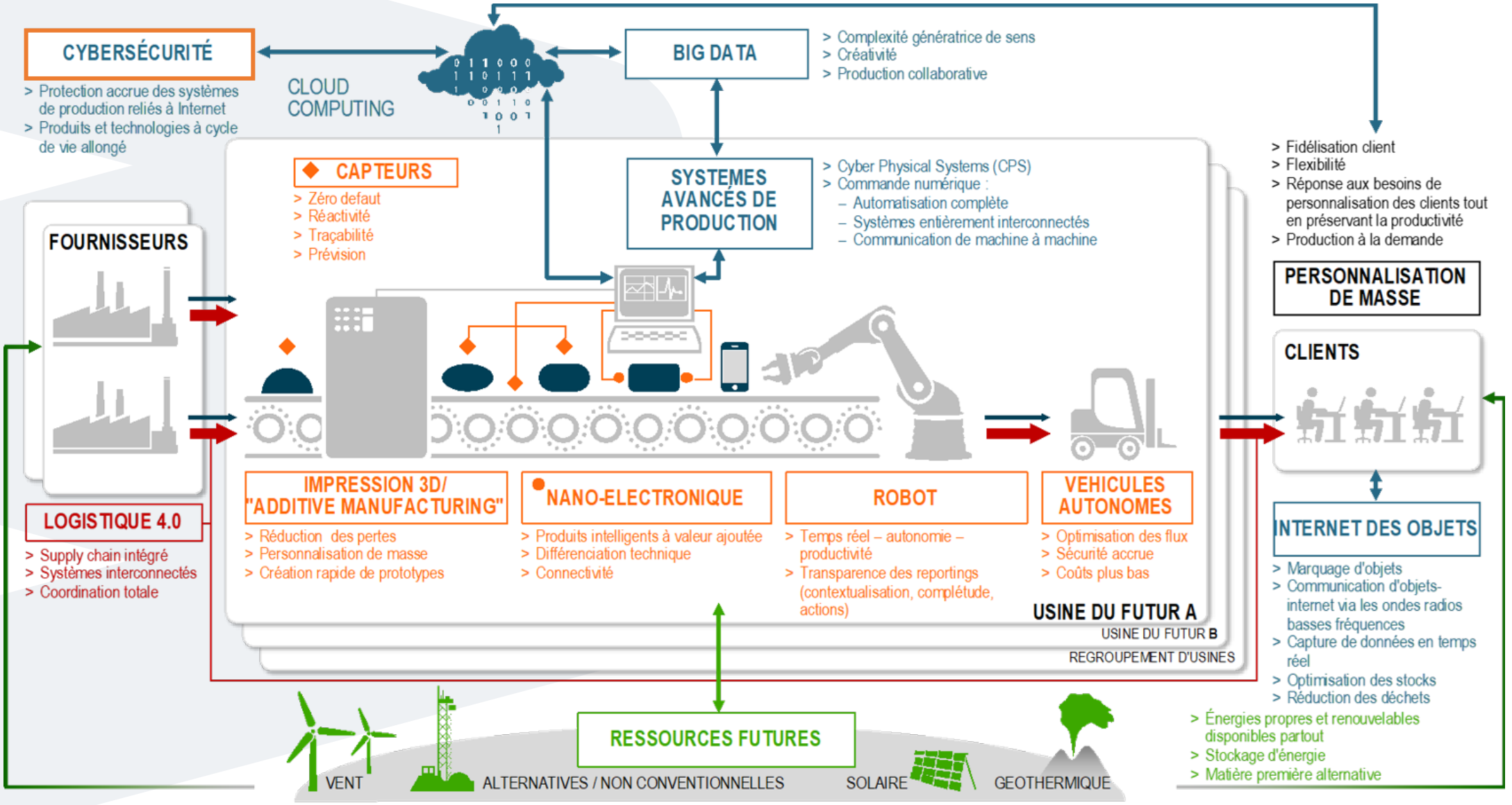
- **L’IT (Information Technology**) désigne la technologie de l’information et traite principalement des Systèmes d’Information d’Entreprise, en charge de la gestion de l’information et des processus de l’entreprises.
- **L’OT (Operational Technology)** est la technologie opérationnelle qui traite les Systèmes d’Information qui ont un impact sur un environnement physique et permettent le bon fonctionnement de l’outil de production, son pilotage opérationnel.
- **L’IoT (Internet of Things)**, désigne l'ensemble des infrastructures et technologies mises en place pour faire communiquer des objets divers par le biais d'une connexion Internet. On parle alors d'objets connectés. Ces objets sont pilotables à distance, le plus souvent à l'aide d'un ordinateur, d'un smartphone ou d'une tablette.
- **L’IIoT (Industrial Internet of Things),** est la déclinaison de l’IoT dans l’environnement industriel. L'IIoT s’appuie généralement sur des outils connectés à Internet et des plateformes d'analyses qui traitent les données produites par les objets. Les objets IIoT peuvent être des petits capteurs de température ou des robots industriels complexes

