NOTE TECHNIQUE

Cybersécurité

When **energy** matters

socomec
Innovative Power Solutions

Objectif du document

Fournir les informations nécessaires afin de répondre à vos questions concernant la cybersécurité.

Méthodologie

Expliquer les principes de base puis présenter les cas d'usage communément installés chez nos clients.

Bien que nous veillons à une sécurisation optimale de nos produits, la robustesse d'une installation dépend également de sa conception globale, car chaque élément, à son niveau, joue un rôle dans la sécurité.
On peut comparer la sécurité d'une installation électrique à une cotte de maille : chaque anneau métallique la constituant, comme le produit, apporte une sécurisation locale. Mais ce qui fait la force de la protection globale est bien l'enchaînement cohérent de chacun des maillons.
Une mauvaise couverture, un trou dans la cote de maille, constitue une faiblesse et le risque de subir une attaque ciblée est décuplé.
Voici le mode d'emploi pour vous accompagner au mieux dans vos choix.

Bonne lecture!

800 000 €

coût moyen d'une violation de sécurité*

Une entreprise subit

29 cyberattaques

par an**

** Source : https://experiences.microsoft.fr/articles/cybersecurite/cybersecurite-chiffres-cles/*

*** Source : https://www.silicon.fr/hub/malwarebytes-hub/cybersecurite-les-10-chiffres-qui-font-peur*

Sommaire

La cybersecurité : définition

« Rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels des états et des organisations ».

Source : Wikipedia

La **cybersécurité,** selon wikipedia, présente des enjeux économiques stratégiques et politiques qui vont donc bien au delà de la seule Sécurité des Systèmes d'Information (SSI). Elle concerne d'ailleurs aussi bien l'informatique de gestion, l'informatique industrielle, l'informatique embarquée que les objets connectés La cybersécurité doit être appréhendée de manière holistique pour prendre en compte les aspects économiques, sociaux, éducatifs, juridiques, techniques, diplomatiques, militaires et de renseignement.

La notion de **cyber-résilience** est une notion complémentaire du management de la cybersécurité, c'est **la capacité du système ou de l'architecture réseau à continuer de fonctionner en cas de panne ou d'attaque.**

Nous verrons à travers ce document comment appréhender globalement la sécurité des informations, en mettant le focus sur nos appareils mais pas seulement.

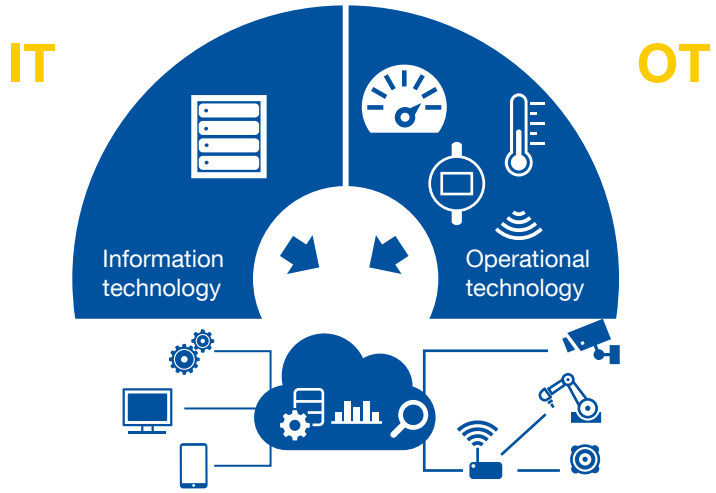
L'objectif étant de faire une proposition globale à nos clients, adaptée à leur besoin et garantissant une solution cohérente, **sécurisée résiliente**.

La cybersecurité : pourquoi ?

Pourquoi le sujet de la cybersécurité est important à prendre en considération ?

Convergence des mondes IT/OT

Définition IT/OT



Historiquement une entreprise industrielle est composée de **deux types d'environnement.**

IT (Information Technology)

OT (Operational Technology)

IT (Information Technology)

• **Définition**
Infrastructure bureautique.

• **Eléments connectés**
PC et serveurs.

• **Niveau de sécurité**
Tous les éléments connectés sur ce réseau sont **homogènes** et **sécurisés** (on retrouve généralement Windows ou Linux).
Les administrateurs de ce réseau ont à disposition un **ensemble d'outils et de services pour maintenir efficacement la sécurité** de l'ensemble (antivirus, firewall, service de déploiement massif de correctifs, mises à jour régulières, service de monitoring d'alerte, etc.).
Ils peuvent **déployer des correctifs rapidement** qui se diffusent sur tous les postes du réseau.
Par ailleurs, le parc informatique est renouvelé fréquemment (**cycle de vie court** de 3 à 5 ans), ce qui évite de garder des produits obsolètes ou électroniquement peu fiables.

OT (Operational Technology)

• **Définition**
Environnement industriel de process.

• **Eléments connectés**
Du capteur communiquant, aux automates industriels, en passant par les compteurs, les moteurs communiquant leurs positions… et l'ensemble des éléments des chaines de production.

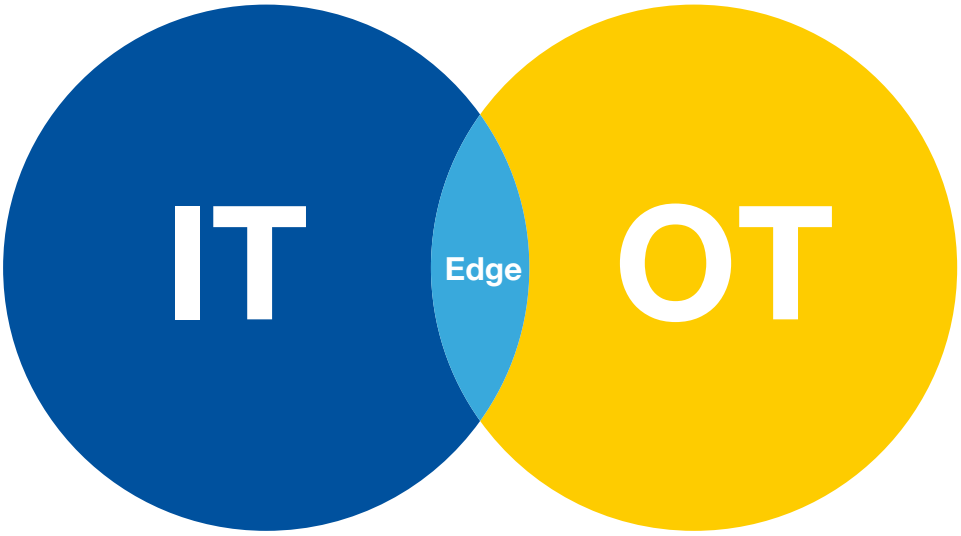
• **Niveau de sécurité**
Tous ces éléments ne sont pas capables de communiquer entre eux du fait de leur **hétérogénéité**. L'ensemble n'est **pas sécurisé dès la conception** car jugé trop couteux jusqu'à présent, et ne bénéficie pas de services communs de maintenance comme la mise à jour.
De plus, ces produits coutant chers et conçus pour durer, ont des cycles de vie d**e 10 à 20 ans**, voire plus. Ainsi un équipement vulnérable peut rester longtemps dans l'entreprise, laissant une porte ouverte suffisamment longtemps pour pourvoir être exploitée.

Remonter les informations des usines pour optimiser les processus et les consommations.

OT : de plus en plus ouvert & communiquant

Pendant longtemps l'OT est resté très vulnérable et peu sécurisé. La seule protection valable et fiable était d'isoler cet environnement de l'entreprise pour ne pas exposer ses vulnérabilités.
Cependant, depuis quelques années, nous assistons à l'essor de la vague **IoT** (Internet of Things) et **industrie 4 0.**
La cause ? Le besoin de remonter les informations des usines pour optimiser les processus et les consommations.
Surveiller, contrôler, optimiser le process industriel (OT) à partir des bureaux ou du **Cloud**, c'est-à-dire de l'environnement IT, devient alors nécessaire & le réseau OT ne peut en conséquence plus être isolé.
Ainsi nous assistons à une convergence des deux environnements qui, malgré leur différence par nature, doivent communiquer.

