Cas pratique

La cybersécurité des systèmes industriels

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

Table des matières

INTRODUCTION

Ce cas pratique complète le document intitulé *Maîtriser la SSI pour les systèmes industriels*[1].

Son objectif est de présenter des situations qui représentent un risque pour les entreprises et de transmettre les recommandations adéquates afin d'accompagner les entreprises dans la sécurisation de leurs systèmes industriels.

De nombreuses bonnes pratiques décrites ici sont similaires à celles de l'informatique de gestion[2], mais leur mise en œuvre est à adapter aux contraintes du domaine industriel.

Les exemples et situations concrètes présentés dans l'étude suivante illustrent l'application de la démarche de déploiement de la SSI dans le contexte industriel. La démarche proposée ainsi que les recommandations peuvent s'appliquer quel que soit le contexte industriel mais doivent toujours être adaptées aux enjeux et aux risques identifiés.

L'étude porte sur un site industriel existant depuis plusieurs dizaines d'années, disposant d'installations hétérogènes, dont certaines sont en phase d'obsolescence. Les installations sont pilotées par des automates industriels (API /PLC) et supervisées par un ensemble de SCADA regroupé dans un centre d'exploitation. Certaines de ces installations, comme les lignes de production de l'atelier d'assemblage, disposent de contraintes « temps réel » et d'autres, comme une unité de distribution de matières dangereuses, de contraintes de sûreté de fonctionnement et de disponibilité.

Le site détient une unité de stockage située géographiquement à quelques centaines de mètres en dehors de l'enceinte du site principal. Cette unité est placée en amont de l'unité de distribution de matière dangereuse.

Les sigles et acronymes utilisés dans le document sont repris en annexe A.

1 http://www.ssi.gouv.fr/systemesindustriels

2 Informatique de gestion : systèmes d'information destinés aux services et applications de bureautique, de gestion des ressources humaines, de relations clients ou encore de gestion intégrée.

1 - LE CONTEXTE

La direction du site demande l'évolution du système de SCADA, afin que celui-ci puisse communiquer avec le système d'information de gestion dans le but d'améliorer les coûts et délais de production. Les informations collectées au niveau du SCADA devront être accessibles à l'ensemble des responsables du site depuis leurs postes bureautique, mais également à ceux des autres sites de l'entreprise. Enfin, en vue d'optimiser les coûts de fonctionnement, il est demandé d'étudier les solutions de télémaintenance.

La compagnie dispose d'un service informatique (IT) responsable de l'infrastructure informatique de gestion (des systèmes bureautiques, des interconnexions entre sites, de la messagerie et des accès Internet).

Depuis plusieurs années, et à la demande de la direction de la compagnie, ce service a déployé une politique de sécurité des systèmes d'information (PSSI).

Suite à des incidents récents, la direction demande que cette PSSI soit étendue aux installations industrielles, dont certaines sont sous la responsabilité du directeur technique, d'autres sous la responsabilité du directeur de production, et certaines directement sous la responsabilité du directeur du site.

En effet, quelques mois auparavant, la propagation d'un virus introduit par une clé USB sur un poste SCADA avait généré un trafic réseau important et provoqué des dysfonctionnements sur les systèmes industriels.

Par ailleurs, une entreprise de conseil qui réalisait un test d'intrusion interne avait trouvé deux moyens de s'introduire sur le réseau bureautique. Le premier en injectant des commandes SQL vers le moteur de bases de données du site Web Extranet et le deuxième en envoyant des fichiers PDF piégés à quelques utilisateurs. Quelques postes, ne bénéficiant pas des correctifs de sécurité du lecteur PDF, ont été compromis. Les auditeurs ont essayé d'élargir la compromission et d'identifier les équipements vulnérables sur le réseau bureautique en exécutant une découverte réseau et des scans de vulnérabilités. Ils ont rapidement mis en évidence la vulnérabilité d'un ensemble d'équipements, basés sur des systèmes anciens, non mis à jour, et la présence de nombreuses interfaces d'administration non protégées par une authentification. Lors de ces tests un automate s'est arrêté ce qui a provoqué l'arrêt d'une chaîne de production pendant une demi-heure. Les équipements identifiés comme vulnérables étaient en réalité des machines SCADA. L'arrêt de l'automate était une conséquence du scan réalisé. Les réseaux bureautiques et industriels étaient connectés suite à une mauvaise configuration, ce qu'ignoraient les différents responsables du site.

Cette mésaventure prouve la nécessité de mieux protéger les systèmes industriels. Elle montre aussi que les attaques externes ne sont pas les seules menaces.

Un coordinateur, récemment embauché, disposant d'une expérience dans le domaine informatique et ayant une culture industrielle, est nommé pour piloter ce projet. Cette fonction recquière de la pédagogie et de la diplomatie. Le coordinateur rapportera directement à la direction du site.

Il découvre les installations et les contraintes métier associées. Il se demande comment étendre la PSSI, qu'il connait encore peu, à des installations industrielles dont les caractéristiques semblent particulières, tout en respectant les contraintes et les habitudes de chacun. Il se rend compte des différences de culture et d'approche existant entre les domaines informatiques, de

production et de sûreté de fonctionnement. Pourtant l'objectif final est pour tous de fournir les produits et services aux clients dans les délais prévus et au moindre coût.

