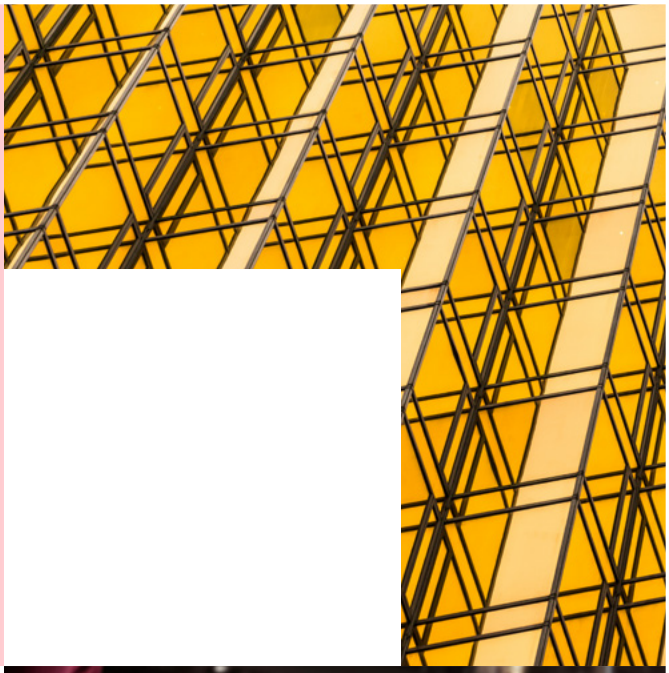


L’industrie 4.0 et la cybersécurité

Comment protéger votre organisation contre les cyberrisques

CGI

Sommaire exécutif

L'adoption des technologies de l'Industrie 4.0 et l'introduction des ambitions de l'Industrie 5.0 entraînent d'énormes changements dans l'industrie manufacturière. Les chefs de file du secteur manufacturier, appuyés par la technologie, se concentrent sur l'offre de services, l'hyperpersonnalisation et la fabrication durable, tout en améliorant l'efficacité et la qualité opérationnelles.

La transformation de l'industrie est stimulante, mais le risque de cybermenaces a augmenté pour plusieurs raisons, notamment :

- l'utilisation d'équipement existant qui n'aurait jamais dû être lié aux réseaux numériques;
- le manque de sensibilisation des employés et les fuites accidentelles;
- le travail à distance en raison de la crise de la COVID-19;
- la technologie et les chaînes d'approvisionnement vulnérables.

La cybersécurité est une considération absolument essentielle pour les entreprises numériques depuis plusieurs années maintenant et elle doit se retrouver dans la mire du conseil d'administration. Dans le secteur manufacturier, le programme La voix de nos clients CGI 2021* révèle un lien étroit entre la transformation numérique et la sécurité de l'information et des opérations. En effet, il s'agit d'un domaine d'intérêt clé pour les dirigeants du secteur manufacturier, puisque 90 % d'entre eux placent la sécurité des technologies de l'information et des technologies opérationnelles (TI et TO) parmi les principales catégories de dépenses. De plus, 79 % des répondants estiment que la formation et la sensibilisation des employés sont des éléments fondamentaux de la cybersécurité, suivis de près par les programmes qui visent à tester les capacités d'intervention organisationnelle.

Avec l'arrivée des usines numériques et de la chaîne de valeur connectée, les pratiques et solutions de sécurité en TI traditionnelles ne consistent qu'en une demi-mesure en ce qui concerne la protection des organisations manufacturières.

Le présent document met l'accent sur les cyberrisques auxquels sont confrontés les activités manufacturières et les usines, les systèmes de contrôle industriel (SCI) et les appareils industriels connectés. Grâce aux meilleures pratiques de l'industrie et à la vaste expérience de CGI dans ce domaine, nous partageons une méthodologie permettant d'évaluer et de sécuriser votre environnement de technologie opérationnelle. Nous présentons également des recommandations et des mesures efficaces que les dirigeants, les directeurs d'usines et le personnel opérationnel peuvent appliquer pour évaluer la complexité et la vitesse croissantes des risques de cybersécurité au sein des usines intelligentes et s'y préparer.

* La voix de nos clients CGI 2021 présente 1 695 entrevues avec des leaders des fonctions d'affaires et informatiques (TI), y compris 171 dirigeants du secteur manufacturier, au sujet des principales tendances sectorielles, des priorités et des plans organisationnels et informatiques.

Table des matières

Pourquoi l'industrie 4.0 représente-t-elle une menace existentielle pour les organisations manufacturières?

L'industrie 4.0 favorise une interconnectivité sans égal dans les environnements de production. Ceux-ci utilisent de plus en plus souvent des appareils connectés à l'Internet des objets (IoT) pour surveiller et contrôler leurs systèmes de production, tandis que les centrales des friches industrielles se transforment en usines intelligentes grâce à l'intégration de dispositifs sans fil connectés à l'Internet des objets. En fait, le nombre total d'appareils connectés à l'Internet des objets dans le monde devrait s'élever 75,44 milliards d'ici 2025.[2]

En outre, les capteurs, les réseaux et les appareils connectés sans fil, tels que les téléphones intelligents, les tablettes ainsi que d'autres technologies portables font leur apparition en milieu de travail. Les systèmes de contrôle industriel (SCI) modernes permettent aux ingénieurs de déployer des sites entièrement automatisés et pratiquement sans personnel. Les fournisseurs de systèmes d'acquisition et de contrôle de données (SCADA), de systèmes à commande répartie et de systèmes d'exécution de la fabrication (MES) proposent des interfaces homme-machine ainsi que des dispositifs de communication sans fil. Ceux-ci permettent aux exploitants et aux ingénieurs de prendre les commandes des appareils depuis des sites situés autant à l'intérieur qu'à l'extérieur de l'usine. En outre, les contrôleurs de systèmes à commande répartie sont désormais munis de serveurs intégrés qui leur permettent d'accéder au Web.

Les appareils qui effectuent les travaux les plus essentiels et difficiles dans nos sociétés, telles que le contrôle de la production et de la distribution d'électricité, la purification et la distribution d'eau ainsi que la production et le raffinage de produits chimiques, sont les plus vulnérables dans un réseau industriel. Étant donné que les systèmes de contrôle industriel sont de plus en plus connectés à Internet, la menace de brèches de sécurité et de dommages éventuels aux installations et aux processus est devenue bien réelle. Le spectre des cyberattaques visant les réseaux et systèmes industriels croît de manière exponentielle, ce qui fait de la cybersécurité dans le secteur manufacturier un sujet plus important que jamais.

Avec l'arrivée des usines numériques et de la chaîne de valeur connectée, les pratiques et solutions de sécurité en TI traditionnelles ne consistent qu'en une demi-mesure en ce qui concerne la protection des organisations manufacturières.

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

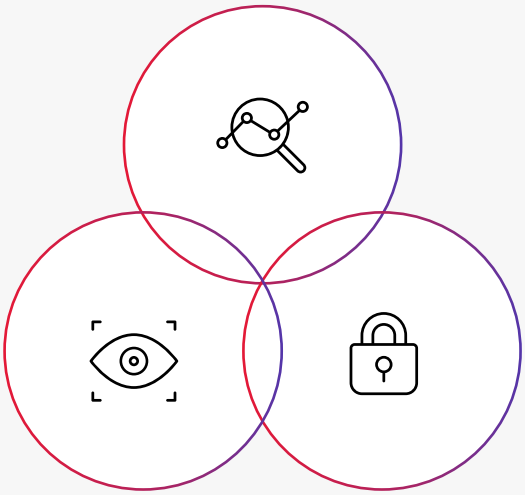
La lutte contre les cyberrisques dans le secteur manufacturier nécessite une solution globale

Avec des usines numériques et une chaîne de valeur connectée, il est nécessaire d'augmenter la sécurité puisque la sécurité actuelle des TI ne suffit plus à protéger les organisations du secteur manufacturier et son renforcement s'impose. Les fabricants doivent adopter une approche globale et complète qui tient compte des personnes, des processus et des technologies pour se protéger de manière adéquate des cyberrisques croissants. Voilà pourquoi nous sommes d'avis que la cybersécurité doit devenir une partie intégrante de la stratégie et de la feuille de route de transformation numérique d'un fabricant, en englobant à la fois les technologies de l'information (TI) et les technologies opérationnelles (TO), qui comprennent les systèmes de contrôle industriels (SCI). Pour y parvenir, il faut adopter une approche sur plusieurs fronts: élaborer des politiques, des procédures et des contrôles de cybersécurité; sensibiliser davantage les employés aux cyberrisques; organiser régulièrement des activités de formation interne pour mettre à jour ses compétences et demeurer au fait de l'évolution des menaces; et recruter les meilleurs professionnels dans le domaine de la cybersécurité.

Dans les pages qui suivent, nous présentons la méthodologie éprouvée de CGI pour cette approche qui vise à aider les organisations à atteindre un niveau de sécurité avancé, à protéger leurs actifs les plus précieux et à assurer la continuité de leurs activités.