L'Edge : zone de convergence sensible



Pour faciliter la convergence de l'IT & de l'OT, on observe une zone d'échange, appelée **Edge**, frontière entre l'environnement industriel et la bureautique.
Dans cette zone, on retrouve des équipements pratiquant des conversions de langage pour passer un message d'un environnement à l'autre.
Ces équipements sont généralement des **passerelles (ou gateway)**, et sont connectés simultanément à l'OT et à l'IT. Elles sont en charge de prendre un message de l'IT, de le transformer de manière compréhensible, avant de l'envoyer sur l'OT, et inversement.

Un hackeur préfère entrer dans une entreprise par son côté connecté le moins protégé, et c'est l'OT qui remporte le suffrage !

Ces équipements sont dans un environnement très exposé :
- proches de l'internet, grande source d'attaque,
- ou connectés à l'IT, exposant les vulnérabilités de l'OT.

Cette zone étant particulièrement sensible, il faut y apporter un maximum de sécurité, notamment en sécurisant les gateways et leur environnement.

Aujourd'hui, l'établissement du Edge se fait souvent sans protection et sans prendre en considération les fragilités et les vulnérabilités industrielles, ce qui explique l'accélération des attaques industrielles !
Un hackeur préfère entrer dans une entreprise par son côté connecté le moins protégé, et c'est l'OT qui remporte le suffrage !

Une accélération des attaques

Chiffres & statistiques

En parcourant la brève histoire de l'informatique, on peut noter que les premières attaques dans le secteur industriel ont débutées en novembre 2007. Le célèbre virus **Stuxnet** a ouvert la voie à une vague d'attaques dans le secteur qui n'a cessé de s'accélérer.
Créé soi-disant par les gouvernements américano-israéliens, Stuxnet avait pour objectif d'attaquer les installations nucléaires de l'Iran et de ralentir leur programme nucléaire. Bien que ces systèmes ne fussent pas connectés à Internet à l'époque, les installations ont été compromises par une diffusion à travers des clefs USB !
Cinq entreprises liées au programme nucléaire ont été piratées.
Des centrifugeuses et des vannes ont été sabotées afin d'engendrer leur destruction physique, tout en remontant des informations erronées aux superviseurs pour ne pas éveiller les soupçons.

Dès lors, ce modèle d'attaque sur les environnements industriels a été répliqué… ces attaques sont significatives puisqu'elles peuvent toucher des process avec de gros enjeux financiers, provoquant des casses de matériels et/ou des impacts sur les humains.

Santé et numérique: faire face aux menaces de cyber-attaques
[Par Stéphane Astier et Claire Lefebvre]
Depuis plusieurs années, les attaques cyber contre les systèmes informatiques des établissements de santé se multiplient : les hôpitaux ont représenté près de 11 % des cyberattaques recensées en France en 2020 et la tendance s'est poursuivie en 2021 avec, entre autres, la cyberattaque de l'AP-HP confirmée le 12 septembre dernier…
Source Haas Avocats

Plus de la moitié des entreprises françaises victimes de cyberattaques
[CESIN – Club des Experts de la Sécurité de l'Information et du Numérique]
Le CESIN vient de dévoiler la 7e edition de son baromètre annuel, réalisé par OpinionWay. Premier constat, 2021 fut une année faste pour les cybercriminels : plus d'une entreprise sur deux déclare avoir subi entre une et trois attaques ayant fait mouche. Et 60 % des entreprises rapportent que ces attaques ont perturbé leur activité.
Source L1FO – CESIN – GlobalSecurityMag – UD – IT Social

Une cyberattaque perturbe la distribution d'essence en Iran
L'Iran fait face a une pénurie d'essence d'ampleur nationale depuis plus de 24 heures. Une cyberattaque a paralysé des stations-service à travers le pays, bloquant l'accès aux pompes par carte électronique et laissant la population dans le désarroi.
Source LMI – SN – Siecle Digital

Pour la deuxième fois en un an, Annecy victime d'une cyberattaque
Les services informatiques de la ville de Haute-Savoie sont de nouveau hors service depuis ce matin à la suite d'une attaque informatique. Les démarches en ligne et les messageries électroniques sont indisponibles.
Source UD

Cyberattaque contre le port de Houston : les cybercriminels s'en prennent aux infrastructures critiques
Le grand port américain de Houston vient de révéler avoir été la cible le mois dernier d'un piratage soupçonné provenir d'un Etat-nation. Les cybercriminels auraient implanté un logiciel malveillant et tenté de voler des informations d'identifications Microsoft. Cependant, les équipes de l'autorité portuaire ont déclaré s'être défendues avec succès contre cette tentative de piratage confirmant qu'aucune donnée ou système opérationnel n'a été touché.
Source UnderNews

159 collectivités locales
ont été la cible d'un piratage en 2020*

119 entreprises
françaises ont été la victime d'une cyberattaque en 2020

Au cours des 12 derniers mois,
18 millions
de personnes ont été
victimes d'une attaque en France,
d'apres une étude menée par Norton**

** Selon le GIP Acyma (Anssi).*
*** Source UD..*

Les attaques visant les données

Les attaques dans les milieux industriels ciblent généralement les données. Plusieurs scénarios sont envisagés.

- **Surveillance malveillante :** la donnée est détournée à des fins de surveillance malveillante. Il peut s'agir de données économiques ou stratégiques qui seront revendues au marché noir à la concurrence. Cela peut également être des données techniques qui permettront à des personnes malveillantes de préparer une attaque.

- **Donnée modifiée :** cette attaque a pour but d'influencer une facturation ou un process industriel en modifiant les données.

- **Donnée supprimée :** suppression de données ou d'informations par exemple du CRM, afin de mettre en difficulté l'entreprise ciblée.

Les attaques visant les processus industriels

Les attaques industrielles peuvent cibler le process industriel, à travers :

- **une modification de la donnée :** par exemple : changement de consigne de production, modification de la valeur de tarification, modification ou effacement de la personne intervenue en maintenance, changement de droits d'accès…

- **une prise de contrôle directe** des actionneurs afin de perturber un process ou de le détruire, voire même de toucher l'humain.

85 %
Risque financier

45 %
Risque sur les données

30 %
Risque d'interruption de l'activité / des opérations

29 %
Risque de réputation pour l'entreprise

Impacts des attaques

Ces attaques ont des impacts financiers, qui se cumulent : perte de production, de chiffre d'affaires, pénalité dû à la perte de disponibilité, départ de clients mécontents…
Les conséquences d'une attaque sur l'image de l'entreprise sont également conséquentes, dénotant l'incapacité à se protéger et à protéger ses clients, d'autant plus si l'entité n'a pas réagi avec un plan de communication et d'actions réactifs.

Que protéger ?

La sécurité du système permet de se protéger d'erreurs de manipulation et/ou d'usage malintentionné.
Une analyse est généralement menée afin de déterminer quelles sont les ressources à protéger (données sensibles ou équipements comme les gateways).
Une autre approche est de considérer les différents scénarios redoutés ce qui permet d'identifier les mesures de protection à déployer.
Dans tous les cas, une protection efficace vise à couvrir la confidentialité et l'intégrité des informations, la disponibilité du process et la traçabilité des actions qui y sont menées.

Confidentialité des données

La confidentialité est la garantie que les données échangées ne sont pas accessibles aux utilisateurs non autorisés.

Toute information sensible ne doit pas être dévoilée à des tiers non autorisés. On parle ici bien entendu des mots de passe, données personnelles, mais également de données d'exploitations dites sensibles, de données d'administration/maintenance…

Ex : une personne non autorisée intercepte le fichier csv des index envoyé au serveur FTP distant. Un faux serveur FTP usurpe l'identité du vrai serveur pour recevoir les fichiers envoyés.