Impact organisationnel :

- Les équipes IT ont en charge la partie gestion « Entreprise » de l’usine, elles interviennent sur l’ensemble des technologies de l’information et de communication (réseau, matériel, logiciel, téléphonie) nécessaires au pilotage commercial, administratif et financier de l’entreprise.
- Les équipes OT se composent des automaticiens et des équipes en charge de l’informatique industrielle et de la maintenance industrielle.

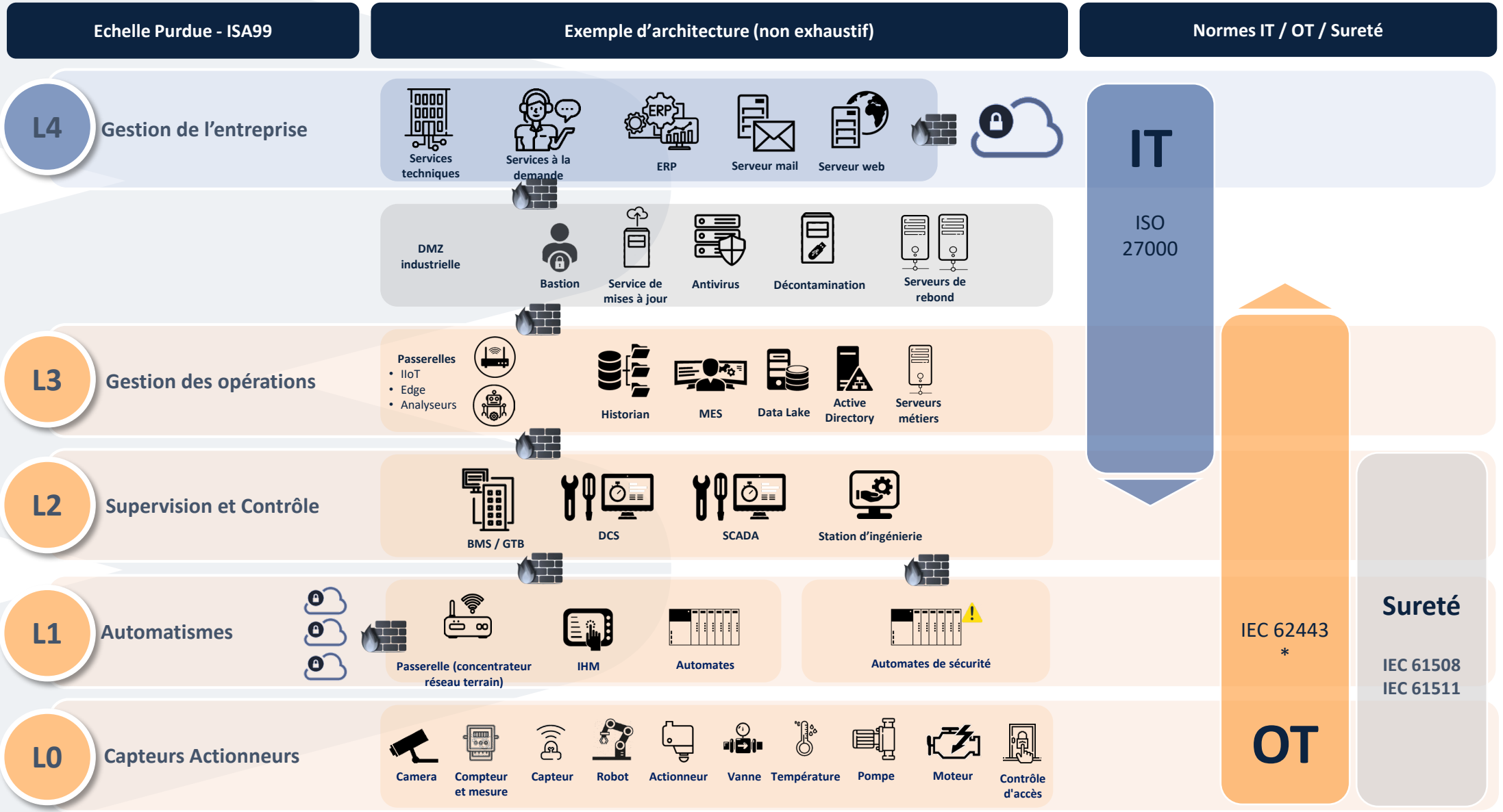


La cybersécurité OT au service de l'Industrie 4.0 et de la compétitivité



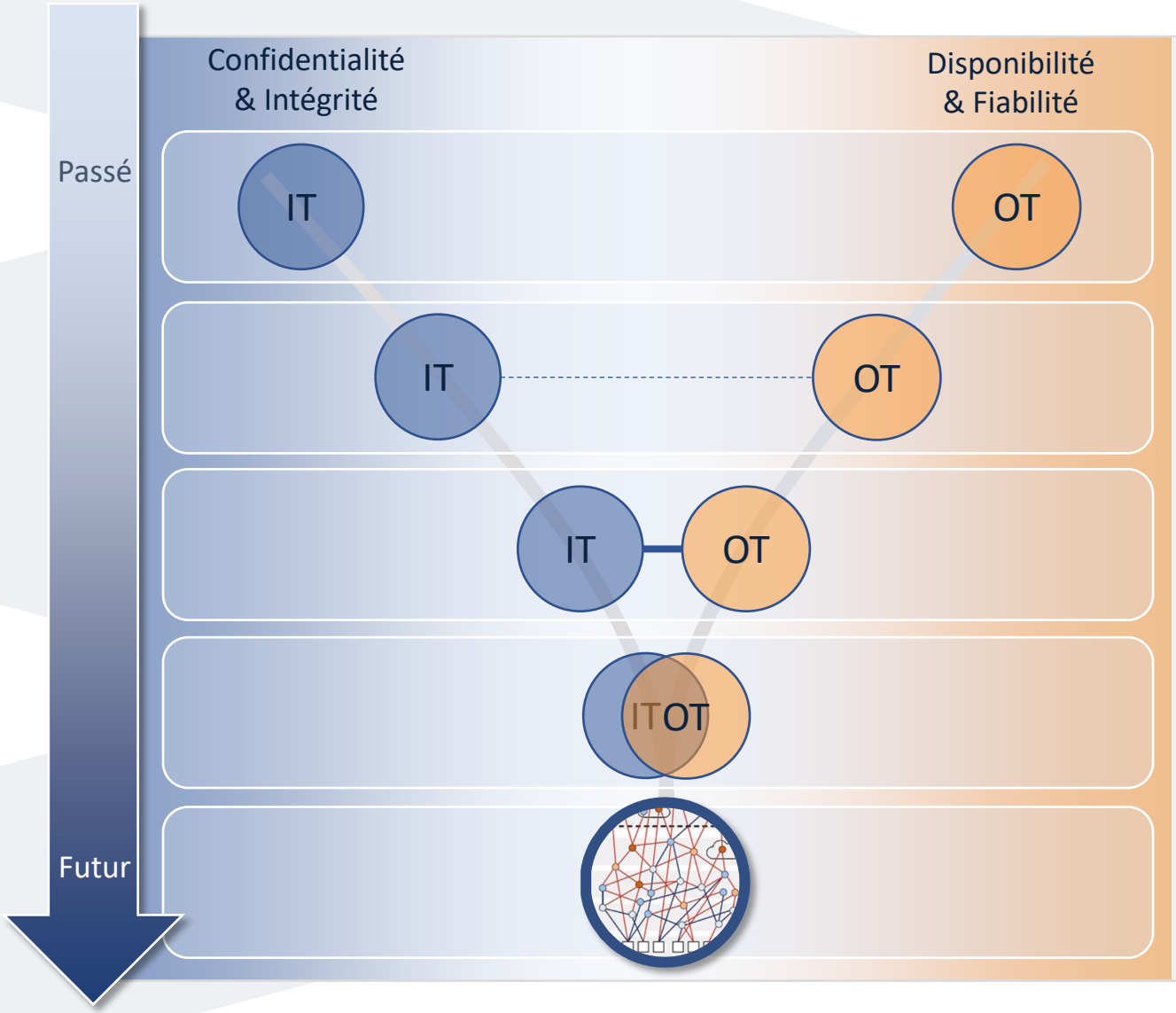
GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