2 - LA DÉMARCHE CHOISIE

La première étape consiste à comprendre les besoins métier, inventorier les équipements et les services. L'objectif est de constituer une cartographie physique et logique des installations et des flux d'informations entre les différents éléments, puis d'établir les niveaux de criticité de chacun.

Ce travail conséquent sera réalisé avec les différents responsables d'installations. Certains disposent déjà d'éléments, par exemple dans les analyses de sûreté de fonctionnement (AMDEC).

Cette cartographie permettra lors de la seconde étape d'établir une évaluation des besoins de sécurité et de réaliser une première analyse des vulnérabilités de l'existant.

Dans un troisième temps, l'analyse des nouveaux besoins permettra d'identifier les mesures de sécurité nécessaires (éléments techniques ou organisationnels) à déployer pour réduire les écarts avec l'existant ainsi que les impacts potentiels sur les installations.

Ces trois étapes sont formalisées dans un plan d'amélioration de la sécurité que le coordinateur proposera à la direction.

Il a conscience de l'ampleur du travail, mais aussi du poids de ses actions sur le travail quotidien de ses collègues : « Encore de nouvelles règles à suivre, il y en a déjà beaucoup, cela va encore nous compliquer le travail. »

Il décide de commencer par communiquer sur son projet, d'en expliquer simplement le but et la façon doit il souhaite procéder. Il organise une présentation aux principaux responsables et les informe de son intention de réaliser une visite des installations, pour qu'ils relaient l'information auprès de leurs équipes. De cette façon il pourra établir le contact avec le personnel et faire passer directement les messages sur l'intérêt de la SSI dans leur travail quotidien. Le rôle pédagogique dans sa démarche est fondamental. Son public étant très préoccupé par la disponibilité et la sûreté, il insiste sur le fait que la sécurité des systèmes d'information ne va pas à l'encontre de la disponibilité, mais au contraire contribue à la renforcer.

3 - LES CONSTATS (LA VISITE)

Le coordinateur accompagné par les divers responsables d'atelier, commence la visite du site par le centre d'exploitation où se trouve l'ensemble des postes SCADA et les opérateurs en poste 24/7.

3.1 - Le centre d'exploitation

Passant devant des baies de brassage réseau du centre d'exploitation, il constate que les baies de brassage pour les SCADA sont bien identifiées et séparées des baies de brassage de l'IT situées à côté.

Pourtant, il remarque un cordon réseau partant des baies SCADA et allant vers les baies IT.

Il demande des éclaircissements au responsable du centre d'exploitation. Ce dernier semble gêné et explique que pour certaines opérations, il est utile d'avoir le SCADA sur un PC bureautique situé dans une autre pièce.

Le coordinateur fait remarquer qu'il y a déjà eu un incident suite à l'interconnexion des réseaux. Le responsable explique qu'il s'agit seulement d'une machine SCADA disposant de deux cartes réseaux (une connectée au réseau bureautique et l'autre connectée au réseau SCADA). Les réseaux ne sont pas interconnectés. Le coordinateur explique que si une personne ou un *rootkit* prend le contrôle de cette machine il prend le contrôle de tout le réseau SCADA. Les risques sont majeurs. Les conséquences seraient les mêmes lors de la propagation d'un virus.

Les éléments du système d'information des gestion disposent de mesures pour faire face aux menaces externes (antivirus, mises à jour régulières, authentification forte...) alors que ce n'est sans doute pas le cas de tous les équipements SCADA. Une machine, non sécurisée, avec deux interfaces réseau offre un chemin pour des attaques et facilite la propagation de virus.

Des solutions, reposant sur les technologies Web ou RDP par exemple, accompagnées de mécanismes de cloisonnement réseau, offrent un accès plus sécurisé au SCADA depuis des postes bureautiques (voir annexe B).

Il faut donc supprimer ce lien qui permet une compromission des installations depuis Internet, par rebond sur le réseau bureautique.

Le coordinateur remarque également une clé USB sur un poste. Visiblement quelqu'un l'a oubliée. Il demande pourquoi des clés USB sont utilisées dans le centre d'exploitation. **On lui répond que l'équipe a besoin d'extraire des données des SCADA pour ses rapports. L'examen de la clé révèle qu'elle contient des données personnelles mais surtout un virus !** Heureusement celui-ci est peu offensif, mais il faudra vérifier l'ensemble des machines et nettoyer celles qui sont infectées. Le chef du centre d'exploitation indique que les clés USB sont le seul moyen d'extraire des données des SCADA ou d'importer des mises à jour de fichiers de configuration par exemple.

Le coordinateur explique que sans interdire les clés USB il est possible de désactiver les fonctions de lancement automatique sur les médias amovibles, fonction utilisée par de nombreux virus (voir annexe B). Il est possible de configurer les politiques de restrictions logicielles pour n'autoriser qu'une liste de programmes (par exemple, ceux des SCADA et quelques utilitaires).

Il est également possible de déployer un sas sécurisé pour échanger les données et de désactiver les ports USB sur toutes les machines SCADA critiques. Des solutions existent !

Les clés USB sont un des principaux vecteurs de propagation de virus. Les incidents sont nombreux !