Évaluer

Déterminer les risques de sécurité potentiels d'un point de vue organisationnel et technique



Surveiller

Surveiller étroitement l'environnement industriel, les actifs et les connexions

Sécuriser

Atténuer les risques de sécurité recensés liés aux personnes, aux processus et aux technologies

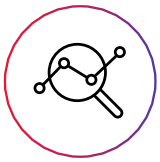
Figure 1 – Méthodologie complète en trois étapes permettant de sécuriser les environnements de la technologie opérationnelle (TO)

Partie 1: évaluation

Déterminer les risques de sécurité potentiels d'un point de vue organisationnel et technique

Pour les fabricants, l'élaboration d'une stratégie de sécurité sûre et solide doit commencer par la détection des risques les plus importants pour leurs processus de production primaires et la détermination des éléments rattachés à leurs actifs les plus précieux. Voici quelques questions importantes à poser.

- Quels systèmes peuvent avoir une incidence sur les processus physiques de l'usine?
- Que se passera-t-il en cas de panne d'un système? Quelles en seront les répercussions?
- En combien de temps les systèmes peuvent-ils être réparés?
- Les systèmes de contrôle industriel sont-ils sécurisés?
- Notre propriété intellectuelle est-elle protégée?
- Notre chaîne d'approvisionnement est-elle vulnérable?
- Que pouvons-nous faire pour protéger l'organisation?



Sécuriser la TO– Partie 1

Créer un aperçu de votre environnement

Évaluation préalable

Déterminer les actifs actuels (personnes, processus, technologies) en s'appuyant sur la documentation existante

Évaluation de la maturité

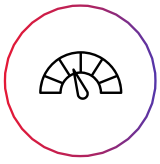
Évaluer le niveau de maturité grâce à des entrevues, des découvertes et des validations dans l'environnement physique ainsi que des simulations

Conformité aux normes de sécurité de la TO

Évaluer la conformité en fonction des normes de CGI ou des clients

Évaluation du réseau de sécurité de la TO

Évaluer le réseau, créer une base de données de gestion des configurations et trouver les vulnérabilités



Évaluation et atténuation des risques

Élaborer un plan d'évaluation et d'atténuation des risques en s'appuyant sur l'évaluation préalable

Rapport sur la sécurité de la TO

Figure 2 – Étapes d'identification des risques de sécurité potentiels

La première étape visant à sécuriser efficacement votre environnement de technologie opérationnelle consiste à l'évaluer en fonction des exigences de conformité, des menaces, des vulnérabilités et des contrôles, ainsi qu'à obtenir un aperçu détaillé du niveau de maturité de votre organisation en matière de sécurité.

Cette évaluation englobe un vaste éventail de mesures de sécurité et la mise en oeuvre de celles-ci dans votre environnement de technologie opérationnelle. Elle comprend les aspects suivants.

1

Évaluation préalable – Cette étape permet de comprendre dans un premier temps quelles mesures de sécurité sont mises en œuvre au sein de l'organisation ainsi que dans le réseau de l'usine ou de la centrale, et comment elles le sont. Dans le cadre de la pré-évaluation, les évaluateurs recueillent alors la documentation disponible telle que les analyses des répercussions sur les activités (ARA), les diagrammes d'architecture réseau, les règles de pare-feu et les politiques de sécurité.

2

Évaluation de la maturité organisationnelle – Cette étape permet de comprendre le niveau de maturité de l'organisation en matière de sécurité. Il s'agit de réaliser des entrevues avec diverses parties prenantes dans l'environnement de l'usine – des opérateurs aux hauts dirigeants – afin d'obtenir une vue d'ensemble de la structure organisationnelle et de la gouvernance de la sécurité, y compris la structure formelle et informelle. Ces entrevues portent sur les normes de sécurité internationales telles que la norme sur la sécurité des systèmes d'automatisation et de contrôle industriels (ISA-99/ IEC 62443), la norme sur la sécurité de l'information (ISO/ IEC 27002), la publication spéciale 800-82 du National Institute of Science and Technology (NIST) ainsi que le cadre de gestion du NIST pour l'amélioration de la cybersécurité des infrastructures essentielles.

Les questions posées doivent notamment porter sur la gouvernance organisationnelle, les politiques et les analyses des répercussions sur les activités (ARA), les cadres de gestion en matière de risques, les plans de continuité des activités, ainsi que sur les mesures de sécurité techniques (protection contre les logiciels malveillants, pare-feu et configuration, correctifs et renforcement de la sécurité, etc.). Il est important de vérifier les réponses par des inspections en usine.

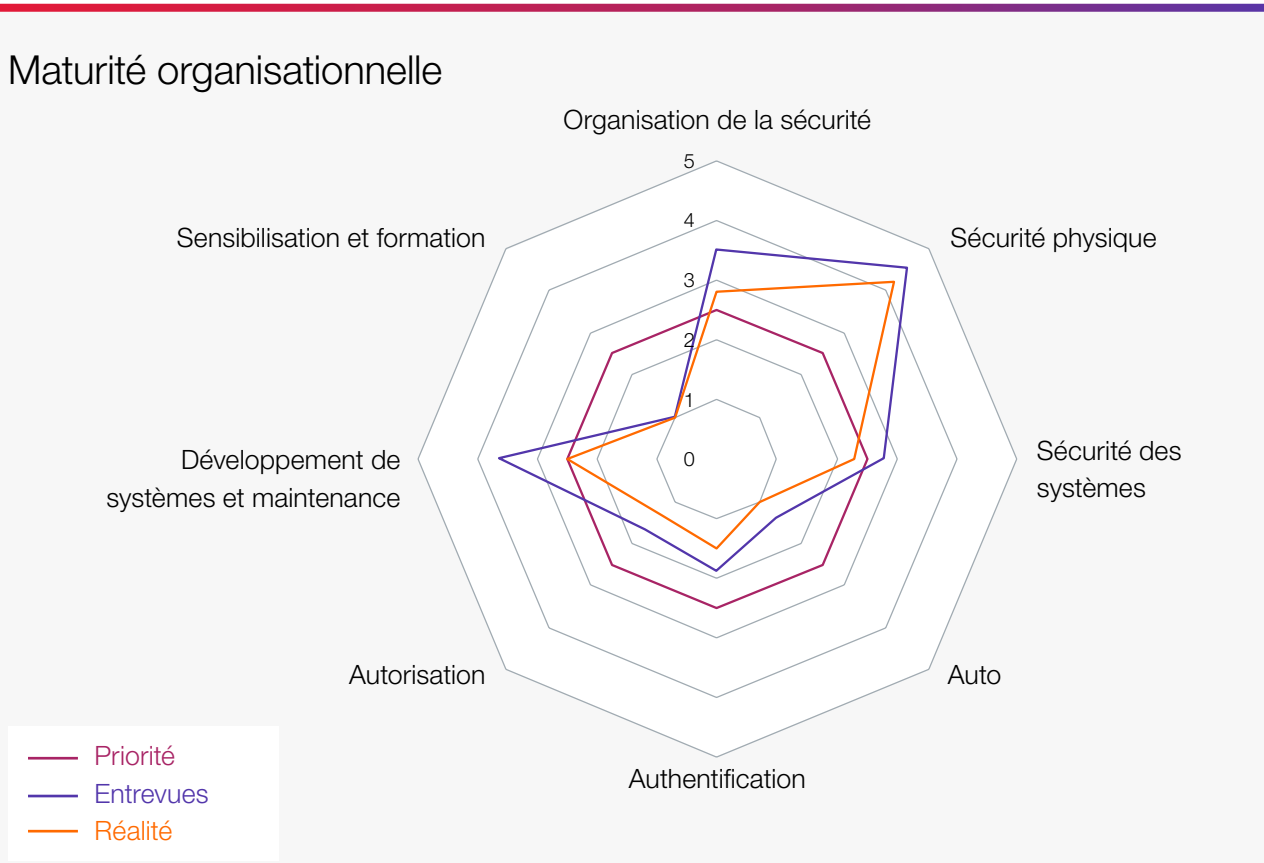


Figure 3 – Multiples diagrammes en forme de toile d'araignée qui aident à visualiser le niveau de maturité de l'organisation en matière de sécurité.

En s'appuyant sur les réponses et leur notation, plusieurs diagrammes en forme de toile d'araignée (figure 3) sont élaborés pour illustrer le niveau de priorité, le niveau déclaré lors des entrevues ainsi que la réalité sur le terrain en fonction des résultats de l'inspection de l'usine ou de la centrale. Ces diagrammes et les renseignements détaillés qui auront été recueillis au cours des entrevues fourniront des indications claires sur les points sur lesquels il faut axer les mesures d'amélioration nécessaires.

3

Conformité aux normes de sécurité de la TO – Bien qu'une évaluation de la maturité organisationnelle mesure le niveau de gouvernance en matière de sécurité de la TO, elle porte expressément sur l'évaluation des mesures pratiques de sécurité de la TO dans l'environnement de l'usine. Des exigences de base complètes en matière de sécurité sont élaborées en fonction de la combinaison de ces deux évaluations. Les thèmes abordés dans l'évaluation de la conformité aux normes de sécurité de la TO doivent notamment comprendre la topologie du réseau, la mise en oeuvre d'une protection contre les logiciels malveillants, la configuration des pare-feu, la gestion des correctifs, les procédures de sauvegarde et le contrôle des identités et des accès. Les résultats de cette évaluation doivent également être vérifiés sur place lors des inspections en usine.