Disponibilité du process

La disponibilité est la garantie que les données sont disponibles à tout utilisateur autorisé, lorsqu'il en a besoin.

Ex : une attaque qui a pour objectif "d'inonder" la passerelle de requêtes jusqu'à ce que cette dernière plante dans le but d'interrompre l'accès aux données.

Intégrité des informations

L'intégrité est la garantie que le système, sa configuration et ses données sont fiables et n'ont pas subie de modifications non autorisées.

On s'assure également que le système reste intègre et que son fonctionnement n'a pas été modifié par un biais non maitrisé.

Traçabilité des actions

La traçabilité permet de garantir l'authentification des utilisateurs et d'imputer la responsabilité des actions menées.

Cette propriété est essentielle en cybersécurité car elle détermine qui a fait quoi et à quel moment…

Comment protéger ?

Etape #1 : faire un audit

Etape #1 : faire un audit

Tracer le parcours de la donnée & identifier tous les points d'entrée potentiels d'une attaque (physiques, wire, wireless etc.).

Produits connectés & APPs locales > *Réseau de communication* > *Plateforme Cloud & service web* > *Web & mobile APPs* > *Services Expert*

Génère la donnée	>	Transmission de la donnée	>	Centralisation & stockage de la donnée	>	Exploitation de la donnée

Etape #2 : identifier les points sensibles

Etape #2 : identifier les points sensibles

Une fois le parcours de la donnée tracé, il s'agit d'identifier les points sensibles du parcours afin d'identifier où la sécurité doit être renforcée.
La protection recommandée est définie selon **la sensibilité des données & la vulnérabilité du lieu de transit, sans faire de surenchère.**

Etape #3 : mettre en place le plan d'action

Etape #3 : mettre en place le plan d'action

A	B	C
Construction ou modification de l'architecture pour **sécuriser la chaine globale**	**Sélection de systèmes** intégrant un niveau de sécurisation adapté	Mise en place d'une **organisation cybersécurisée**

A Construction ou modification de l'architecture pour sécuriser la chaine globale

De nombreux moyens existent pour se protéger : sauvegardes, chiffrement des informations, canaux de communication cryptés,….
Seulement, il est essentiel que **ces mesures soient réparties sur toute la chaine pour garantir une couverture globale et suffisante.**
Focaliser exclusivement sur un élément est une erreur car, même si ce maillon est ultra renforcé, le système reste faillible à cause de la faiblesse de son environnement…
En distillant de la sécurité sur chacun des éléments de la chaine de valeur, la donnée peut suivre son parcours sans risque d'être captée ou modifiée frauduleusement.

Pour plus d'informations, voir la section «La proposition Socomec - protection des architectures».

Pour plus d'informations sur les standards, voir page 12

Cette approche d'amélioration continue permet d'intégrer la sécurité dans l'ADN de l'entreprise…

B Sélection de systèmes intégrant un niveau de sécurisation adapté

Sécuriser l'ensemble de la chaine globale suppose évidemment de sélection les systèmes qui la composent de manière judicieuse. Pour s'assurer que le système sélectionné a un niveau de sécurité suffisant voici quelques critères à vérifier.

Critère #1 : la conception du produit "security by design"

Pour garantir un bon niveau de sécurité, la cybersécurité doit être envisagée dès la conception du produit, pour des usages donnés, en le plaçant dans son environnement final.
Dans une approche de « security by design » il est impératif d'envisager la sécurisation du produit mais également des architectures dans lesquelles il sera branché selon l'usage.

Critère #2 : les standards

La question de la cybersécurité au niveau des entreprises se trouve à un tournant.
L'intensification de la législation en Europe et en France introduit un changement de paradigme sur la question. L'obligation réglementaire étant dorénavant introduite, les considérations actuelles des entreprises sur la cybersécurité évoluent. Un produit ou système répondant aux exigences d'une norme ou d'un standard est un gage de qualité.

C Mise en place d'une organisation cybersécurisée

Pour être efficiente, la démarche doit également s'appuyer sur une organisation orientée cybersécurité afin de **sécuriser la conception en amont** et d'assurer au client **le soutien et l'assistance en aval**.

Approche organisationnelle et gestion des risques

Ainsi une fois les risques identifiés, on détermine pour chacun le ratio entre :
- la probabilité qu'il se réalise,
- l'impact d'un tel événement.

En fonction de ce ratio, on détermine les mesures de protection pouvant être appliquées :
- la réduction du risque, en réduisant son impact potentiel,
- la prévention du risque, en réduisant la probabilité qu'il se produise,
- le partage du risque avec un prestataire,
- l'acceptation du risque, par exemple si la mesure à mettre en place coûte trop cher par rapport au risque.

Amélioration continue

Ce Plan de Traitement du Risque est alors décliné en plan d'actions.
Ces actions peuvent être très diverses, allant de la mise en place d'un pare-feu à la formation des équipes en passant par la définition de processus de communication et de transmission des informations…
Ce plan d'actions peut bien entendu être décliné sur le long terme, et inclut notamment un contrôle opérationnel afin de s'assurer du bon fonctionnement sous cette nouvelle organisation.
Des indicateurs clés régulièrement analysés permettent d'identifier en continue les axes d'amélioration et en conséquence d'adapter le plan d'actions.

Conformité

Cette approche est très pragmatique et est appropriée pour chaque entreprise. Afin de s'assurer que tous les pans de la cyber sont couverts, il convient de suivre des lignes directrices éprouvées et reconnues internationalement.
Un ensemble de normes guide cette démarche et apporte un poids supplémentaire quant à la cohérence du processus, à sa reconnaissance et la confiance mis dans cette nouvelle organisation ISO 27001.

Spotlight sur les normes & standard

L'impact de la LPM sur l'industrie	La loi pour la Programmation Militaire (LPM) en vigueur depuis 2013 a permis d'identifier et de classer plus de 200 entreprises - Opérateurs d'Importance Vitale OIV privés et publics - qui exploitent ou utilisent des installations jugées indispensables pour la survie de la nation. L'obligation de mise en conformité va accélérer le processus de rapprochement entre OIV et acteurs de la confiance numérique et favoriser le développement d'une industrie pérenne de la cybersécurité.
Transposition de la directive européenne NIS	La directive Network and Information Security (NIS), qui est entré en vigueur en décembre 2018, pose un cadre européen, compatible avec la LPM, que chaque pays aura la responsabilité de décliner sur son territoire. Elle traite des mesures à mettre en place afin d'assurer un niveau élevé de sécurité en matière de systèmes de réseaux et d'information des 27 États membres de l'Union Européenne. En France, un cadre réglementaire a été définit pour renforcer la cybersécurité des opérateurs de services qui sont essentiels au fonctionnement de l'économie et de la société (OSE). Fin 2019, on en dénombre 600. Décembre 2022, la version 2 de la directive est entrée en vigueur élargissant les acteurs concernés. On parle dorénavant d'entités essentielles et importantes.
Réglementation sectorielle	En dehors des obligations qui découlent de la LPM, il existe de nombreux textes ou règlementations en vigueur pour les entités privées et publiques. Deux émergent largement au niveau industriel et rayonnent internationalement.

Normes ISO 27001

Cette norme s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) et définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI).
Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme.

L'objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. Cela apportera la confiance des parties prenantes.

L'ISO/CEI 27001 énumère un ensemble de points de contrôles à respecter pour s'assurer de la pertinence du SMSI, permettre de l'exploiter et de le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002 classées dans 14 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de faire certifier un organisme ISO/CEI 27001.

Standard IEC 62443

(standard dans le secteur industriel et nucléaire)

L'IEC 62443 est une norme internationale multi industrie. Elle liste un ensemble de standards, de rapports techniques et d'informations relatives aux implémentations sécurisées industrielles.
Cet ensemble est organisé en **4 catégories générales** appelées Général, Politiques et procédures, Système et composants.