Le coordinateur demande comment le personnel interne et sous-traitant est sensibilisé aux enjeux de la SSI. Le responsable indique que théoriquement ils suivent une petite formation mais qu'elle est plutôt orientée sur la partie bureautique et qu'il faudrait la suivre régulièrement pour qu'elle soit efficace. Le coordinateur indique que les règles d'hygiène informatique pour l'informatique de gestion sont applicables au domaine industriel.

Les 10 règles de base de la SSI pour les systèmes industriels pourraient être affichées dans le centre d'exploitation et dans les unités de production. Des pictogrammes sur le principe de ceux utilisés en sûreté de fonctionnement pourraient également être utilisés pour signifier l'interdiction des clés USB sur les installations critiques, l'interdiction de connecter un PC portable sans autorisation ou encore la nécessité de signaler toute anomalie…

De nombreuses actions et réglages des installations sont possibles depuis le centre d'exploitation. Les applications SCADA sont nombreuses et hétérogènes. Le coordinateur demande ce qu'il se passerait si un opérateur exécutait une mauvaise commande ou se trompait dans la saisie d'une valeur de réglage (saisie de 10000 tour/min pour un moteur au lieu de 1000 par exemple).

Le responsable explique que des contrôles sont prévus dans la conception des installations pour limiter les risques d'erreur de la part des exploitants. Cela peut donc aussi freiner des attaquants déclare le coordinateur.

Les fenêtres de saisie sont bornées dans le SCADA : un utilisateur ne peut pas saisir une valeur en dehors des limites de fonctionnement des équipements. Ces bornes sont également intégrées dans les automates et sont figées. Il n'est pas possible de les modifier sans changer le code source du PLC.

Par ailleurs, pour éviter certaines mauvaises manipulations, l'application SCADA demande une confirmation avant d'envoyer la télécommande. Cela limite les risques d'erreur qui restent malgré tout toujours possibles. Il faut envoyer une demande de commande (bit à 0) puis lorsque l'automate l'a acceptée envoyer la commande (bit à 1). Le responsable explique que ce mécanisme a permis d'empêcher l'arrêt d'une installation lors d'une intervention récente. Un automaticien a rechargé dans l'automate des données qui avaient été sauvegardées. Dans cette sauvegarde les bits de commande d'arrêt de plusieurs installations étaient activés mais pas celui de la demande de commande. Les installations ne se sont pas arrêtées et une alarme de discordance est remontée au SCADA permettant ainsi de détecter le problème. Le coordinateur indique que cet exemple montre que parfois des mécanismes simples permettent

d'éviter des problèmes. Cette mesure serait inefficace contre un attaquant disposant d'une parfaite connaissance du système mais peut permettre de détecter de nombreuses autres attaques moins sophistiquées.

3.2 - L'atelier de production

Pendant sa visite, le coordinateur aperçoit un poste de travail situé dans un recoin de l'atelier de production. A coté de ce poste, un intérimaire du service de nettoyage est en train de passer un coup de chiffon. Il demande au responsable de l'atelier à quoi sert ce poste. Celui-ci lui répond qu'il s'agit d'un poste de SCADA « déporté » utilisé par les chefs d'équipe et les techniciens de maintenance.

En s'approchant, il constate que l'application SCADA est démarrée avec un login « Maintenance ». Le chef d'atelier explique qu'il y a eu une maintenance la veille sur une ligne de production qui s'est terminée tard et que le technicien a probablement oublié de se déconnecter.

Le coordinateur fait remarquer que, du coup, n'importe qui peut utiliser l'application comme l'intérimaire qui travaillait dans le secteur. Ne serait-il pas judicieux d'intégrer dans l'application un mécanisme de verrouillage automatique après un certain délai d'inactivité ?

Le responsable indique que cela n'aurait que peu d'effet car les logins sont génériques, attribués à une équipe et donc connus par de nombreuses personnes.

Le coordinateur explique qu'il serait tout de même judicieux de prévoir une déconnexion automatique de ce poste isolé et de limiter les fonctionnalités de télécommandes ou modification de paramètres pour ces logins génériques. Mais surtout il faut déplacer ce poste dans un endroit plus visible de l'atelier, dans des zones couvertes par le système de vidéo-protection par exemple.

D'autres pistes sont à étudier car tous les employés disposent d'un badge pour accéder physiquement aux locaux et certainement d'un compte informatique pour la bureautique. Ces systèmes pourraient être utilisés par l'application de SCADA à la place des logins génériques qui sont souvent une facilité historique.

Le responsable de l'atelier répond que ces pistes sont intéressantes et sont à appronfondir.

Le coordinateur rencontre un technicien qui utilise un écran tactile situé sur la toute nouvelle chaîne d'assemblage. Le technicien est ravi, car depuis cet écran tactile, il dispose des mêmes fonctionnalités que depuis les postes SCADA, tout en étant physiquement devant son installation.

Il peut l'utiliser pour modifier un ensemble de paramètres de procédés (process), visualiser des courbes, exécuter des commandes. Le technicien explique qu'il peut forcer certains modes de marche, inhiber des capteurs, forcer des valeurs, ce qu'il ne pouvait pas faire depuis le SCADA. Très intéressé et très curieux, le coordinateur demande comment cet écran tactile est connecté à l'installation.