4

Évaluation des risques de sécurité du réseau de la TO – Cette évaluation offre un aperçu détaillé des composants actifs présents dans l'environnement de la technologie opérationnelle. Au cours de cet examen, un ou plusieurs flux de données de l'environnement de la technologie opérationnelle sont extraits de manière non intrusive pour définir les actifs et déterminer l'interaction entre eux ainsi que les protocoles communs utilisés. Un schéma topologique interactif (aussi appelé carte de réseau) (figure 4) est alors créé. On peut comparer les vulnérabilités découvertes à une base de données actualisée des vulnérabilités connues et les signaler à des fins d'élimination. L'information recueillie au cours de cette évaluation peut également être mise à profit pour créer, vérifier ou enrichir la base de données de configuration ou de gestion des actifs d'un fabricant.

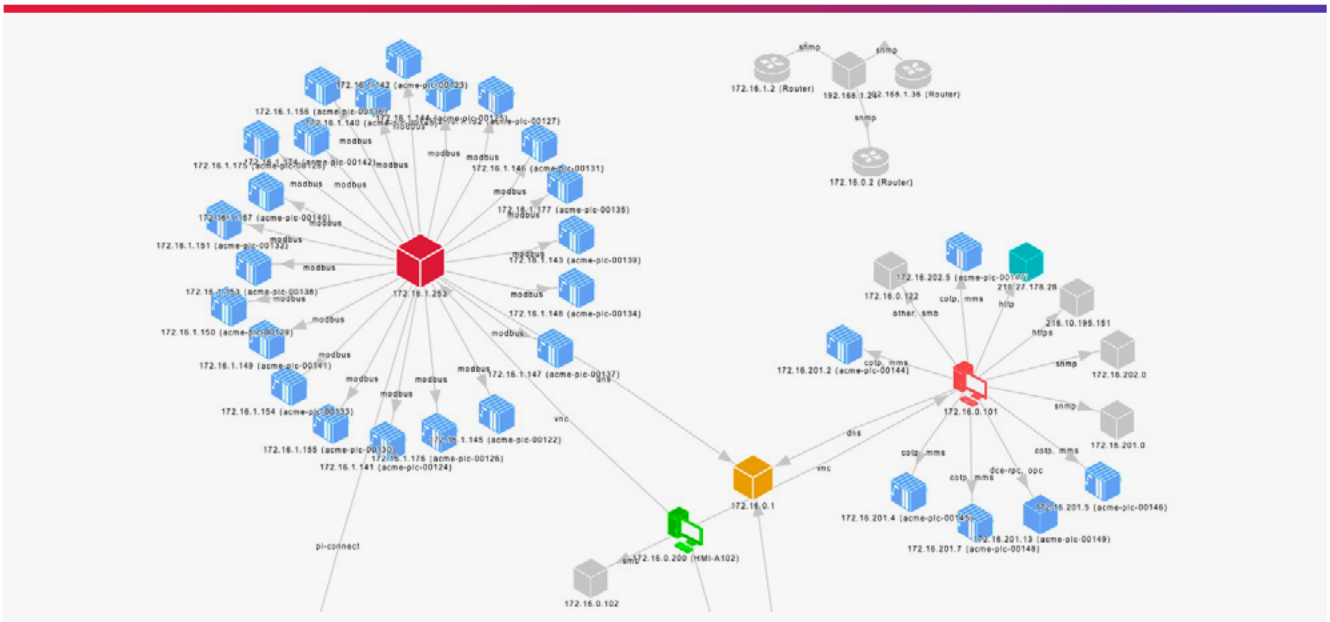


Figure 4 – Exemple d'une carte de topologie de réseau qui illustre les communications régulières axées sur les protocoles TCP/IP (en bleu), les protocoles communs dans l'environnement de la TO (en jaune) et les vulnérabilités potentielles (en rouge).

5

Évaluation et atténuation des risques – Les conclusions tirées des évaluations précédentes sont reflétées sur une carte des points chauds (figure 5) qui illustre de façon concise les risques de sécurité potentiels pour l'environnement industriel de l'organisation. Cette représentation permet de visualiser et de schématiser les risques décelés au sein d'une matrice en fonction de leur incidence et de leur probabilité. À ce stade, on peut déterminer des mesures d'atténuation visant à réduire les risques à des niveaux acceptables, notamment l'établissement de priorités et d'indications budgétaires.

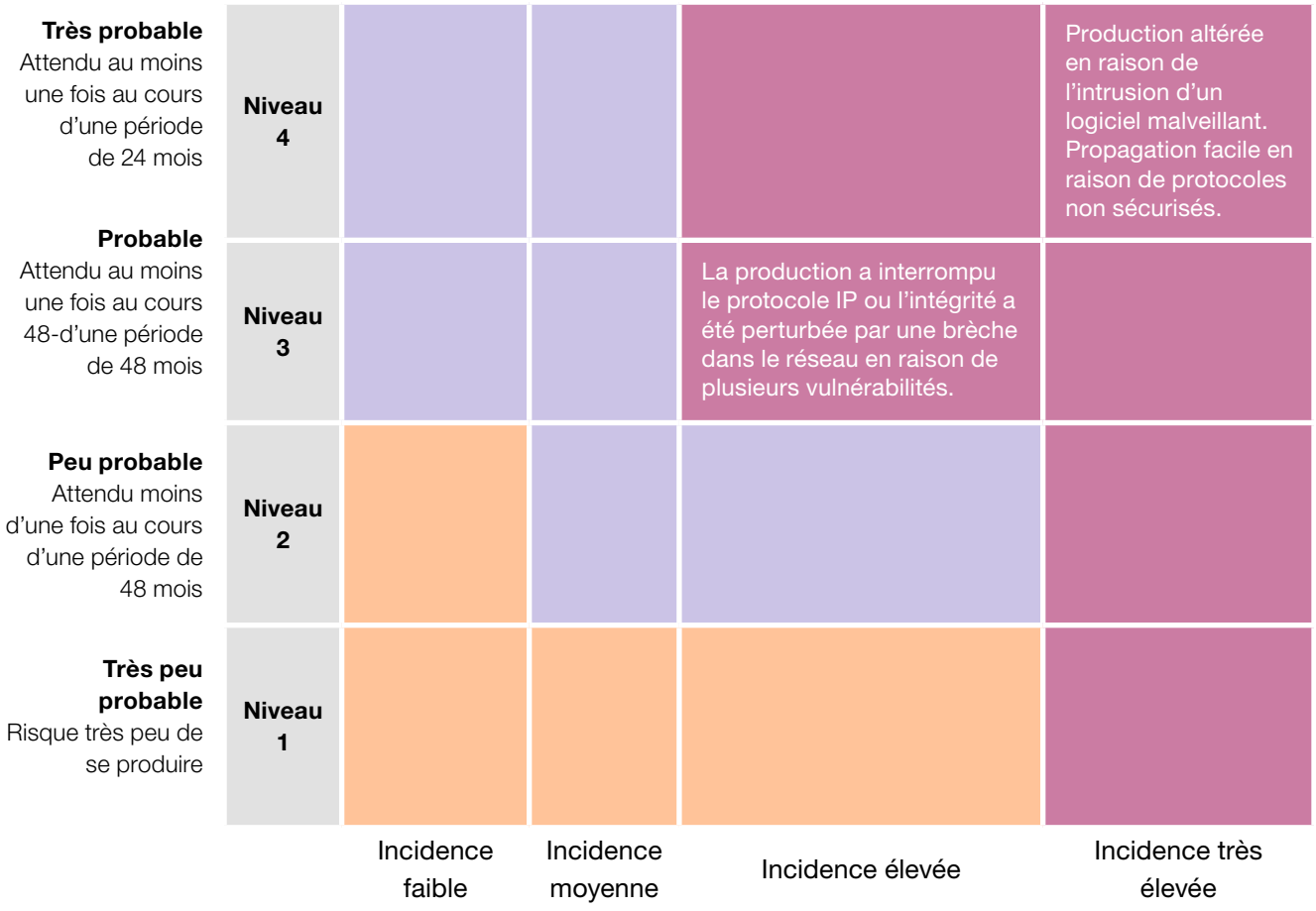


Figure 5 – Exemple d'une carte des points chauds en matière de risques

Production d'un rapport sur la sécurité de la TO

Une fois l'évaluation terminée, les observations et les conclusions qui en sont dégagées peuvent être résumées dans un rapport complet sur la sécurité de la TO. Ce rapport énonce les expositions aux risques et les exigences de base, en plus de fournir des indications claires sur les façons de rehausser la sécurité dans les usines.

Constatations fréquentes

Le diagramme ci-dessous illustre les vulnérabilités fréquemment décelées qui nécessitent des mesures visant à atténuer les risques aux activités. Ces résultats sont fondés sur bon nombre de nos évaluations de divers environnements de technologie opérationnelle dans le secteur manufacturier, le secteur pétrolier et gazier, les services publics et l'industrie alimentaire.

Les chiffres ne représentent pas un classement, mais nous considérons que le manque de connaissance en matière cybersécurité et de gouvernance dans les environnements de technologie opérationnelle constitue la plus grande priorité, car il s'agit du principal facteur d'augmentation des risques. D'après nos évaluations effectuées en 2019, voici les causes les plus importantes de perte ou de détérioration de la disponibilité des systèmes qui nuisent soit à la capacité de production, soit à l'intégrité de ce processus.