La cybersécurité concerne toutes les couches d'un système industriel



* Des normes sectorielles complètent l'approche

Malgré des différences métiers fortes, on observe une convergence progressive des technologies et de la gouvernance entre l'IT et l'OT



Evolutions Technologiques	Evolutions de la Gouvernance
Réseaux séparés Technologies et cycles de vie différents	Gouvernance distincte Equipes métiers dédiées
Connexion des équipements industriels à Internet Interconnexion de l'OT avec l'infrastructure IT	Premières prises de conscience de façon indépendante
Adoption et installation de systèmes IT dans le périmètre OT Industrialisation de matériels IT	Sensibilisation des équipes, échanges entre les instances IT et OT, voire instances communes Convergence sur les objets communs
Industrie du Futur, jumeaux numériques, cyber physical systems, sécurité by design	Gouvernance partagée Formation croisée des équipes IT/OT Intégration forte entre les processus portés par IT et OT
Plateforme technologique intégrée	Gouvernance commune/intégrée

GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

Sureté et Cybersécurité, deux mondes pas si différents ?

Sureté de fonctionnement des installations OT

- Historiquement, la priorité dans le **domaine industriel et urbain** (***OT***) étant la *sécurité des personnes et des biens,* la donnée opérationnelle doit être **fiable** et complètement **disponible** pendant la production afin de ne prendre aucun risque de perte d'information pouvant générer un danger.
- Cette protection est alors assurée par des procédures de "sécurité", des relais de "sécurité", puis des automates de "sécurité" répondant à certaines obligations (par exemple SIL2) et assurant ainsi fiabilité et disponibilité de l'information.

Sureté de fonctionnement des installations OT		Cybersécurité des données et du SI
Protection des biens et des personnes / fonctionnelle	Objectifs visés	Protection de l'information
Accidentelle	Source du Risque	Actes volontaires
Disponibilité **Fiabilité** Intégrité Maintenabilité Confidentialité	Valeurs principales & **valeurs historiques**	Disponibilité Fiabilité **Intégrité** Maintenabilité **Confidentialité**
Safety Integrity Level (SIL)	Niveau de sécurité	Security Level (SL)
En : Safety Ger : Sicherheit	Equivalence en Anglais et en Allemand	En : Security Ger : Sicherheit
Etude de risque AMDEC/HAZOP	Démarche préventive	Analyse de risque EBIOS
Directive machine	Aspect règlementaire	Directive NIS 2

Cybersécurité des données et du SI

- Avec l'arrivée des **systèmes d'informations d'entreprises** (***IT***) est apparue la notion de *sécurité de l'information.* Les données doivent ici être absolument **confidentielles** et **intègres** pour éviter que l'information soit volée ou corrompue.
- Les infrastructures informatiques sont protégées par des équipements de "sécurité" et une bonne hygiène informatique, assurant les niveaux de "sécurité" (SL) exigés.

La cybersécurité des installations doit être traitée en se repositionnant dans le contexte du risque industriel global.

Les SI, de plus en plus utilisés dans les domaines OT, se doivent d'être complètement fiables et disponibles pour assurer une production sans risques. En parallèle, les menaces de cyber-attaques ciblent davantage les systèmes OT, et ces attaques peuvent impacter la sécurité des biens et des personnes.

Quelles obligations réglementaires sont à venir ? Et pour qui ?