Le technicien pense que l'écran tactile est connecté sur l'automate pilotant la chaîne de production. Il ouvre le compartiment courant faible de la chaîne et montre l'automate. Cet automate est connecté sur un commutateur Ethernet visiblement intégré dans un backbone

en fibre optique. Un deuxième câble de cuivre part du commutateur et arrive jusqu'à l'écran tactile. **Pour résumer, dans la configuration actuelle l'écran tactile et l'automate sont accessibles depuis le réseau bureautique !**

Cet écran tactile (OP) ressemble fortement à un PC, physiquement plus robuste, avec un système d'exploitation standard. Il présente certainement des vulnérabilités facilement exploitables dont il faudra tenir compte dans les mises à jour et les politiques d'accès. Il peut être utile de réaliser des tests d'intrusion depuis ce type d'équipement. L'OP dispose de ports USB : que se passe-t-il par exemple si l'on branche un clavier ? Est-ce que cela donne accès à des fonctions systèmes ou à la liste des programmes installés sur l'OP par exemple ?

Le coordinateur demande comment le centre d'exploitation est informé de l'utilisation de modes de marche particuliers. Le technicien répond qu'en général il appelle les opérateurs pour les informer car ces informations ne remontent pas au centre d'exploitation.

Le responsable de l'atelier explique que cette ligne d'assemblage récente est bien plus rapide que les anciennes. En revanche elle s'arrête plus souvent et nécessite des réglages plus précis et plus fréquents que les anciennes. C'est pourquoi, afin de ne pas polluer le centre d'exploitation, toutes les informations ne remontent pas sur le SCADA.

Le coordinateur explique qu'au contraire plus de traçabilité et de remonté d'information sur le SCADA pourrait aider à identifier les dysfonctionnements et à détecter des comportements anormaux. Les logiciels et systèmes actuels sont capables de gérer de grandes quantités de données. Les espaces de stockage ne sont plus une contrainte majeure.

Le coordinateur indique qu'il était surpris de voir dans le centre d'exploitation une application SCADA pour l'atelier A et B et une autre pour l'atelier C. Le responsable explique qu'il aimerait bien avoir une application unique pour les trois et surtout le même niveau de fonctionnalités. Cela faciliterait la corrélation des données de production. Mais les automates de l'atelier A et B dialoguent avec le SCADA via des protocoles spécifiques non supportés par les autres constructeurs et les nouveaux SCADA.

Pour le responsable de l'atelier, les SCADA utilisant des protocoles spécifiques ne sont pas vulnérables. Le coordinateur explique qu'en réalité les systèmes propriétaires ne sont pas à l'abri. Ils sont souvent développés à partir de composants standards et s'exécutent sur des systèmes d'exploitation également « standards » et non spécifiques aux systèmes industriels. Les mécanismes de sécurité sont souvent faibles. Une analyse ainsi qu'une étude d'une évolution de ce système avec l'équipementier est nécessaire.

3.3 - L'unité de stockage de matières dangereuses

Le coordinateur poursuit sa visite sur l'unité de stockage des matières dangereuses. Celle-ci est située à quelques centaines de mettre du bâtiment de production, en dehors de l'enceinte principale du site.

Il constate que les équipements de mesure de niveau des cuves (radar) de matière dangereuse sont disposés « en pleine nature », et sont facilement accessibles à des personnes étrangères à l'entreprise. Il fait remarquer au responsable de l'unité que ces niveaux pourraient être modifiés par des personnes malintentionnées et demande quels en seraient les impacts.

Le responsable lui répond que l'indisponibilité des niveaux peut perturber le fonctionnement des installations. L'automate peut fermer des vannes de distribution s'il détecte un niveau très bas sur un réservoir par exemple. Dans le passé un dysfonctionnement sur un capteur avait entraîné des comportements aléatoirement aberrants sans cause apparente. Le diagnostic est difficile car aucune information de cette unité ne remonte au centre d'exploitation. Depuis les capteurs ont été doublés pour plus de fiabilité.

Le coordinateur déclare qu'une protection physique des équipements éloignés et situés en extérieur semble nécessaire ainsi qu'un minimum de report d'information vers le centre d'exploitation.

Le responsable de l'unité indique qu'il existe un projet d'extension qui serait une opportunité d'améliorer la surveillance de l'installation. Ceci éviterait aux équipes d'exploitation un nombre important de rondes pour s'assurer qu'il n'y a pas d'anomalie sur l'installation.

Par ailleurs, le coordinateur identifie un modem relié à l'automate. L'intégrateur l'a installé pour intervenir à distance et ainsi réduire les coûts de maintenance et les délais d'intervention.

Après analyse, il s'avère que le mot de passe pour accéder au programme de l'automate est vide (ce qui est la valeur par défaut). Ni l'exploitant, ni l'intégrateur n'ont pensé à changer cette configuration. Le coordinateur indique qu'il est urgent de mettre en place une politique de mot de passe pour les automates ainsi que les autres équipements de terrain (capteurs et actionneurs par exemple).

Un attaquant scannant la plage téléphonique de l'entreprise pourrait alors identifier le modem, prendre le contrôle de l'automate, modifier le programme et provoquer des dysfonctionnements sur l'installation. **Par chance, le modem de l'automate dispose d'une fonction de rappel (callback)**[3]. Ainsi, un attaquant ne peut plus prendre la main sur l'automate, même s'il en connaissait le mot de passe.