- **Intrusion de logiciels malveillants –** L'industrie 4.0, conjuguée à une ou plusieurs des vulnérabilités énumérées précédemment et à de nombreuses méthodes d'attaque, constitue la combinaison parfaite pour les logiciels malveillants. Depuis 2015, on assiste à une croissance exponentielle d'attaques réussies dans les environnements de technologie opérationnelle.
- **Attaques à distance ciblées –** Une connectivité accrue conjuguée à l'intrusion de logiciels malveillants ou aux vulnérabilités énumérées dans le diagramme ci-haut permet aux cybercriminels d'obtenir un accès non autorisé et sans surveillance aux usines et aux centrales.

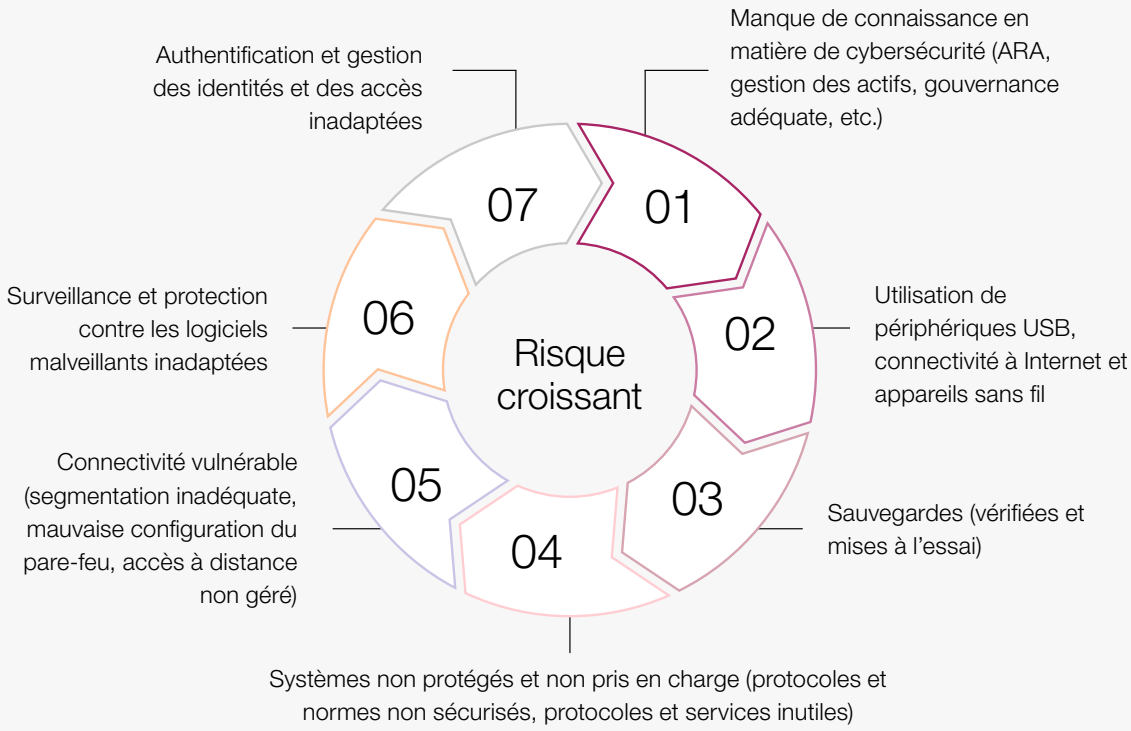


Figure 6 – Vulnérabilités fréquemment décelées

Partie 2: sécuriser

Atténuer les risques de sécurité décelés pour les personnes, les processus et les technologies

L'étape suivante consiste à adopter des mesures de sécurité adéquates pour protéger l'environnement industriel en s'appuyant sur les risques ciblés au cours de l'évaluation de la technologie opérationnelle. Pour le faire correctement, des normes, des lignes directrices et des cadres de gestion de sécurité accessibles au public devraient être appliqués, tels que les normes IEC 62443, ISO 27001 et 27002, la publication spéciale 800-82 du National Institute of Science and Technology (NIST) ainsi que le cadre de gestion du NIST pour l'amélioration de la cybersécurité des infrastructures essentielles.[3] Ces cadres proposent les meilleures pratiques pour des domaines clés comme le renforcement des systèmes informatiques, les zones, les conduits et le contrôle des droits d'accès.

[3] CGI suit de près les nouvelles initiatives de sécurité en matière de TO telles que l'architecture ouverte NAMUR (NOA) et l'Open Process Automation Forum (OPAF). Nous adaptons les nouvelles normes, le cas échéant, dans notre méthodologie de sécurité en matière de TO.

Sécuriser la TO – Partie 2

Sécuriser son environnement

Gouvernance de sécurité de la TO et formation

Mettre en œuvre une gouvernance de la sécurité et une sensibilisation accrue à la sécurité

Conception de référence et politique de sécurité de la TO

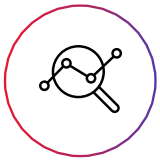
Créer une base de référence pour un environnement de TO sécurisé

Segmentation et renforcement

Segmenter les zones, les conduits, les périphériques et les niveaux de sécurité; renforcer tous les systèmes et composants de réseau et mettre en place une protection adéquate contre les logiciels malveillants

Gestion des identités et des droits d'accès

Contrôler les identités et l'accès aux systèmes et aux réseaux



Surveillance et maintenance

Surveiller et maintenir les personnes, les processus et les technologies

Environnement sécurisé

Figure 7 – Cinq mesures à prendre pour atténuer les risques de sécurité pour les personnes, les processus et les technologies

1

Gouvernance de sécurité de la TO et formation:

- **Faire une distinction claire entre la sécurité des TI et la sécurité de la TO, tout en priorisant ce thème** – L'application des directives de sécurité des TI dans les environnements de TO n'est pas viable, car la manière dont les mesures et les contrôles sont mis en œuvre ainsi que la nomenclature utilisée sont différentes pour ces deux environnements. En outre, les priorités de la sécurité des TI en matière de confidentialité, d'intégrité et de disponibilité sont en fait inversées dans l'environnement de TO. Dans le secteur manufacturier, bien que les processus en tant que tels sont un secret commercial, la sécurité de l'usine est plus importante. Si la sécurité des TI est appliquée à l'environnement de TO, des accidents et des incidents de sécurité peuvent survenir. Par exemple, une décision guidée par les TI peut exiger qu'une porte soit fermée pour des raisons de confidentialité, tandis qu'une décision guidée par la technologie opérationnelle exige que la porte soit laissée ouverte pour que les gens puissent s'échapper en cas d'urgence.

  Une autre raison pour laquelle les priorités sont inversées est que la confidentialité de la TO pourrait probablement être entièrement assurée dans l'environnement de TI. La compréhension de ces principes et de la différence entre les cultures TI et TO s'avère essentielle pour améliorer et optimiser la sécurité des deux environnements.

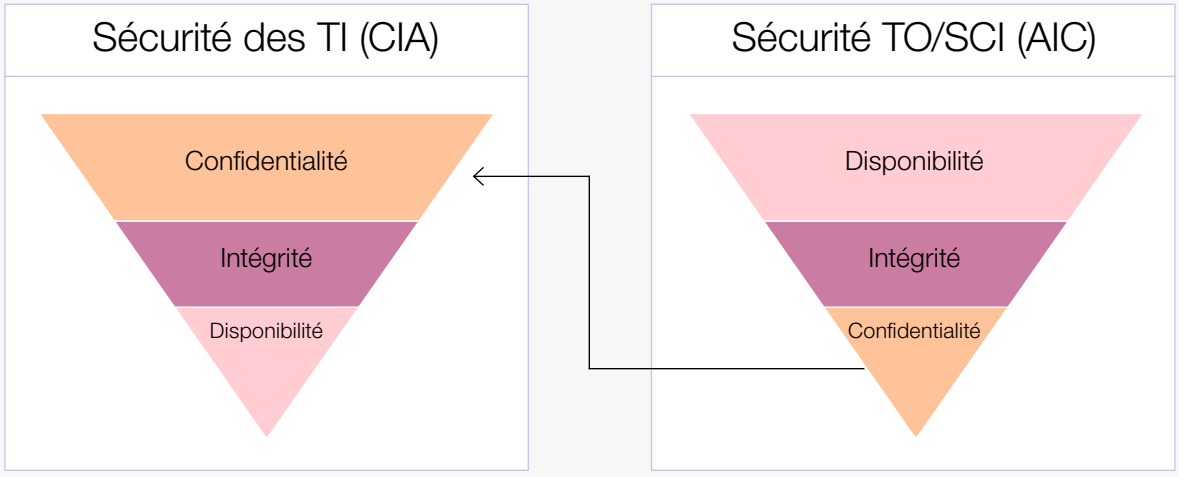


Figure 8 – Les priorités en matière de sécurité des TI sont inversées dans un environnement de TO.