- La première catégorie inclut les informations fondamentales comme les concepts, modèles et terminologies.
- La seconde catégorie cible le propriétaire du produit. Elle aborde les différents aspects de la création et de la maintenance d'un programme de sécurité.
- La troisième catégorie décrit un guide de conception pour le système et les exigences pour l'intégration sécurisée de ce système. Son cœur est basé sur le modèle de zone et de conduits.
- La quatrième catégorie décrit le développement de produit spécifiques et les exigences techniques.

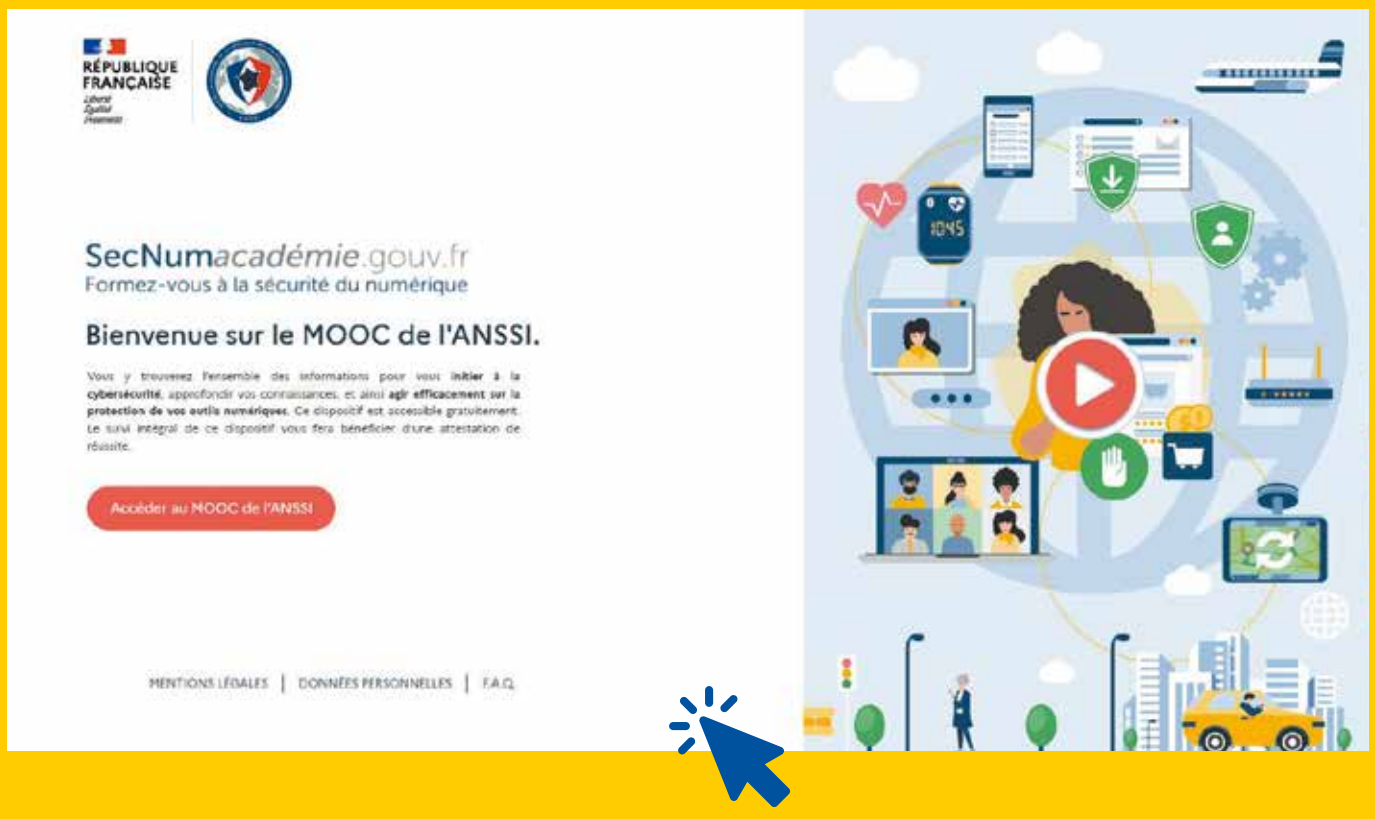
Pour aller plus loin…

L'Agence Nationale de la Sécurité des Système d'Information (ANSSI)

Se perfectionnant, le secteur de la cybersécurité se retrouve donc de plus en plus encadré et certifié par des labels.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé par décret en juillet 2009.
Ce service à compétence nationale est rattaché au secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.
Aujourd'hui, l'ANSSI a toujours une mission de défense des systèmes d'information de l'État mais elle est aussi chargée d'une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale.
L'ANSSI propose deux niveaux de certification, effectuées par tierce partie.
La certification permet d'attester par une tierce partie indépendante et impartiale qu'un produit dispose d'un niveau de sécurité conforme aux services de sécurité qu'il avance, et que sa résistance lui permet de résister à un certain niveau d'attaques donné.

Formez-vous à la cybersécurité en ligne !



La proposition Socomec

Socomec a toujours eu à cœur d'intégrer la sécurité dans ses produits afin de garantir la sureté de l'installation et de protéger ses utilisateurs. Les produits évoluent et leur conception devient plus complexe puisqu'elle intègre de nouvelles couches technologiques comme l'électronique ou l'informatique.
De plus, les fonctionnalités apportées à nos clients se globalisent, puisqu'elles ne sont plus portées par un produit unique et isolé, mais par un système, composé d'un ensemble de produits, de réseaux de communication, en passant par des serveurs virtualisés sur le Cloud et leurs applicatifs.

Socomec et la cybersécurité

Comme évoqué dans le précédent chapitre, sécuriser uniquement les produits n'a pas grand intérêt : il faut s'intéresser à l'ensemble de la chaîne de valeur pour obtenir un niveau de sécurité suffisant.
Les maillons de cette chaîne sont bien entendu les produits mais également les moyens de communications, les données qui y circulent, etc.
C'est pourquoi Socomec propose des **solutions intégrées** afin de garder une maitrise de la chaine globale et de garantir un niveau de sécurité suffisant sur tous les éléments de la chaine.
Même si de nombreux tests sont réalisés à tous niveaux (développement, labo, intégration), chez Socomec, la sécurité est un sujet essentiel et nous tenons à **qualifier toutes nos offres par des tiers extérieurs.**
Ainsi, en toute impartialité, les attestations délivrées par ces organismes **certifiés 27002**, garantissent la sécurité et l'homogénéité de toute la chaine de valeur. Ainsi, l'entreprise mène des travaux sur les produits sensibles (type passerelle), sur les architectures dans lesquelles ils sont installés, mais aussi sur l'optimisation de l'organisation qui permet d'encadrer l'ensemble.

Protection des produits Socomec

Dans une architecture technique, Les premiers produits sensibles sont les **passerelles de communication.**

Pourquoi les passerelles sont-elles particulièrement sensibles ?

Une passerelle concentre les connexions où transitent toutes les informations. Ce carrefour de l'information est le lieu idéal si l'on souhaite supprimer, modifier les données.
De plus, les passerelles apportent la première connectivité sur le média Ethernet ce qui permet un accès facile à partir de l'extérieur.
Cette facilité permet d'opérer à distance discrètement sur un canal grande vitesse pour tenter plusieurs modes opératoires de hacking en simultané.

Comment sont sécurisées les passerelles Socomec ?

Produits Ethernet sécurisés

Les produits Ethernet Socomec sont renforcés et compatibles avec la norme industrielle internationale ISO/IEC 62443-4-2. Cette norme, reconnue internationalement par son exigence, permet de garantir une couverture complète des domaines sécuritaires devant être traité.