Le responsable explique que l'intégrateur propose de connecter l'interface Web de gestion de l'automate à Internet (via un VPN par exemple), ce qui lui donnerait accès à des fonctions de diagnostic plus évoluées.

Le coordonnateur comprend le besoin et la demande. Néanmoins, il est primordial d'en évaluer les risques.

3 Callback : Son principe consiste à configurer un numéro de maintenance; lorsque le modem est appelé, il raccroche et appelle automatiquement le numéro défini.

L'utilisation des services Web sur un automate peut être des plus dangereux.

La couche Web est certainement un composant standard, non spécifique à l'automate pouvant présenter des vulnérabilités pour l'ensemble de l'automate (déni de service par exemple). Sur les systèmes de gestion les services Web font régulièrement l'objet de correctifs ce qui n'est certainement pas le cas sur les automates.

Ces fonctions, souvent optionnelles, doivent être désactivées sur les installations critiques !

3.4 - L'unité de distribution des matières dangereuses

Dans l'unité dédiée à la distribution de matières dangereuses le coordinateur aperçoit plusieurs postes de SCADA.

Ne ressemblant pas à ceux qu'il a vus jusqu'à maintenant. Le responsable de l'unité lui explique que dans cette unité **le SCADA est maintenu par la société qui l'a intégré**. Elle intervient à leur demande en cas de panne sur les postes et il lui est arrivé de les remplacer. Le coordinateur est surpris et demande pourquoi ce service n'est pas assuré par les équipes de l'IT. Étant sur le site ils pourraient agir plus vite et surtout fournir du matériel standard certainement moins coûteux.

Le responsable explique qu'historiquement les SCADA de cette unité n'étaient pas dans le périmètre de l'informatique de gestion. De plus **les besoins particuliers des applications (logiciels spécifiques, OS obsolètes...) n'étaient pas compatibles avec les standards IT**. Les PC, standard de l'informatique classique, ne supportent pas les environnements industriels et sont équipés de logiciels antivirus qui entrent en conflit avec les applications. De plus il est nécessaire d'avoir des droits administrateur pour utiliser ces applications.

Le coordinateur explique qu'il comprend cette problématique d'incompatibilité des applications avec les configurations « durcies » fournies par l'IT. Mais ces postes sont des vulnérabilités pouvant s'étendre à tous les SCADA. Les logiciels antivirus ne sont peut être pas supportés par ces anciennes applications, de même que les mises à jour des OS mais il existe certainement des contres mesures. Il faut étudier les solutions avec l'IT et l'intégrateur. A minima il est nécessaire de mettre en place des journaux d'événements, de surveiller ces machines et définir un mode de fonctionnement avec l'IT afin qu'ils apportent leur expertise sans interagir avec les métiers de l'entreprise.

Le coordinateur souhaite qu'on lui explique le processus de distribution de matières dangereuses et comment l'ensemble est piloté.

La distribution est entièrement automatique, en fonction des besoins sur les chaînes de production. L'installation demandant une forte disponibilité est pilotée par trois automates haute disponibilité.

Le coordinateur demande s'il existe un lien avec l'unité de stockage. Le responsable répond que la majorité des asservissements sont indépendants. Il existe tout de même un lien, puisque, en cas de fuite, l'installation de distribution se met à l'arrêt et envoie un ordre de stop à l'unité de stockage qui ferme des vannes de sécurité. Les informations de détection de fuite, Tout

Ou Rien (TOR), sont câblées directement sur les vannes. Dans la perspective d'une extension de l'unité de stockage, une connexion par bus ou WiFi est envisagée. Cela offrirait plus de souplesse pour exploiter les installations.

Les PLC communiquent avec le SCADA via un réseau Ethernet qui semble être le même que celui des autres automates du site.

Le coordinateur s'interroge sur la gestion de la maintenance de ces installations. Le responsable de l'unité lui répond que la maintenance est assurée par la société qui a mis en service l'installation, comme pour les SCADA. Les interventions de maintenance sont plutôt rares car le système est robuste et se limitent aux défaillances matérielles. Elles concernent parfois les coupleurs de communication Ethernet. Une fois rendus indisponibles, suite à une surcharge de trames par exemple, il faut redémarrer l'automate pour les réinitialiser. Le coordinateur demande si ces surcharges ont été identifiées. Le responsable répond que non car les intervenants n'ont pas nécessairement les compétences suffisantes en réseau pour établir un diagnostic.

Le coordinateur explique qu'il serait nécessaire de configurer des outils d'analyse et de monitoring sur le réseau. Ils peuvent être simples à déployer et totalement transparents pour les installations. Ils permettront de détecter des événements, d'empêcher des incidents ou simplement de fournir des éléments pour analyser des comportements qui ont aujourd'hui un impact sur le procédé (process).

Un canal de diagnostic complémentaire au SCADA est nécessaire pour détecter des incidents par exemple dans le cas où le SCADA serait compromis. La généralisation de l'utilisation des protocoles Syslog et SNMP (v3) dans les équipements industriels permet de créer ce deuxième canal pour détecter des défaillances « systèmes » sur les composants et les applications.