Opérateurs d'Importance Vitale, (OIV)
Un statut Français introduit par la **Loi de Programmation Militaire** de 2013 applicable à certains opérateurs particulièrement critiques, publics ou privés et qui exploitent des équipements et des installations indispensables au fonctionnement de la nation, donc à sa survie.

LPM
2013

Opérateurs de Services Essentiels, ou Entités Essentielles
La directive européenne NIS 2 (2022 en EU et 2024 en FR) étend le dispositif des OIV à une catégorie plus large appelée Entités Essentielles, soit tous les acteurs des secteurs critiques dont les interruptions pourraient avoir des effets négatifs sur le fonctionnement du pays *(Energies, Transport, Marchés financiers, Banques, Santé, Eau potable, infrastructures numériques, Eaux usagées, Administration publique)*

NIS
2018

Entités Importantes,
La directive européenne NIS 2 créé ce nouveau statut pour les entreprises ayant un rôle majeur dans l'économie du pays et la vie quotidienne des citoyens (18 secteurs dont Industries chimiques, agroalimentaire, **fabricants d'équipements ou de machines, fabricants d'équipements électriques, fabricants de produits électroniques**, services digitaux)

NIS2
2024

Autres entités,
Les autres entreprises ou acteurs ne sont pas concernés par les obligations règlementaires et doivent prendre des initiatives volontaires, telles que l'application de certaines normes. Il est a noter que toutes les petites et micro-entreprises quelles que soient leurs secteurs (y compris les activités essentielles) sont dans cette catégorie.

NIS 2 : quel impact en 2024 pour vos entreprises ?

2018 – NIS : la base du système

- La directive européenne (UE) 2016/1148 Network and Information System Security (NIS) définit un cadre général pour assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (SI) des pays européens.
- La Loi adoptée en février 2018 a permis de transposer cette directive en droit français. Elle définit le cadre général pour réguler la sécurité des SI des acteurs essentiels au maintien de l'activité économique et sociétale du pays. Ces acteurs sont d'une part les Opérateurs de services essentiels (OSE), et les Fournisseurs de services numériques (FSN).
- Les obligations concernant les OSE sont de trois niveaux :
  - **L'application de 23 règles de sécurité** aux SIE identifiés par l'OSE sur 4 catégories (gouvernance, protection, défense, résilience).
  - **La notification à l'ANSSI des incidents de sécurité** survenus sur les SIE ;
  - **La coopération en cas contrôle par l'ANSSI** (ou d'un prestataire d'audit qualifié par l'ANSSI).

2024 - NIS 2 : un élargissement important

- **La transposition de la Directive NIS est attenue pour la fin d'année 2024**. Le travail est en cours, dirigé par l'ANSSI, le GIMELEC sera impliqué en S2 2023.
- Les obligations pour les entreprises seront basées sur celles de NIS mais leur application sera progressive par paliers et étagée dans le temps (T+6 mois, T+18 mois…)
- **Les principaux points à retenir à ce stade sont :**
  - Par défaut, **toutes les entreprises des secteurs listés sont concernées** sauf les micro et petites entreprises (<100 salariés), l'ANSSI pourra relever le niveau de certaines entreprises individuellement
  - **Harmonisation des exigences entre Pays Membres de l'UE** (niveaux de sécurité et contraintes associées)
  - Elargissement du champ d'application de 250 entreprises pour NIS 1 à **plus d'un millier d'entreprises pour NIS 2**
  - **Mêmes exigences entre Entités Essentielles et Importantes**, mais des niveaux de profondeur adaptés
  - **Pouvoir de contrôle et d'amende de l'ANSSI avec des sanctions fortes** y compris pour les Entités Essentielles avec un plancher à 7 M€ ou 1,4% du CA en cas de manquements
  - Diffusion attendue des exigences au travers **des relations contractuelles** entre entreprises
  - Reporting obligatoire des incidents de sécurité dans l'entreprise avec **des délais très courts** (entre 24 et 72h après prise de connaissance)
- **Encore beaucoup de questions pratiques mais un calendrier serré !**

Quelles sont les spécificités techniques de l'OT ? Pourquoi faire appel à des spécialistes ?