Politique de mots de passe robuste

Pour accéder aux profils « Utilisateur avancé », « Admin » ou « Cyber sécurité » qui permettent de modifier la configuration, une politique de mots de passe plus robuste a été mise en place sur le web server :

- **les mots de passe par défaut doivent être modifiés lors de la 1ère connexion**. Ceci empêche qu'une personne non autorisée connaissant les mots de passe par défaut accède au menu de configuration,
- **les nouveaux mots de passe doivent remplir certains critères de robustesse** (minimum 10 caractères, une minuscule, une majuscule, un caractère numérique et un caractère spécial),
- **les mots de passe doivent être changés au moins une fois par an** pour accéder à nouveau au menu de configuration,
- **protection contre les tentatives d'usurpation d'identité :** après 3 tentatives de connexion erronées, l'utilisateur sera banni temporairement pendant une heure. Cela évite que des programmes malicieux ne puissent accéder au système.

De plus, les **mots de passe sont cryptés**, ce qui empêche un hackeur de les utiliser s'il parvient à les intercepter.

Les avantages à travailler avec Socomec

Prise en compte de la sécurité dans la conception et la réalisation de nos produits (certification norme ISO 27001)

Produits Ethernet sécurisés, conformes à la norme internationale ISO/IEC 62443

Audits réguliers des produits et de leurs usages dans les architectures cibles par des tiers certifiés

Cloud souverain Socomec

Produits concernés

Passerelles de communication DIRIS Digiware M-xx

DIRIS Digiware D-xx (à partir de la version 2.2)

DATALOG H80 (à partir de la version 2.5)

Carte NetVision (à partir de la version 7.2)

Politique de sécurité personnalisée

L'utilisateur Cyber sécurité peut **personnaliser sa politique de sécurité en fonction de son application** pour réduire l'exposition de la passerelle/de l' afficheur à d'éventuelles cyber-attaques. Il pourra par exemple :

- désactiver le port USB et le port RS485 s'ils ne sont pas utiles,
- désactiver les protocoles de communication non utilisés (BACnet, SNMP),
- désactiver certains services (écriture Modbus pour empêcher les modifications de configuration).

Protocoles de communication chiffrés

Les passerelles et afficheurs sont compatibles avec les versions sécurisées des protocoles de communication en utilisant des **certificats numériques de type SSL/TLS**. Le certificat a un double but : il chiffre la donnée échangée entre client et serveur et permet une vérification de l'identité du serveur distant par le client.

- **HTTPS pour la navigation web**. Les scripts échangés entre la passerelle (serveur) et le navigateur web (client) sont chiffrés pour empêcher un hackeur de les analyser, les interpréter et finalement les réutiliser à des fins de cybercriminalité.
- **FTPS** (export csv) et **SMTPS** (email) pour l'envoi de données depuis la passerelle (client) vers un serveur distant.

Pare feu

L'utilisateur peut renseigner **un nombre de requêtes maximum par seconde et un débit max en bit/s**. Quand un attaquant dépasse l'un de ces paramètres, il sera bloqué pendant 1 minute.

Autres fonctions de sécurité

- Mise à jour sécurisée (véritable firmware certifié).
- Stockage sécurisé des données personnelles (chiffrement AES 256).
- Contrôle de l'integrité des fonctions de sécurité au démarrage.

De manière générale, notre but est de fournir à nos clients un système exposé le moins possible aux cyber-attaques, et d'assurer que la configuration de la passerelle, sa hiérarchie et les données historisées ne sont pas perdues en cas de cyber-attaque.

Accès local

Cloud

Sans fil

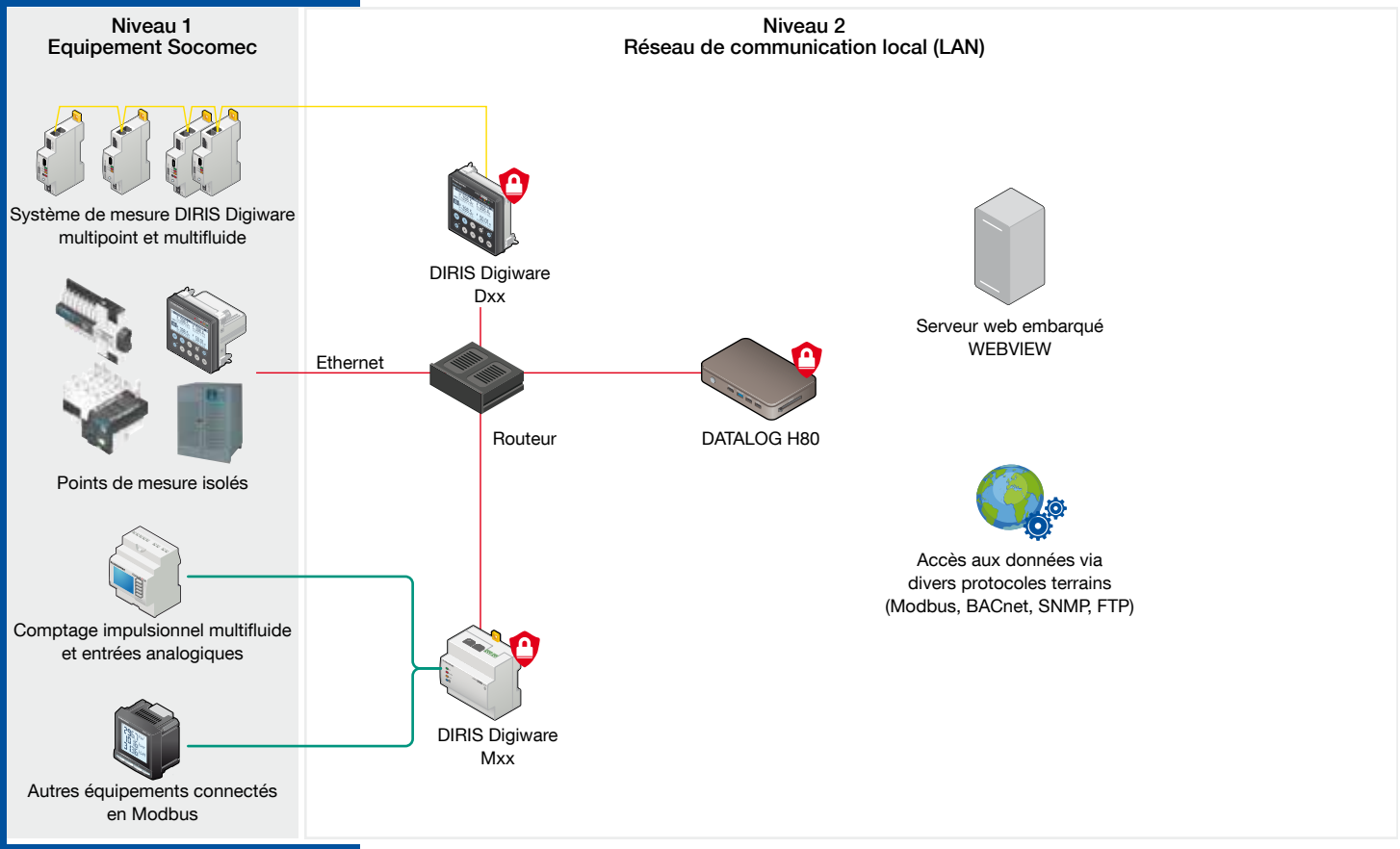
Protection des architectures

Les architectures de référence ci-dessous couvrent les cas d'utilisation les plus fréquents. Nos produits sont conçus afin de répondre à ces besoins et de manière à s'intégrer nativement de cet environnement. Tous nos tests et qualification vérifient cette compatibilité et la résilience de l'installation lors de tentative d'intrusion.

Accès local

Principe

Cette installation permet de monitorer l'ensemble des données des produits de manière locale et centralisée. L'affichage des données se fait au travers d'afficheurs locaux ou via une application de type WEBVIEW embarquée dans les passerelles de communication DIRIS Digiware M, les afficheurs DIRIS Digiware D, le DATALOG H80, ou encore les centrales multi-mesure DIRIS A-40. Plus on monte dans la hiérarchie, plus l'équipement est en capacité de monitorer l'ensemble des produits qui lui sont connectés.