Le coordinateur demande comment se déroulent les interventions. Le responsable répond qu'en général, un technicien de la société se déplace, connecte sa console sur l'automate, ou sur le réseau, réalise un diagnostic et corrige le problème. Le coordinateur s'inquiète de savoir si cette connexion donne aussi accès aux autres automates du site et si les accès aux PLC sont protégés par des mots de passe par exemple. Le responsable ne sait pas, il faudra demander à l'intégrateur.

L'intégrateur indiquera qu'aucun mot de passe n'est configuré dans les automates. Cela simplifie les interventions. De plus, ces automates, comme le SCADA sont bien connectés sur le même réseau Ethernet que celui sur lequel sont connectés les autres automates du site.

Le coordinateur conclut que pour des interventions très ponctuelles et peu fréquentes des intervenants extérieurs se connectent sur le réseau SCADA avec leurs propres outils et disposent d'un accès à tous les automates du site puisqu'aucun mot de passe n'est configuré. Il s'agit d'une vulnérabilité majeure. Ces interventions doivent être encadrées par des procédures, les accès aux automates limités et protégés par des mots de passe et surtout les consoles de maintenance doivent être maitrisées et mises à disposition des intervenants en cas de nécessité.

L'accès physique aux automates, bus de terrain, SCADA et autres équipements doit être limité autant que possible.

4 - LE BILAN

4.1 - La première analyse

Une fois son tour des installations terminé, le coordinateur dresse rapidement et dans le désordre un premier bilan :

- les utilisateurs commes les responsables ont très bien collaborés. Néanmoins, le coordinateur a ressenti que sa présence pouvait parfois contrarier du fait de sa mise en exergue de vulnérabilités ;
- les systèmes sont hétérogènes et ne sont pas tous gérés de la même façon ;
- le niveau de maîtrise des installations est plutôt faible. Beaucoup d'éléments reposent uniquement sur les intégrateurs voire sur les personnes ayant participé à la mise en service initiale des installations il y a plusieurs dizaines d'années ;
- pour leurs besoins qui semblent légitimes, les utilisateurs emploient des moyens peu sécurisés qui créés des vulnérabilités ;
- les diverses personnes rencontrées sont volontaires, mais le *turnover* et les intérimaires sont nombreux ;
- il est assez facile pour n'importe qui de se connecter sur le SCADA (sessions ouvertes sur les postes avec des niveaux d'accès importants) ;
- les protections physiques sont incomplètes ;
- il n'existe pas de notion de cloisonnement. Tous les éléments semblent être sur le même réseau, quel que soit leur niveau de criticité et leurs fonctionnalités. L'arrêt de l'automate lors des tests d'intrusion confirme la nécessité de mettre en œuvre au plus vite une solution de filtrage entre les réseaux et de limiter les accès ;
- la création d'un processus de veille sur les vulnérabilités est indispensable (abonnement aux CERTs, suivi du site des constructeurs, contrat avec des sociétés spécialisées dans cette activité…
- il manque une procédure (à afficher dans le centre d'exploitation par exemple) concernant le traitement des incidents ainsi que la chaîne d'alerte à activer
- de même il semble intéressant d'afficher en évidence les 10 règles d' « hygiène informatique » d'utilisation des systèmes industriels (cf. annexe D) ;
- il est nécessaire de prévoir un cursus de sensibilisation spécifique aux systèmes industriels.

4.2 - Une réflexion globale

Globalement, le coordinateur a essayé de comprendre les problématiques des utilisateurs et de faire preuve de pédagogie. Néanmoins, cela n'est pas suffisant. Les contraintes métier sont importantes. Il doit montrer aux utilisateurs que la SSI apporte des solutions et les rassurer à nouveau : les mesures seront prises en commun et n'iront pas à l'encontre des objectifs métier.

Si certaines actions lui viennent rapidement à l'esprit et semblent simples à réaliser comme le cloisonnement des réseaux ou encore la définition d'une politique de gestion des médias

amovibles, les contraintes de certains ateliers ainsi que l'obsolescence de certaines installations demandent une analyse plus globale. Celles-ci impliquent plusieurs domaines d'expertise et l'obligent à adapter la démarche qu'il avait envisagée en trois étapes.

En particulier, les besoins d'évolution des SCADA des ateliers A et B ou encore de l'automatisme de l'unité de stockage et de distribution de matières dangereuses semblent plus complexes. Dans cette dernière unité, des aspects pour la protection des biens et des personnes (*safety*) sont en jeu. Une approche commune avec les experts du domaine de la sûreté est nécessaire.

Par ailleurs la question des sauvegardes et de la documentation n'a pas été abordée. Il est prévu de l'aborder, de même que d'autres thèmes transverses lors de la réunion de débriefing que le coordinateur veut organiser avec les différents responsables concernés par le sujet.

4.3 - Cartographie

La première étape de sa démarche est inchangée. Il établit une cartographie des installations suivant différentes vues qui lui permettront d'identifier les points faibles et les axes d'améliorations possibles. Les études AMDEC disponibles ont déjà clairement défini les niveaux de criticité des installations, ce qui permet d'établir rapidement une première cartographie des systèmes.