Des installations à longue durée de vie
Rentabilisation sur plusieurs dizaines d'années
Obsolescence des composants
Difficultés à pérenniser la maintenance

Des composants vulnérables
Pas ou peu de mécanismes de cybersécurité intégrés
Patch management complexe à mettre en œuvre

Une production continue
Considération physique et économique
Disponibilité 24/7
Fenêtre de maintenance réduite

Hétérogénéité et empilement technologique
Besoins variés / spécificités des constructeurs
Différents intégrateurs et gestion par lot
Rénovations et extensions favorisant l'empilement de produits (générations et technologies différentes)

Contraintes environnementales
Poussière, humidité, chaleur, rayonnement électromagnétiques…

Systèmes temps réels
Maîtrise du temps de cycle automate
Maîtrise des temps de réponse

Utilisation de protocoles industriels
Normés ou spécifiques
Pas ou peu de mécanismes de sécurité

Flux de communication
Difficulté à maîtriser les matrices de flux et la visibilité des échanges

Quelles sont les spécificités organisationnelles de l'OT ? Pourquoi faire appel à des spécialistes ?

Environnement réglementaire exigeant
Normes fondamentales
Normes de spécifications
Normes de méthodes d'essais et analyse
Normes d'organisation

Pérennisation de systèmes obsolètes
Maintien en Condition Opérationnelle à moindre coût
Gestion des vulnérabilités : équipements en production et pièces de rechange

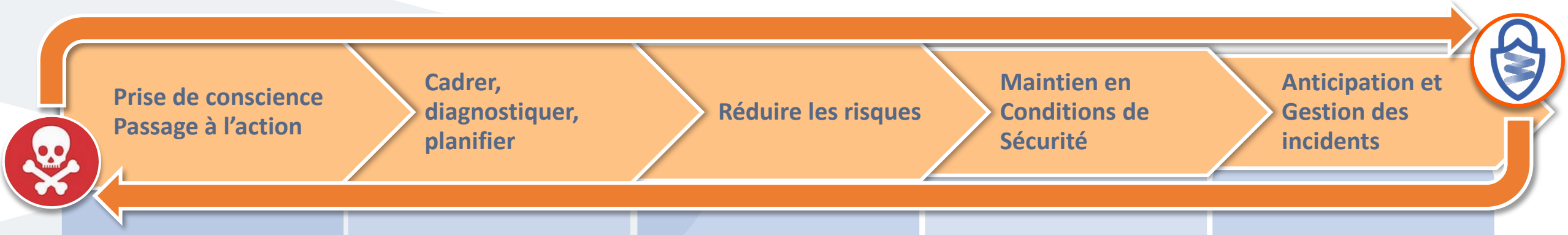
Objectifs et nombre des intervenants
Equipes en 3/8
Exploitant, fournisseur, intégrateur
Opérateur, mainteneur…

Optimisation des coûts par l'externalisation
Perte de la maîtrise de l'installation
Pas ou peu de prise en compte de la cybersécurité dans les plans d'extension, rénovation

12 fausses croyances très usuelles dans la cyber-OT

1. Mes équipements et réseaux industriels sont **isolés d'internet** et donc protégés
2. Je suis protégé car notre OT repose sur des **protocoles et des systèmes d'exploitation spécifiques**
3. L'intégration des mécanismes de cybersécurité (chiffrement, filtrage, authentification) est **incompatible avec la puissance des automates** nécessaires sur mes chaines de production
4. Les mesures de cybersécurité ne sont **pas compatibles avec les contraintes de temps réel** exigées et risquent de ralentir mon système de production.
5. La **cybersécurité coûte cher** ! Autant prendre le risque de payer une rançon ou contracter une assurance !
6. J'ai un **automate de sécurité,** donc je suis protégé.
7. La cybersécurité est juste une **contrainte**, elle ne m'apporte pas de valeur
8. Mon système industriel n'a **aucune raison d'être ciblé** par un attaquant
9. Une attaque cybersécurité se limite au vol de données et n'a **pas d'impact physique sur mon système**
10. Une cyberattaque **n'a jamais tué personne**
11. J'ai **protégé mes postes contre les rançongiciels** donc je suis tranquille
12. La **complexité de mon système est une protection** : il faudra beaucoup de temps à un attaquant pour comprendre le système

Retrouvez nos services et systèmes !