Intégration de fonctions de securité et audit par un organisme extérieur indépendant, spécialiste agréé en cybersécurité.

Préconisations

- Isoler les équipements de mesure sur un réseau dédié (équipements réseaux séparés ou VLAN spécifique).
- Désactiver les fonctions non utilisées.
- Changer les mots de passe par défaut.
- Changer les mots de passe régulièrement.

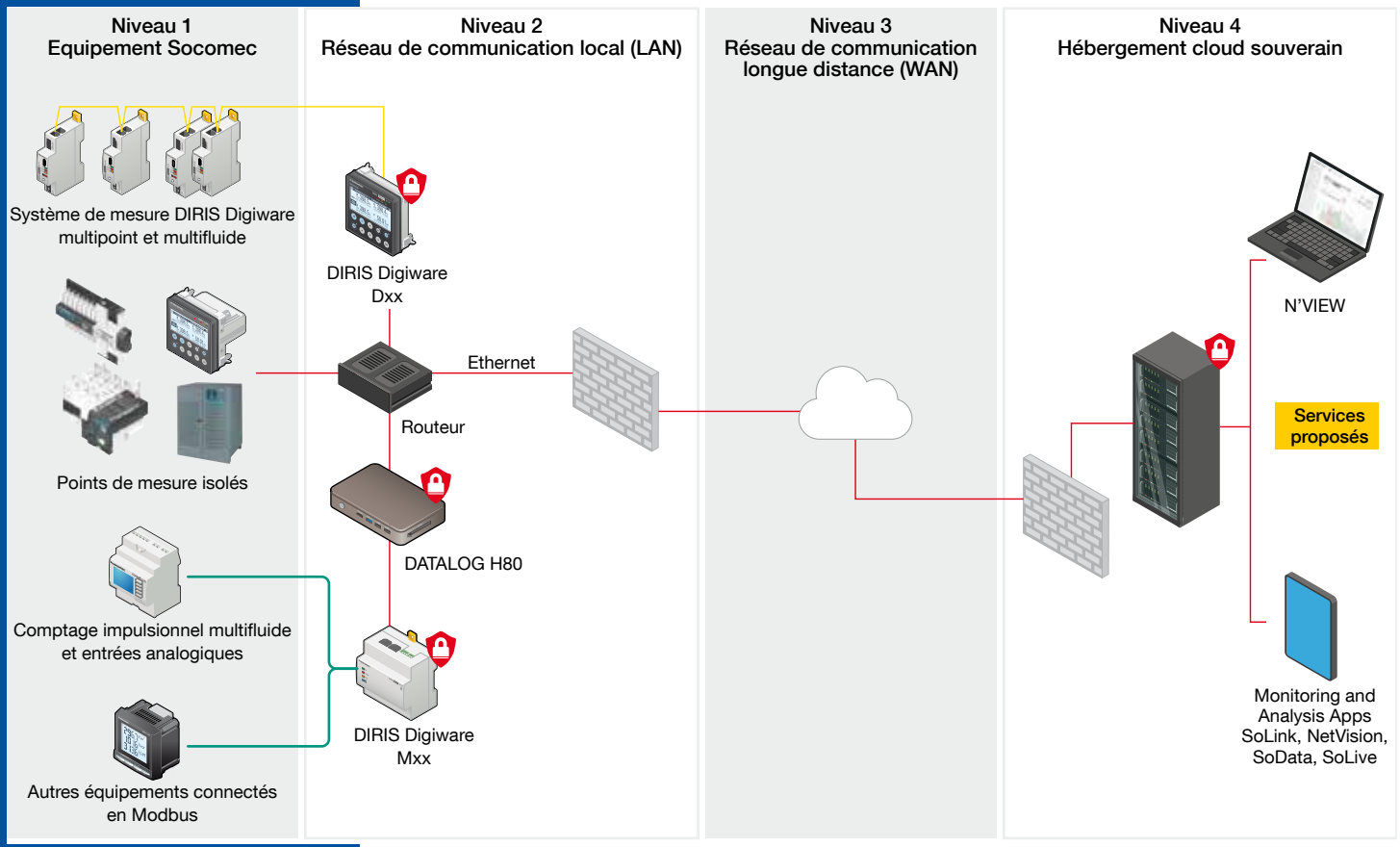
Proposition Socomec

- Politique mots de passe robustes.
- Accès aux produits protégés par mot de passe, modifiables par les personnes habilitées.
- Maitrise des fonctions sécurités via un site web protégé, accessible uniquement par les personnes habilitées.

Cloud

Principe

Ce cas d'usage donne la possibilité de monitorer les données de l'entreprise (un ou plusieurs sites) à partir de l'Internet.
Pour ce faire, les données locales mesurées par les produits sont remontées sur Internet de manière centralisée et sécurisée, sur le Cloud. Des applications dédiées et sécurisées sur le Cloud exploitent ensuite ces données afin de donner des informations sur l'installation.
L'envoie des données hors entreprise se fait de manière sécurisé via des protocoles cryptés (FTPs, HTTPs, MQTTs).



Préconisations

- Autoriser l'accès distant aux équipements uniquement au travers de connexions authentifiées (VPN sur le pare-feu à placer entre les équipements et Internet).
- Filtrer les adresses IP sources ayant accès à l'équipement au travers du routeur Internet.
- Activer sur l'équipement (Mxx, Dxx, Datalog H8x) la fonction datalogueur (push données /export des données sur serveur distant) qui permet la remontée des données sur le Cloud.
- Ouvrir les ports au niveau du Proxy/FW de votre entreprise selon le protocole choisi (HTTPS : TCP 8080 ; FTPS : TCP 990…) - généralement géré par le service IT.

Proposition Socomec

- Accès aux produits protégés par mot de passe, modifiables par les personnes habilitées.
- Maitrise des fonctions sécurités via un site web protégé, accessible uniquement par les personnes habilitées.
- Cloud souverain Socomec certifié ISO 27001 et HDS : stockage des données sur la zone France, maitrise de la sécurité et des données, scalabilité.
- Sécurité de l'ensemble de la chaine attestée par un organisme extérieur indépendant, spécialiste en cyber sécurité.
- Applications dédiées à une utilisation Cloud (robustesse, scalabilité, tenue de charges, protections pour ce type d'environnement…).