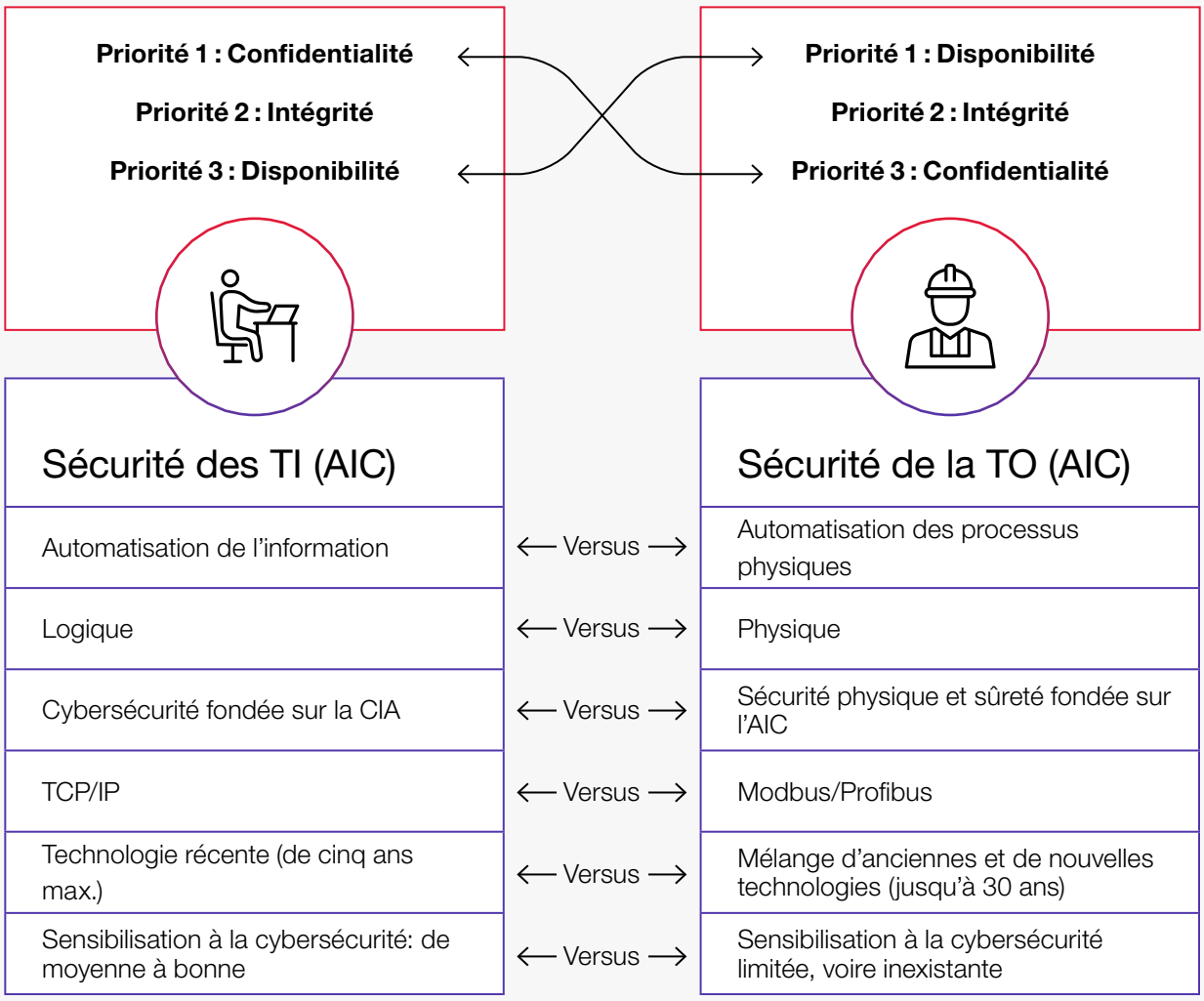


Figure 9 – Principales différences entre les environnements TI et TO

- **Déterminer qui est responsable de la sécurité** – Dans la plupart des organisations, la cybersécurité relève du chef de la sécurité informatique. Toutefois, la portée de sa responsabilité s'arrête souvent là où commence la production physique, c'est-à-dire des TI de l'entreprise jusqu'aux pare-feu qui protègent la TO. Toutefois, au sein de l'environnement de la TO, la sécurité physique relève du responsable de la sécurité et de la santé ou du directeur d'usine. Elle n'englobe souvent pas les aspects logiques ou de cybersécurité, ce qui laisse l'automatisation des processus physiques dépourvue de protection contre les cybermenaces. Pour contribuer à améliorer la gouvernance, nous recommandons de nommer un chef de la sécurité opérationnelle, qui sera responsable de la TO par intérim jusqu'à ce que cette responsabilité puisse être prise en charge soit par le chef de la sécurité informatique (de préférence), soit par le directeur de l'usine ou de la sécurité.

- **Sensibiliser les employés à la cybersécurité** – Tout employé autorisé à accéder (à distance) aux données de la TO et des TI ou à utiliser des appareils sur place doit recevoir une formation en sécurité adéquate afin de minimiser le risque d'atteintes internes. Sans une telle formation, les employés peuvent ne pas pleinement comprendre les conséquences de l'utilisation, par exemple, d'un périphérique de stockage USB, de l'ajout d'une nouvelle imprimante à connexion Wi-Fi ou de la création d'une liaison entre deux systèmes pour obtenir un certain type de données vraisemblablement non essentiel aux fins de production de rapport. La sécurité de la TO doit être intégrée dans les programmes existants afin de les protéger d'une brèche qui pourrait avoir une incidence sur la sécurité. Par exemple, un dispositif USB porté par un employé pourrait être utilisé pour s'introduire dans l'usine ou déstabiliser les installations en instaurant un logiciel malveillant.

  Par ailleurs, il est très important d'accroître la sensibilisation de la haute direction et des employés aux menaces qui pèsent sur la sécurité de la TO ainsi qu'aux risques d'établir des connexions non sécurisées entre la TO et le réseau de l'entreprise. Bien qu'il puisse être difficile pour les cadres et les employés de garder la sécurité en tête de leurs préoccupations, les hauts dirigeants des fonctions TI peuvent jouer un rôle clé dans cette sensibilisation grâce au partage d'information et aux programmes de formation continue offerts à tous les niveaux de l'organisation.

  Il faut également garder à l'esprit que la formation est essentielle, mais qu'elle sera efficace seulement si elle est adaptée au niveau de connaissances de base de l'apprenant et aux installations disponibles. Un programme unique pour tous ne fonctionnera pas. Par exemple, les employés qui jouent un rôle dans la sécurité de la TO au quotidien recevront la formation « Global Industrial Cyber Security Professional » (GICSP), tandis qu'une formation « SANS » standard sur la sécurité des SCI est plus adaptée aux cadres supérieurs. Pour les travailleurs d'usine, des formations vidéo élaborées dans leur propre environnement de travail rendront l'information plus pertinente à leurs yeux.

- **Stimuler une culture de la vigilance** – Personne n'est mieux placé pour déstabiliser une usine qu'un individu qui y travaille. En fait, la plupart des brèches de sécurité sont d'origine interne. Les travailleurs sur site sont le facteur le plus important à prendre en considération lors du renforcement des mesures de sécurité. Le contrôle de tous les employés et sous-traitants ainsi que du personnel externe et le contrôle constant de leurs droits d'accès aux renseignements confidentiels et aux systèmes peuvent contribuer à combler toute lacune en matière de sécurité. Les invités doivent également être surveillés de près. Des protocoles stricts de gestion des identités et des droits d'accès doivent être mis en place pour s'assurer que les employés ne puissent accéder qu'aux renseignements et aux installations nécessaires à l'exercice de leurs fonctions. Les organisations doivent cultiver et encourager une culture de sécurité. Par exemple, si un employé est surpris en train d'utiliser un système de contrôle auquel il n'aurait normalement pas accès, il y aurait lieu de mettre en doute ses motivations.

2

Modèle de référence et politique de sécurité – Les politiques de sécurité des TI ne peuvent pas être appliquées de façon arbitraire dans les environnements de TO. Au sein de la TO, il existe différentes exigences de sécurité pour les actifs de réseau et le personnel des usines qui nécessitent des politiques de sécurité spécifiques à la TO, comme celles liées à la gestion des accès, à la sécurité physique et environnementale, aux renforcements et aux correctifs, aux sauvegardes. Par exemple, dans la plupart des cas, les procédures liées aux correctifs dans un environnement de TO divergent fortement des pratiques afférentes dans les fonctions de TI. La disponibilité dans les environnements de TO étant une priorité absolue, il est possible d'effectuer des correctifs minimes et une réinitialisation très limitée des actifs, et ce, uniquement à des intervalles de temps prédéfinis.

Les fabricants qui possèdent plusieurs usines se heurtent souvent à des obstacles pour mettre en oeuvre de telles politiques au sein de leurs différentes installations. Les différences de processus de production, d'infrastructure de réseau, de fournisseurs et de solutions locales font en sorte que des usines qui semblent se ressembler diffèrent grandement. L'élaboration d'un modèle de référence qui décrit l'environnement de la TO souhaité, notamment les solutions de sécurité que chaque usine peut adopter, conduira en fin de compte à des marchés sectoriels sans ambiguïté.

3

Segmentation et renforcement – Pour assurer la sécurité, les fabricants doivent veiller à ce qu'il y ait une segmentation et une séparation suffisantes entre les actifs et les utilisateurs non autorisés, conformément aux normes du secteur ou au modèle de Purdue (figure 10). Il est important de regrouper les actifs qui comportent un ensemble commun d'exigences de sécurité, à la fois physiques et logiques. Il est tout aussi important de contrôler la communication et les interconnexions entre ces zones, en se servant de conduits qui déterminent le flux d'information autorisé entre les zones.