4.3.1 - Vue macroscopique des criticités

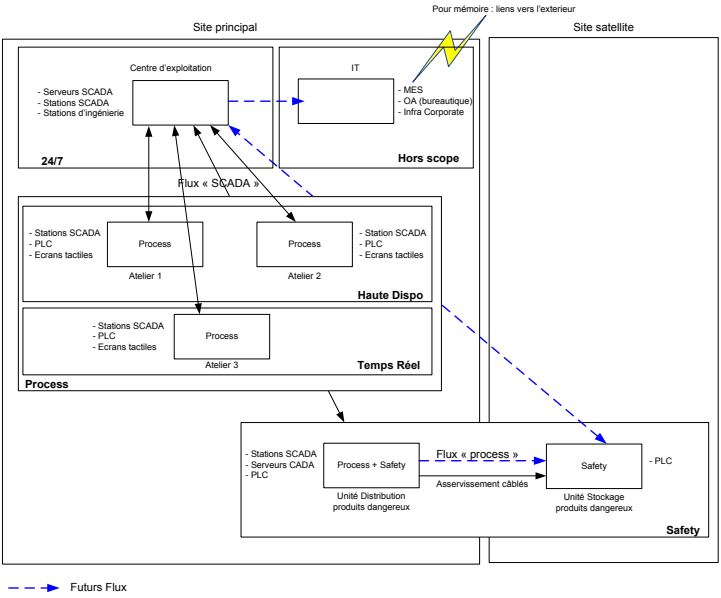

Fig. 1 - Cartographie macroscopique des installations en fonction des criticités

Les flux en pointillés sont les demandes d'évolutions.

Les installations situées dans le quartier « Haute Disponibilité » ont un impact fort sur la production en cas d'arrêt. L'atelier d'assemblage qu'il a visité se trouve dans ce quartier.

L'installation de distribution de matière dangereuse située dans la zone « safety » impacte également fortement la production en cas d'arrêt. Elle doit assurer une haute disponibilité mais la priorité est donnée aux fonctions safety.

Le centre d'exploitation est considéré comme stratégique car il permet de visualiser l'état des installations et de s'assurer que toutes fonctionnent correctement. Un niveau de disponibilité élevé est demandé même s'il est possible d'arrêter les installations de SCADA pendant quelques minutes sans qu'il y ait un impact significatif sur le bon fonctionnement du site. La procédure en cas de perte totale du SCADA dans le centre d'exploitation pendant plus de 15 minutes, comme cela est arrivé dans le passé suite à une panne réseau, entraîne sur décision du responsable de la sûreté l'évacuation du bâtiment de production.

4.3.2 - Vue physique de la topologie du réseau

Une analyse plus approfondie de la topologie du réseau est nécessaire pour comprendre comment sont connectés les différents équipements. Actuellement la situation n'est pas très claire. Il réalise ce travail avec des personnels du service IT habitués à ce type d'exercice et obtient la topologie suivante.

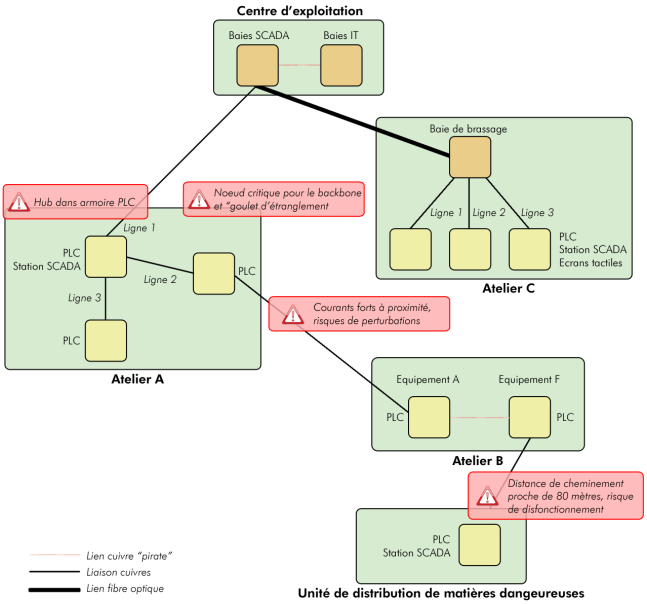

Fig. 2 - Vue physique de la topologie du réseau industriel

La topologie du réseau n'est pas cohérente et semble peu robuste. Elle a suivi les évolutions des ateliers mais n'a pas été pensée de façon globale.

Certains équipements sont raccordés sur des commutateurs placés dans des baies de brassage alors que d'autres sont raccordés sur des hub disposés directement dans les armoires électriques.

Une panne sur un hub de la ligne n°4 entraîne la perte du SCADA de l'atelier B et de l'unité de distribution de matières dangereuses.

Toujours avec le support des équipes de l'IT et en collaboration avec les différents responsables d'atelier il établit la topologie logique des installations.