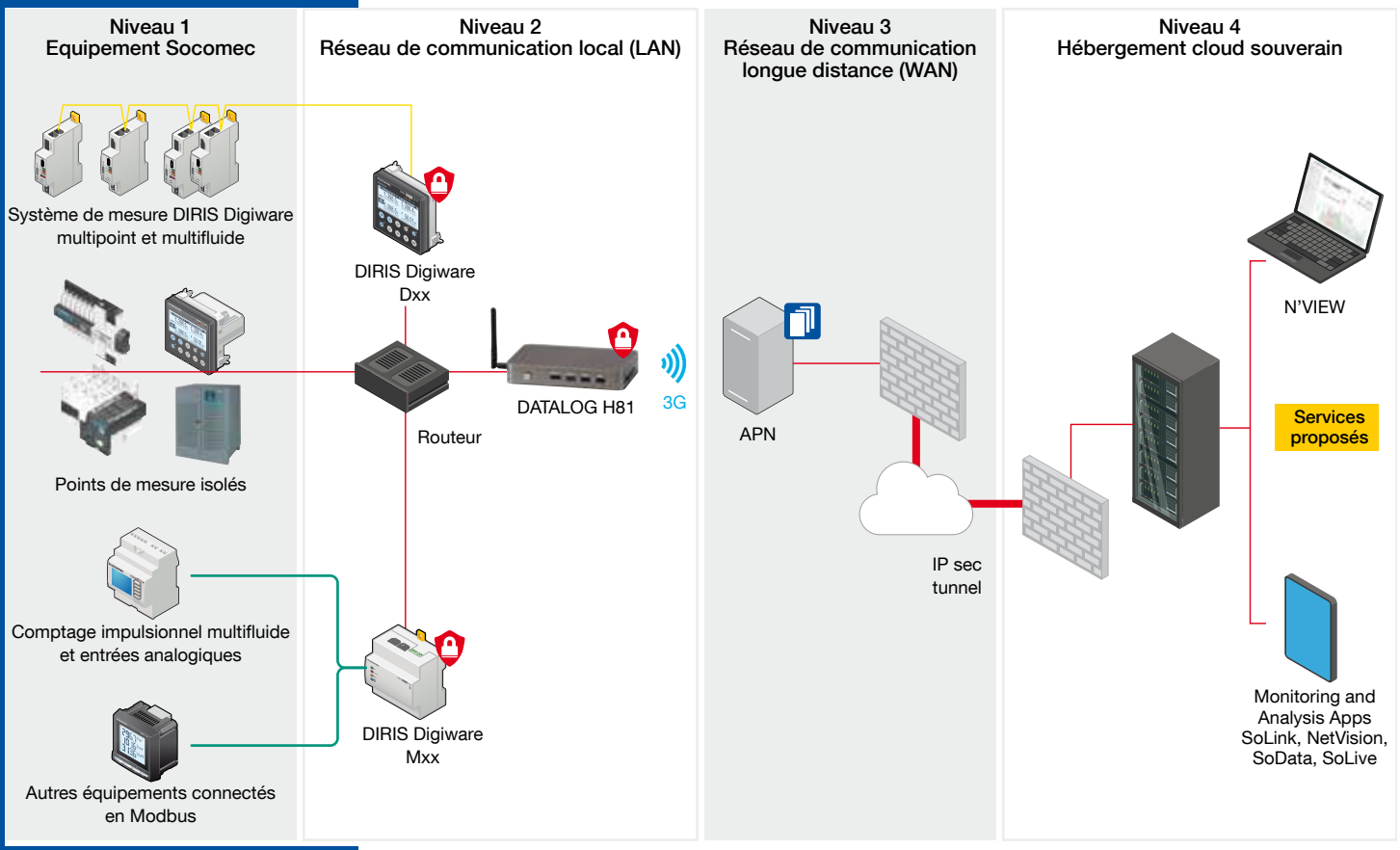
Sans fil

Principe

Infrastructure trop restreinte ou inexistante ? Passez par les airs !
L'utilisation des réseaux mobiles permet de s'affranchir des contraintes existantes du terrain (contraintes IT, infrastructures rigides ou inexistantes…).

Architecture 3G

La connexion sans fil est assurée par une passerelle fournie par Socomec (H81) accompagnée d'un abonnement (3G).
La sécurisation des flux de données et leur stockage est assurée par nos installations, hébergées en France (Cloud souverain).



Préconisations

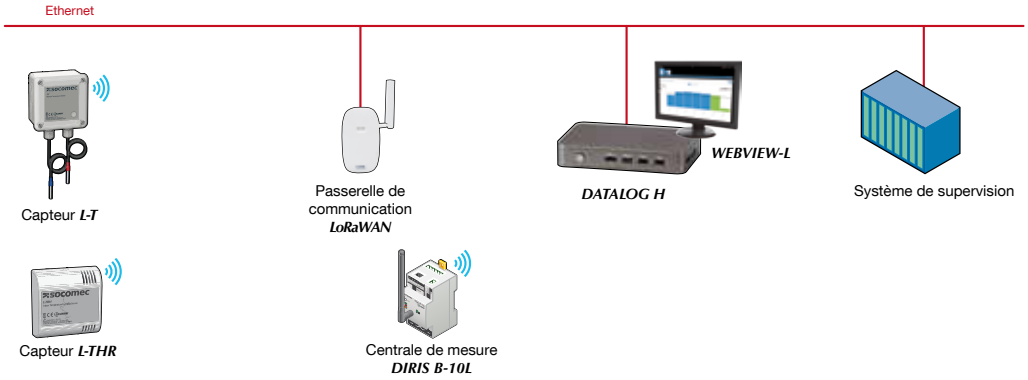
- Isoler les équipements de mesure sur un réseau dédié (équipements réseaux séparés ou VLAN spécifique).
- Activer uniquement les services nécessaires.

Proposition Socomec

- Accès 3G/4G assuré dans le monde entier.
- Configuration simplifiée pour une installation rapide et sécurisée.
- Cloud souverain Socomec : stockage des données sur la zone France, maitrise de la sécurité et des données, scalabilité.
- Applications dédiées à une utilisation Cloud (robustesse, scalabilité, tenue de charges, protections pour ce type d'environnement…).

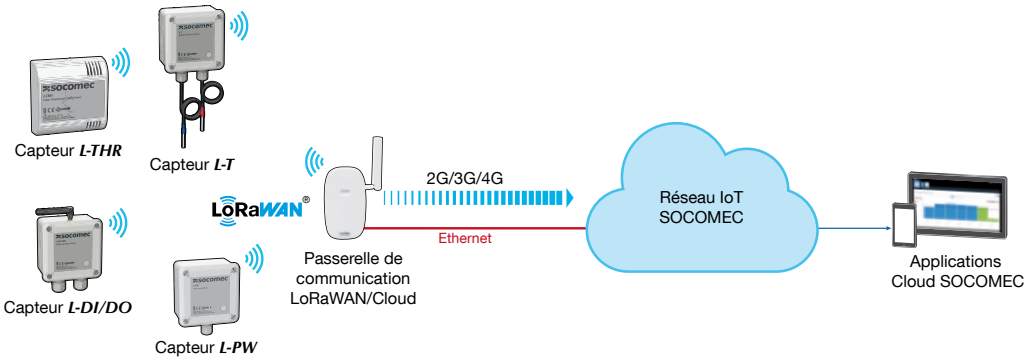
Architecture locale

Réseau privé avec exploitation locale des données de mesure.



Architecture Cloud

Réseau privé avec envoi des données de mesure vers une plateforme Cloud.



Protection par l'organisation

Socomec a décidé de renforcer son organisation afin de garantir la confidentialité, l'intégrité et la disponibilité des informations lors de la création d'un nouveau produit/service.
Cela garantit la maitrise de la circulation des informations et donne l'assurance qu'elles ne pourront pas être utilisées pour corrompre un produit durant sa conception.

L'**ISO/IEC 27001** est une norme internationale de sécurité des systèmes d'information.
Elle s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) et définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI).

Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme. L'objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. Cela apportera la confiance des parties prenantes.

Afin d'apporter cette assurance à nos clients, notre organisation est certifiée ISO 27001 sur le périmètre IoT.

Découvrez nos certificats ISO.

Glossaire

APN

Access Point Name ou APN, appelé aussi identifiant du point d'accès réseau, est un identifiant qui permet à un utilisateur de téléphonie mobile d'un
réseau 2G, 3G ou 4G de se connecter à Internet en identifiant le Gateway GPRS Support Node (GGSN pour la 2G et la 3G) ou le Packet Data Network
Gateway (PGW pour la 4G) qu'il doit utiliser. L'APN est généralement constitué d'un identifiant alphanumérique et des codes MCC et MNC permettant d'identifier l'opérateur de réseau mobile. Le téléphone va lui-même compléter l'identifiant alphanumérique par le code MCC et MNC qu'il déduit de l'IMSI de la carte SIM du téléphone.

Audit d'architecture

Étude de la conformité d'un système d'information par rapport aux exigences de l'environnement métier.