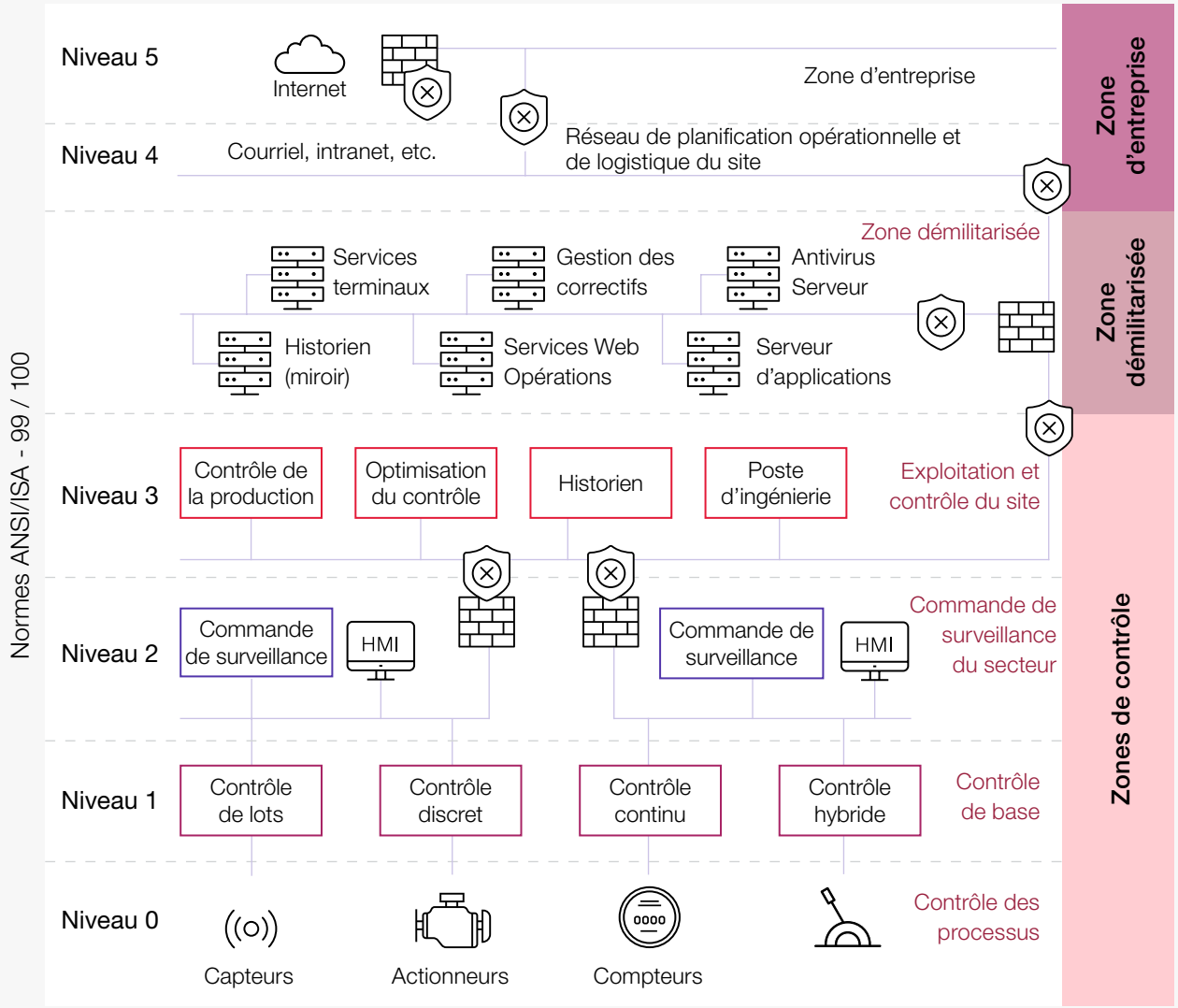


Figure 10 – Utilisation de zones pour regrouper les réseaux d'entreprises et de SCI

On peut définir les zones en termes de « **zones d'entreprise** » et de « zones de contrôle ». Dans la zone d'entreprise, on peut faire une distinction entre l'Internet qui relie les fabricants au monde extérieur et l'intranet de l'entreprise. La création d'une zone démilitarisée protège la zone de contrôle de l'interaction, de l'exploitation et de l'accès des utilisateurs dans la **zone d'entreprise**. Dans les zones de contrôle, une distinction doit être faite entre les éléments suivants.

- Les **zones de contrôle des opérations**, qui comprennent des systèmes d'exécution de la fabrication (MES), des historiens et des postes d'ingénierie.
- Les **zones de commande de surveillance**, qui renferment des interfaces homme- machine et des systèmes d'acquisition et de contrôle de données (SCADA) utilisés par les opérateurs pour interagir avec les équipements terminaux à distance, les appareils électroniques intelligents ainsi que les contrôleurs programmables.
- Les **zones de contrôle de base**, qui englobent des dispositifs de commande tels que des contrôleurs programmables permettant d'ouvrir des vannes, de déplacer des actionneurs ou de démarrer des moteurs.
- Les **zones de sécurité**, qui contiennent des systèmes de sécurité actifs destinés à détecter un état de fonctionnement potentiellement dangereux et à le remettre en état sûr.
- Les **zones de contrôle des processus**, qui englobent des capteurs, des actionneurs et des contrôleurs visant à gérer les processus physiques et chimiques de fabrication.

Il est conseillé de créer un réseau sans fil sécurisé distinct pour les appareils qui mettent à profit l'Internet des objets et qui ont été installés dans l'environnement de production. Il est également recommandé de maintenir les appareils personnels de même type, tels que les téléphones mobiles et les autres technologies portables, hors du lieu de travail ou du moins de les restreindre à un réseau pour les invités. Chacune de ces zones devrait comporter ses propres exigences de sécurité ainsi que des conduits bien définis.

4

Gestion des identités et des accès – doivent gérer tout flux d'information, qu'il soit automatisé ou manuel. Par exemple, lorsqu'une maintenance est en cours, il doit y avoir un délai convenu pour accéder aux systèmes TO et les connexions correspondantes doivent être automatiquement interrompues au moment convenu. Ce fonctionnement permet d'éviter qu'un agent de maintenance favorise l'accès à des données confidentielles en omettant de réinitialiser un système correctement.

5

Surveillance et maintenance – Le résultat des recommandations précédentes sur l'élimination des risques doit être suivi par un plan de surveillance, ce qui apportera des renseignements essentiels sur l'entretien adéquat de l'environnement de la TO.

Conseils pour renforcer vos systèmes et vos terminaux

Les fabricants ne doivent déployer que des appareils, des systèmes et des applications sécurisés et renforcés. Ils doivent d'abord faire appel à fabricants d'appareils et des développeurs de logiciels qui peuvent démontrer avoir mis en oeuvre des pratiques de codage sûres tout au long des cycles de vie de développement de composants matériels et logiciels. Règle générale, les professionnels en TI surveillent l'accès aux terminaux informatiques (ordinateurs de bureau, ordinateurs portables, appareils mobiles, serveurs de bases de données, d'applications et de sites Web basés sur le protocole Internet) et leur sécurité. Ils peuvent facilement mettre ces appareils à jour de façon automatique lorsqu'ils sont connectés à Internet et à l'intranet. En revanche, les professionnels en TO se préoccupent généralement moins de l'accès aux terminaux de TO et de leur sécurité. La plupart des gens croient que ces systèmes sont moins vulnérables puisqu'ils ne sont pas connectés à l'Internet et au réseau d'entreprise, et qu'ils disposent d'environnements, de protocoles, de canaux de communication spécialisés et de matériel exclusif. Les terminaux de TO qui sont délibérément isolés de l'Internet et de l'intranet ne sont pas non plus mis à jour automatiquement.

Compte tenu de la nécessité de renforcer à la fois les systèmes et les terminaux, il est essentiel de protéger les systèmes de contrôle industriel au niveau des serveurs, des applications, des systèmes d'exploitation, des utilisateurs ainsi qu'au niveau physique. Voici une liste non exhaustive des mesures que l'on peut prendre pour renforcer les systèmes.

- Installer des pare-feu
- Mettre à jour les correctifs de sécurité et les réparations immédiates
- Fermer les ports qui sont inutiles au fonctionnement du système
- Installer des systèmes de détection des intrusions pour déceler les logiciels espions et malveillants
- Supprimer les programmes et les comptes d'utilisateur inutiles
- Utiliser une protection par cryptage si possible
- Tirer parti de la gestion des accès et des identités (physiques et numériques)

Partie 3: surveillance

Surveiller étroitement l'environnement industriel, les actifs et les connexions

Établissez une surveillance continue – Pour demeurer alerte face aux menaces éventuelles, il faut surveiller en permanence les systèmes, les réseaux, les appareils, le personnel et l'environnement. Les systèmes de TO et de TI doivent être surveillés en s'appuyant sur des paramètres qui représentent un fonctionnement normal du réseau. Si ces paramètres sont dépassés un tant soit peu, les systèmes doivent être examinés. Les solutions de surveillance de la TO décèlent les anomalies qui dérogent aux règles de fonctionnement habituel et émettent une alerte pour que des mesures soient prises. Si, par exemple, un terminal à distance se met soudainement à communiquer avec un appareil d'un autre poste, ou si la quantité de données générées par un appareil électronique atteint soudainement un pic, il y aurait lieu de se demander si cette situation s'est produite parce que quelqu'un a piraté le système ou s'il y a une faille dans l'environnement de la TO. Voici quelques façons d'établir une surveillance continue.