- Sensibilisation du management via la communication des équipes, des autorités et des associations
- Prise de conscience suite à des attaques de concurrents ou partenaires
- Echanges entre équipes IT et OT sur la stratégie cybersécurité
- Rédaction d'un avant projet et d'un cahier des charges pour un premier accompagnement

- Etablir une cartographie initiale du système industriel
- Réaliser un audit organisationnel et technique
- Mener une analyse de risque pour caractériser les ratios Risques / Vulnérabilités
- Faire réaliser des tests d'intrusions sur l'OT
- Réaliser des POC Cyber-OT
- Mettre en place une stratégie cybersécurité industrielle globale et priorisée.
- Planifier son implémentation
- Faire évoluer l'organisation IT/OT sur la gouvernance cyber

- Déployer une campagne de sensibilisation, de formation et de conduite du changement sur les processus IT/OT
- Durcir les systèmes OT :
  - *Mise à jour ou isolement des systèmes obsolètes*
  - *Segmentation réseaux OT*
  - *Sécurisation des accès et des droits utilisateurs*
  - *Gestion et durcissement de tous les périphériques*
  - *Rédaction des procédures*
  - *Gestion des sauvegardes*
  - *Paramétrage sécurité, …*
- Durcir la sécurité physique des sites industriels
- Tests, Commissioning

- Réaliser des Audits réguliers du niveau de sécurité des sites OT
- Veille sur les vulnérabilités et le niveau de menace
- Coordination entre maintenance prédictive et gestion des patchs pour optimiser la disponibilité
- Maintien des cartographies à jour sur les systèmes OT
- Surveillance des installations, planification et remédiation (*Management des logs, analyse du trafic réseau et des données opérationnelles, …*)
- Valorisation des données collectées et de la sécurisation pour optimiser les performances opérationnelles

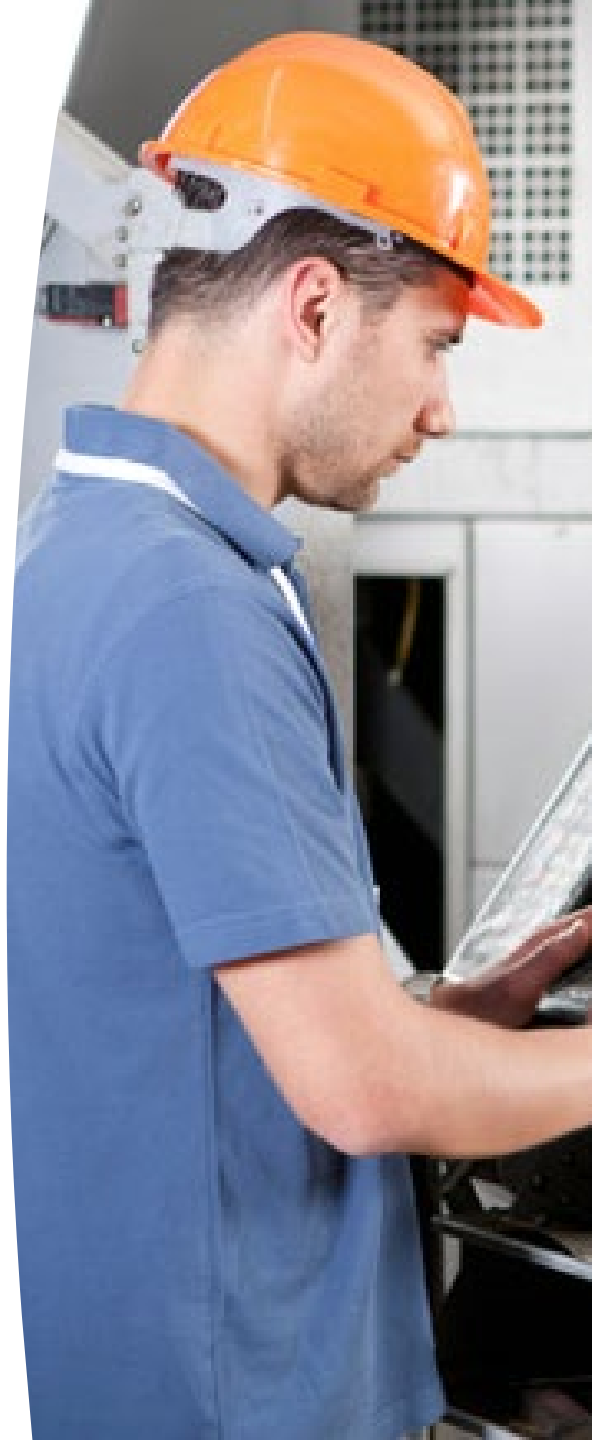
- Préparation du plan de continuité de l'activité
- Tests de reprise après incidents
- Sécuriser une capacité ponctuelle de réponse à incidents, de gestion et de résolution de crise
- Entretien des canaux avec les partenaires cybersécurité (ANSSI, SOC, CSIRT)
- Supervision des mesures de sécurité