Cloud

Processus consistant à utiliser des serveurs inforamtiques distants au travers des réseaux Internet. Le cloud permet aux entreprises de stocker leurs données dans des serveurs externes, et d'y avoir accès à distance. Il existe 3 types de clouds : cloud public, cloud privé et cloud hybride. Le cloud est devenu au fil des années un atout incontournable et indispensable pour toutes les entreprises qui souhaitent à la fois évoluer et faire face à la concurrence

Cloud souverain

Selon une circulaire du Ministère de l'Intérieur et du Ministère de la Culture datant d'avril 2016, le cloud souverain est "un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de cloud sont physiquement réalisés dans les limites du territoire national par une entité de droit français et en application des lois et normes françaises." Autrement dit, le cloud souverain est une notion complémentaire d'un service de stockage de données, focalisée sur le fait de protéger au maximum les données hébergées en fonction du droit français. Les spécificités de ce cloud sont d'être hébergé et géré par un prestataire français, non affilié à une entreprise étrangère, et disposant d'infrastructures situées en France et respectant la loi et les normes en vigueur. Cette certification garantit donc que les données stockées soient soumises au contrôle des autorités françaises et que les hébergeurs soient en règle avec la loi.

Coeur de réseau

Le cœur du réseau peut être défini comme « le centre » du réseau informatique. De façon beaucoup plus concrète, lorsque vous envoyez « une information » d'un site A vers un site B, cette information envoyée du site A est récupérée par le cœur du réseau puis transmise au site B. Le cœur du réseau est donc le point de concentration et de distribution des informations. Dans la pratique, ce cœur de réseau est constitué d'un Switch encore appelé commutateur réseau et d'une protection électrique.

Cybersécurité

Ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non- répudiation).

Cyberrésilience

Capacité à se préparer et s'adapter à des conditions en perpétuelle évolution ainsi qu'à récupérer rapidement ses capacités suite à des attaques délibérées, des accidents, des catastrophes naturelles ou encore des incidents dans le cadre de l'utilisation de moyens informatiques et de communication. (Source : http://www.ab-consulting.fr/blog/non-classifiee/cyber- securite-vs-cyber-resilience).

Cybercriminalité

Ensemble des infractions pénales commises sur ou au moyen d'un système informatique, généralement connecté à un réseau.

Edge

L'edge computing (informatique en périphérie ou informatique en périphérie de réseau, est une méthode d'optimisation employée dans le cloud computing qui consiste à traiter les données à la périphérie du réseau, près de la source des données. Il est ainsi possible de minimiser les besoins en bande passante entre les capteurs et les centres de traitement des données en entreprenant les analyses au plus près des sources de données. Cette approche nécessite la mobilisation de ressources qui peuvent ne pas être connectées en permanence à un réseau, tels que des ordinateurs portables, des smartphones, des tablettes ou des capteurs. L'edge computing permet aussi d'éviter la transmission de données nombreuses et peu pertinentes vers les centres de données ou le cloud, apportant fluidité et rapidité de réaction,

Industrie 4.0

Le concept d'industrie 4.0 ou industrie du futur correspond à une nouvelle façon d'organiser les moyens de production. Cette nouvelle industrie s'affirme comme la convergence du monde virtuel, de la conception numérique, de la gestion (opérations, finance et marketing) avec les produits et objets du monde réel. Les grandes promesses de cette quatrième révolution industrielle sont de séduire les consommateurs avec des produits uniques et personnalisés, et malgré de faibles volumes de fabrication, de maintenir des gains.

IoT

IoT est le raccourci utilisé pour désigner «l'Internet Of Things» ou en français «l'Internet des objets connectés».
Le terme d'IoT fait généralement référence à l'écosystème des objets connectés qui comprend le marché de ces objets, mais également tous les modèles économiques et marketing issus de leur développement.

Local Area Network (LAN)

Système de communication permettant de relier quelques centaines d'ordinateurs et de périphériques dans un rayon de quelques kilomètres. Apparu dans les années 1970, le réseau local a connu un essor considérable avec le développement de la micro-informatique dans les années 1980 et l'avènement de la norme de communication Ethernet. A l'inverse, le réseau étendu (WAN) peut regrouper des milliers d'ordinateurs séparés par des centaines, voire des milliers de kilomètres.

LoRaWAN

LoRaWAN est un protocole de communication radio fondé sur la technologie LoRa. Dans le cadre de l'Internet des objets, il permet de structurer un réseau étendu à basse consommation (LPWAN), intégrant des équipements terminaux à faible consommation électrique par l'intermédiaire de passerelles.
(Source : Wikipedia).

Pare-feu ou Firewall

Outil permettant de protéger une ou des machines connectées à un réseau des attaques externes (filtrage entrant) et de bloquer les connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes (source : ANSSI).

Passerelles (ou gateway)

Dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet. Le plus souvent, elle sert également de pare-feu, de proxy, effectue de la qualité de service, etc. (source : Wikipedia).

Sécurité des Systèmes d'Information (SSI)

Ensemble des moyens techniques, organisationnels, juridiques et humains mis en oeuvre pour empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement d'un système d'information.

Security by design

Méthode qui consiste à prévoir la sécurité d'un produit (ou d'un système) au moment de sa conception, en partant du principe qu'il soit nécessairement exposé à un certain nombre de menaces potentielles ou réelles, dans le cadre usuel de son fonctionnement.

Virtual Private Network (VPN)

Système permettant de créer un lien direct entre des machines distantes, en isolant ce trafic du reste du système d'information. L'utilisation d'un VPN est fortement recommandée lors de l'utilisation de ressource de l'entreprise depuis l'extérieur.

Wide Area Network (WAN)

Type de réseau de télécommunications (ou un réseau informatique) capable de couvrir une zone géographique très vaste comme la superficie d'un ou de plusieurs pays réunis, voire la planète toute entière. Le fonctionnement d'un WAN repose sur la technique de la liaison point à point qui consiste à établir une connexion entre un opérateur (Free, SFR, Bouygues Telecom par exemple pour la France) et le réseau d'un client via une ligne louée (ligne en cuivre comme pour la téléphonie classique ou en fibre optique).

Socomec, l'innovation au service de votre performance énergétique

1 constructeur indépendant

3 900 collaborateurs dans le monde

10 % du CA consacrés au R&D

400 experts dédiés aux services

L'expert de votre énergie

COUPURE

MESURE

CONVERSION D'ÉNERGIE

STOCKAGE D'ÉNERGIE

SERVICES EXPERTS

Le spécialiste d'applications critiques

- Contrôle, commande des installations électriques BT.
- Sécurité des personnes et des biens.
- Mesure des paramètres électriques.
- Gestion de l'énergie.
- Qualité de l'énergie.
- Disponibilité de l'énergie.
- Stockage de l'énergie.
- Prévention et intervention.
- Mesure et analyse.
- Optimisation.
- Conseil, déploiement et formation.

Une présence mondiale

12 sites industriels
- France (x3)
- Italie (x2)
- Tunisie
- Inde
- Chine (x2)
- USA (x3)

28 filiales et implantations commerciales
- Afrique du Sud • Algérie • Allemagne • Australie
- Belgique • Canada • Chine • Côte d'Ivoire
- Dubaï (Emirats Arabes Unis) • Espagne • France • Inde
- Indonésie • Italie • Pays-Bas • Pologne • Portugal
- Roumanie • Royaume-Uni • Serbie • Singapour
- Slovénie • Suisse • Thaïlande • Tunisie • Turquie • USA

80 pays
où la marque est distribuée

SIÈGE SOCIAL

GROUPE SOCOMEC
SAS SOCOMEC au capital de 10 607 040 €
R.C.S. Strasbourg B 548 500 149
B.P. 60010 - 1, rue de Westhouse - F-67235 Benfeld Cedex
Tél. 03 88 57 41 41 - Fax 03 88 57 78 78
info.scp.isd@socomec.com

VOTRE CONTACT

www.socomec.com

100 years OF SHARED ENERGY

socomec Innovative Power Solutions

DOT 01031 01 fr - 02/23 - Photo : Martin Bernhart - Réalisation : Socomec - Gyss Imprimeur Obernai