A. Utiliser les systèmes SIEM de gestion de l'information et des événements liés à la sécurité pour surveiller à la fois le réseau d'entreprise et les réseaux de commande (y compris les réseaux sans fil). Ces systèmes proposent:
   - la détection des menaces et la réponse aux incidents de sécurité grâce à la saisie en temps réel de ces incidents et l'analyse de leur historique;
   - la production de rapports sur la conformité;
   - des enquêtes sur les incidents grâce à l'analyse des données historiques.

B. Tirer parti d'un centre de gestion de la sécurité dédié en vue d'avoir accès aux services précédemment mentionnés à un prix raisonnable ainsi qu'à des niveaux avancés de protection sur une plateforme évolutive. Cette approche permet de s'adapter rapidement aux exigences liées au contexte commercial et aux risques, en plus d'atteindre et de maintenir la conformité.

C. Utiliser des plateformes de surveillance de la sécurité TO pour effectuer un suivi et une détection en continu dans l'ensemble de la zone de vulnérabilités aux attaques.

D. Se servir de l'intelligence artificielle pour détecter les menaces à la sécurité et aux activités.

Créez de la redondance – Les entreprises manufacturières doivent relever des défis uniques en matière de sécurité. Contrairement à un environnent de TI, il n'est tout simplement pas possible d'arrêter des systèmes de TO aux fins de maintenance, de mises à jour de logiciels ou de correctifs. Le flux de production ne peut être interrompu, il est donc nécessaire de trouver une solution qui neutralise la menace et la tienne à l'écart jusqu'à ce que des mesures plus étendues puissent être prises. On peut y arriver en concevant des systèmes tout en gardant à l'esprit la redondance : chaque composant essentiel possède une contrepartie redondante qui peut être mise hors ligne aux fins de mises à jour, sans incidence sur le processus de production. Un autre moyen consiste à passer d'un réseau redondant à un autre pour maintenir la production pendant que les appareils reçoivent les correctifs, puis à changer de réseau à nouveau par la suite.

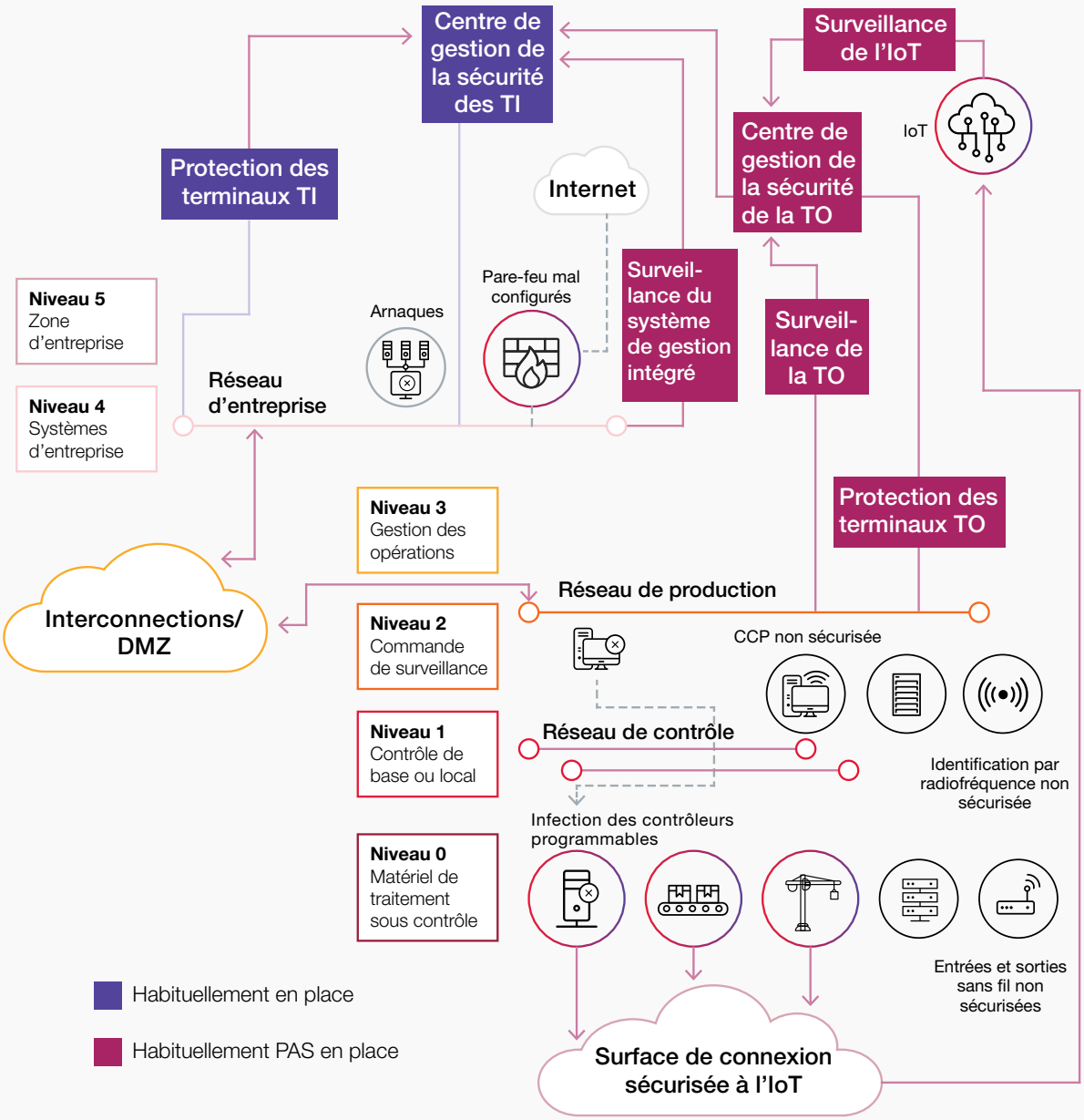
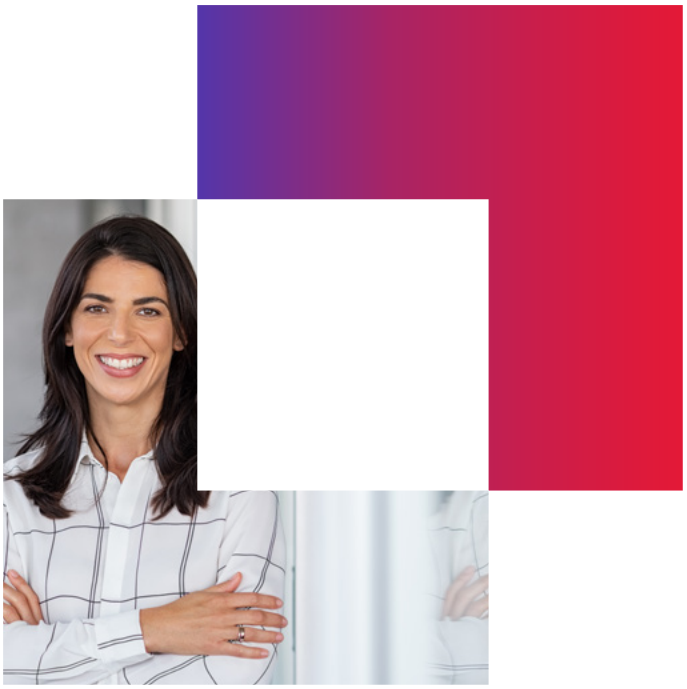


Figure 11– Un centre de gestion de la sécurité intégré. Les mesures de sécurité désignées en rouge ne sont souvent pas en place pour les fabricants.

Soyez résilient – Dans un environnement risqué en constante mutation, il arrive que des incidents se produisent. Ce qui importe, c'est que chaque système bénéficie d'un processus de récupération adéquat qui tient compte de la criticité du système, du temps de récupération maximum acceptable et de la méthode de récupération. Pour arriver à cet objectif, il faut se poser des questions importantes. En voici quelques-unes.

- Procédons-nous régulièrement à des sauvegardes de nos systèmes et de nos données?
- Avons-nous un plan de reprise après sinistre?
- Combien de temps faudra-t-il pour se remettre d'un incident?
- En combien de temps pouvons-nous corriger les dégâts causés par un incident?



Conclusion

Demeurer vigilant et résilient

Par le passé, les fabricants considéraient la cybersécurité comme un processus distinct. Aujourd'hui, nous observons que les entreprises la considèrent de plus en plus comme une activité intégrée. En effet, elles mettent en œuvre davantage de stratégies de transformation numérique, notamment en adoptant l'industrie 4.0. À l'heure actuelle, seule une approche globale qui tient compte des personnes, des processus, des technologies et de la gouvernance peut offrir la meilleure défense contre la rapidité et la panoplie croissantes des cybermenaces. Pour se protéger efficacement de la cybercriminalité, les fabricants doivent demeurer vigilants et faire preuve de résilience. L'évaluation, la sécurisation et la surveillance régulières des systèmes de TO sont essentielles à une protection adéquate contre les risques actuels et à venir.