Certification ISO et IEC

GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

Focus sur la question clé de la maintenance

- La cybersécurité est une démarche large concernant toutes les phases du cycle de vie des systèmes.
- La prise en compte de la cybersécurité est essentielle lors des phases de conception pour de nouvelles installations, lors de projets de rénovation ou d'évolutions d'installations existantes.
- Malgré cela, les systèmes conçus et intégrés avec des mesures de cybersécurité (dits « **secured by design** ») resteront fragiles et vulnérables à de nombreuses menaces d'origine cyber, compte tenu des contraintes opérationnelles et de la durée de vie des systèmes au regard de l'évolution de la menace.
- **L'enjeu de la maintenance porte cependant en priorité sur les systèmes peu sécurisés, conçus parfois il y a des dizaines d'années, à une époque où le concept de cybersécurité des systèmes industriels n'existait simplement pas.**
- Ces systèmes représentent « malheureusement » aujourd'hui la majorité des systèmes en exploitation. Les personnes en charge de ces systèmes souhaiteront éviter que les opérations de maintenance, très souvent externalisées, soient le principal vecteur d'entrée d'une cyber-attaque conduisant à un incident important.
- Ces enjeux de maintenance du « quotidien » se retrouvent sur le guide ECC4iU (Cluster à l'origine du Club Cyber-OT du GIMELEC) : « Pour la maintenance des installations Industrielles ».
- La maintenance du quotidien est différente **du Maintien en Conditions de Sécurité (MCS).** Cette dernière doit être prévu et défini en amont, lors de la conception et de l'intégration des installations, par des procédures et des moyens techniques. Ces opérations se prévoient et se définissent en amont sur la base des recommandations et des exigences, réglementaires ou non.
- Les principes généraux de la MCS se retrouvent dans le guide de l'ANSSI : Maîtriser la SSI pour les systèmes industriels et mesures détaillées



Nos convictions sur l'évolution de la certification

1. **La cybersécurité est la condition pour la réussite de la transformation digitale des industries**
   - Les produits de notre industrie sont largement utilisés dans toutes les infrastructures industrielles, des plus simples aux plus critiques
   - Ils assurent le contrôle et la sécurité des procédés et des systèmes
   - Nos entreprises investissent massivement afin d'apporter à leurs clients des produits sécurisés, développés et fabriqués dans le cadre de processus internes de sécurité
2. **La certification doit être adaptée aux enjeux du monde industriel**
   - La certification nécessite des référentiels communs internationaux
   - La chaine de valeur toute entière doit être prise en compte
   - Le cycle de vie des produits mis en place par les fabricants doit être intégré dans les schémas de certification de cybersécurité
3. **Le Club Cyber-OT travaille sur des propositions concrètes avec les parties prenantes**
   - **S'appuyer sur le standard industriel de cybersécurité IEC 62443**. Il peut être appliqué à tous les domaines industriels et donne les bases pour la certification, à la fois des produits et de leur cycle de vie (IEC 62443-4-1).
   - **Faire reconnaitre le schéma Certificat de Sécurité de Premier Niveau (CSPN) de l'ANSSI** en Europe et œuvrer davantage pour son adaptation à nos référentiels et cycles de développement
   - **Pour les fabricants ayant certifié le cycle de vie sécurisé du produit, reconnaitre une auto-déclaration de conformité des différentes versions des produits aux standards de cybersécurité**.