Les solutions de CGI

Depuis des années, CGI est un conseiller de confiance auprès de dirigeants mondiaux, notamment des fabricants des industries automobile, minière et métallurgique, chimique, aérospatiale ainsi que de la haute technologie. Nos solutions et services complets et intégrés de cybersécurité des TI et de la TO protègent l'organisation numérique et sécurisent le continuum numérique dans l'ensemble de la chaîne de valeur. Au cours des 15 dernières années, CGI a développé et fourni des solutions spécifiques à la TO pour aider les dirigeants d'entreprises manufacturières et les directeurs d'usine à relever les défis liés à la protection du processus de production et des travailleurs contre les cybermenaces.

Dans la présente étude technique, nous avons présenté notre méthodologie visant à évaluer et à sécuriser l'environnement de la technologie opérationnelle, ainsi que nos meilleures pratiques et notre expérience dans ce domaine. Nous vous invitons à communiquer avec nous si vous souhaitez :

- mener une évaluation complète visant à déterminer ainsi qu'à qualifier l'état actuel de l'environnement opérationnel et de l'organisation, ainsi qu'effectuer un exercice d'évaluation et de priorisation des risques;
- valider et améliorer votre stratégie de cybersécurité en matière de technologie opérationnelle en fonction des normes de l'industrie et des meilleures pratiques de CGI;
- améliorer et gérer vos services de sécurité, surveiller vos réseaux et vos actifs, ainsi que détecter et éliminer les cybermenaces par l'entremise de centres spécialisés de gestion de la sécurité TO.

La cybersécurité est centrale à notre approche

Depuis plus de 40 ans, CGI crée des systèmes opérationnels essentiels dans des environnements complexes du monde entier, notamment dans les secteurs de la défense et du renseignement. Nous avons considérablement investi dans le développement de nos compétences en collaborant étroitement avec des associations internationales de sécurité et des organismes de normalisation. Bien que les cybermenaces soient mondiales, nous savons que les exigences varient selon la région et que les défis sont uniques à chaque organisation. À l'aide de nos experts, nos connaissances techniques et commerciales approfondies, nos centres de gestion de la sécurité, nos meilleures pratiques et nos cadres de gestion, nous veillons à ce que la sécurité soit intégrée, et non ajoutée. Les entreprises font donc appel à CGI tout particulièrement pour définir leurs risques de sécurité, produire des résultats sécurisés et continuer à exercer leurs activités en toute confiance.

Mots-clés et définitions

Intelligence artificielle	**IA**	Un domaine de l'informatique qui vise à créer des machines intelligentes.
Restriction de la zone d'attaque		La zone d'attaque est la somme des vulnérabilités des appareils et des logiciels connectés qui sont accessibles aux utilisateurs non authentifiés. Il est possible de restreindre cette zone en fermant les ports inutiles et en minimisant le nombre de ressources accessibles aux utilisateurs non fiables et par Internet.
Zone démilitarisée		Réseau ou chemin sécurisé entre le réseau interne d'une organisation et le réseau externe. On met en œuvre une zone démilitarisée principalement pour protéger un réseau interne de l'interaction avec des réseaux externes ainsi que pour prévenir l'intrusion de ceux-ci et l'exploitation qui en découlerait.
Système à commande répartie		Système de contrôle informatisé pour les processus ou les installations qui comporte généralement un grand nombre de boucles de régulation et dans lequel des contrôleurs autonomes sont répartis, avec une commande de surveillance par l'opérateur central.
Terminal		Typiquement, les terminaux TI sont les ordinateurs de bureau ou portables, les appareils portables comme les tablettes et les téléphones intelligents ainsi que les serveurs de bases de données, d'applications et de sites Web qui sont connectés à Internet et à l'intranet. Les terminaux TO sont habituellement les serveurs d'application, les serveurs de base de données, les systèmes de fabrication, les interfaces homme-machine, les postes de travail et les systèmes de contrôle.
Système de gestion intégré	**ERP**	Processus par lequel une entreprise gère et intègre des processus d'affaires. Un système de gestion de l'information intégré incorpore des domaines tels que la planification, les achats, les stocks, les ventes, le marketing, les finances et la gestion des ressources humaines.
Renforcement		Pratique qui consiste à rendre un système plus sécurisé. Il s'agit notamment de la suppression ou la désactivation des protocoles et services inutilisés, de la modification des valeurs par défaut, de la mise à jour des systèmes, de l'activation des pare-feu ainsi que de l'utilisation de logiciels antivirus.
Interfaces homme-machine		Application logicielle qui présente de l'information sur l'état d'un processus à un exploitant, qui l'utilisera pour établir ses instructions de contrôle. En général, l'information s'affiche sous forme graphique. Une interface homme-machine fait souvent partie d'un système de télésurveillance et d'acquisition de données (SCADA).
Gestion des identités et des droits d'accès	**IAM**	Discipline de sécurité, cadre de politiques et technologies qui permettent à des personnes autorisées d'accéder aux ressources qui leur sont destinées au bon moment et pour les bonnes raisons. Au sein d'une entreprise, cette approche vise à s'assurer que seules les personnes concernées aient accès aux ressources TI.
Système de contrôle industriel	**SCI**	Terme général qui englobe plusieurs types de systèmes de contrôle et instruments utilisés dans le contrôle des processus industriels (niveaux 1, 2 et 3 du modèle Purdue).
Industry 4.0	**I4.0**	La quatrième révolution industrielle.
Information Technology	**TI**	Se dit de l'utilisation d'ordinateurs au sein d'une entreprise (niveaux 4 et 5 du modèle de Purdue).

Appareil électronique intelligent		Contrôleur à microprocesseur de l'appareillage du réseau électrique, notamment les disjoncteurs, les transformateurs et les batteries de condensateurs.
Internet des objets	**IoT**	Se dit des dispositifs (capteurs, appareils et machines) qui fonctionnent ensemble grâce à la connectivité de l'Internet des objets (IoT) dans le but d'améliorer les processus industriels et de fabrication.
Protocol Internet	**IP**	Protocole de communication qui définit les formats de messages numériques et les règles d'échange de messages entre des ordinateurs sur un réseau, grâce à la suite de protocoles Internet.
Système de détection des intrusions		Type de logiciel de sécurité conçu pour alerter automatiquement les administrateurs lorsque quelqu'un ou quelque chose tente de compromettre le système d'information. Un tel logiciel surveille l'activité du système en examinant les vulnérabilités de ce dernier et l'intégrité des fichiers, et en effectuant une analyse des modèles fondés sur des attaques précédentes.
Système d'exécution de la fabrication	**MES**	Système d'information qui relie, surveille et contrôle en temps réel les processus de fabrication et les flux de données dans une usine. L'objectif principal d'un système MES est d'assurer l'exécution efficace des activités de fabrication et d'améliorer le rendement de la production.
Technologie opérationnelle	**TO**	Se dit de l'utilisation d'ordinateurs dans la production (niveaux 1, 2 et 3 du modèle de Purdue). L'acronyme « TO » a été adopté pour distinguer l'environnement de travail de TI de l'environnement de production des systèmes de contrôle industriel.
Contrôleur programmable		Ordinateur renforcé que l'on utilise pour automatiser un processus précis, une fonctionnalité d'appareil ou une chaîne de production. Il est spécialement conçu pour résister à des environnements hostiles ainsi qu'à la chaleur, au froid, à la poussière et à l'humidité.
Modèle de Purdue		Architecture de référence pour les systèmes de contrôle industriel.
Terminal à distance		Dispositif électronique commandé par microprocesseur qui surveille les paramètres sur place et transmet les données aux systèmes à commande répartie ainsi qu'aux systèmes d'acquisition et de contrôle de données (SCADA).
Gestion de l'information et des événements liés à la sécurité	**SIEM**	Approche qui regroupe les fonctions de gestion de l'information et des événements liés à la sécurité en un seul système de gestion de la sécurité. Les systèmes SIEM sont utilisés aux fins de collecte et d'analyse centralisées de données provenant de divers systèmes et dispositifs sur un réseau donné. Ils servent également à déterminer les écarts par rapport à la norme, détecter les menaces et prendre les mesures qui s'imposent, comme la vérification, l'endiguement, l'atténuation ou la réparation.
Centre de gestion de la sécurité		Établissement centralisé où une équipe de sécurité de l'information travaille précisément à prévenir, détecter et évaluer les menaces et incidents de cybersécurité ainsi qu'à y répondre, en plus de respecter et évaluer la conformité réglementaire.
Système d'acquisition et de contrôle de données		Système de contrôle industriel qui fait partie intégrante de nombreux secteurs, comme le secteur manufacturier, le secteur de l'énergie, le secteur de l'eau et le secteur de la production et la distribution d'électricité.

À propos de CGI

Allier savoir et faire

Fondée en 1976, CGI est l'une des plus importantes entreprises de services-conseils en TI et en management au monde.

Nous sommes guidés par les faits et axés sur les résultats afin d'accélérer le rendement de vos investissements. À partir de centaines de sites à l'échelle mondiale, nous offrons des services-conseils complets, adaptables et durables en TI et en management. Ces services s'appuient sur des analyses mondiales et sont mis en œuvre à l'échelle locale.

cgi.com/manufacturing