4.3.3 - Vue logique des installations

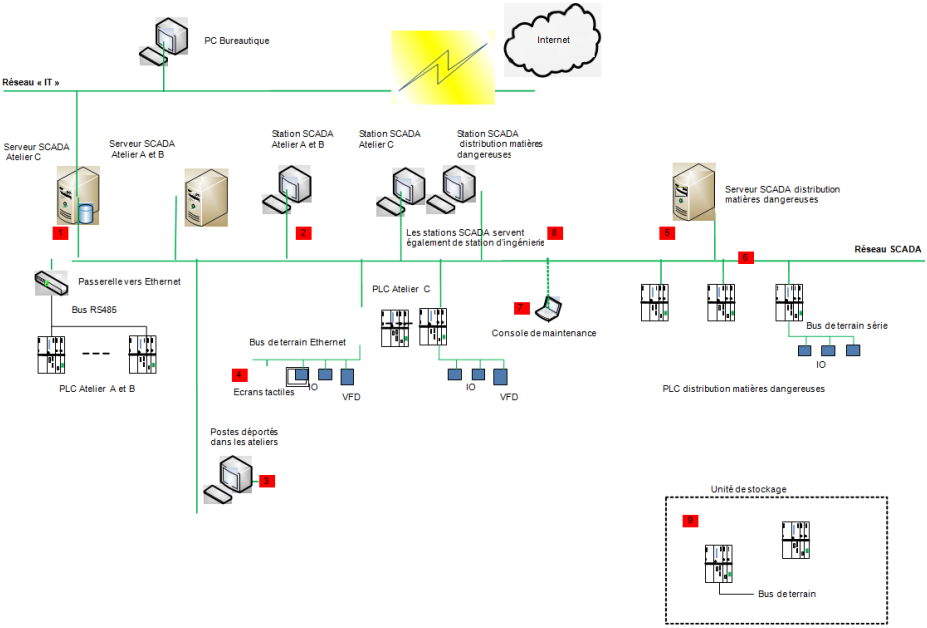

Fig. 3 - Vue logique des installations sur le réseau industriel

Le coordinateur indique sur le schéma les vulnérabilités recensées :

1. compromission possible depuis le réseau bureautique pouvant s'étendre vers le réseau industriel et réciproquement
2. systèmes obsolètes non maintenus, logiciels de configuration et de développement installés sur les postes permettant la modification des applications
3. login générique, poste facilement accessible
4. machines et systèmes « standards » sans mises à jour, peu de traçabilité des actions réalisées
5. serveur dans zones techniques, pas de mise à jour, peu de maitrise de la configuration, non uniforme avec les autres serveurs
6. tous les équipements sont connectés sur le même réseau sans aucune distinction de niveau de criticité. Un incident sur le réseau rend indisponible l'ensemble du centre d'exploitation et peut impacter les automates

7. console appartenant à un sous-traitant, pas de maitrise de sa configuration, risque d'introduction de virus
8. pas de mot de passe pour accéder au programme automates ou à sa configuration
9. pas de contrôle d'accès physique, peu de maitrise sur les configurations

Cette cartographie permet de positionner rapidement les principales vulnérabilités et de les expliquer aux utilisateurs. Le coordinateur s'en servira comme un document pédagogique pour expliquer aux divers responsables les risques.

4.4 - Analyse des nouveaux besoins

4.4.1 - Cas de la liaison WiFi

Le projet d'extension prévoit la mise en place d'une connexion WiFi entre les automates de l'unité de stockage et l'unité de distribution. La pose d'une fibre optique serait complexe et coûteuse du fait de la configuration physique du site.

Les solutions WiFi ne sont pas les solutions préconisées pour des installations sensibles. Les risques par rapport aux liaisons « filaires » sont plus importants que ce soit en termes de disponibilité (brouillage facile) ou d'intégrité des installations en amont (point d'accès physique facile).

La portée du Wifi est souvent sous estimée. Les technologies actuelles permettent de capter les signaux Wifi sur des distances importantes (plusieurs centaines de mètres voire plusieurs kilomètres suivant les configurations). Le Wifi est parfois utilisé lorsque la pose de fibre optique ou d'autre média est complexe voir impossible.

Il est important d'analyser les risques qu'apporte ce type de solution et de mettre en place les mesures pour les limiter.

Les études menées avec les personnes en charge de la sûreté ont indiqué que pour assurer la protection des biens et de personnes la perte de la liaison informatique entre les automates de l'unité de stockage et de distribution devra entraîner la fermeture des vannes de sécurité de l'unité de stockage (principe de sécurité positive).

Les risques SSI identifiés sur cette liaison sont la perturbation de la liaison (défaillance matérielle ou brouillage des ondes) et l'intrusion sur les installations suite à une vulnérabilité exploitée dans les équipements.

La perturbation de liaison n'impactera par les fonctions *safety*.

La configuration d'un pare-feu derrière le point d'accès serait un plus mais les automates utiliseront un protocole de niveau 2 (trames Ethernet) et pour des questions de maintenance, le filtrage sur adresse MAC n'est pas souhaité. La principale protection réside dans le chiffrement du protocole WPA2 et dans la configuration des clients et AP WiFi. Une mauvaise implémentation du protocole entrainera de nombreuses vulnérabilités.

Le cloisonnement de l'installation de distribution de matière dangereuse par rapport aux autres installations est fondamental pour éviter tout risque d'extension à l'ensemble

du site d'une éventuelle compromission par le WiFi.

L'analyse des flux et des connexions sur les équipements ainsi que la veille sur les vulnérabilités potentielles des équipements Wifi sont d'autant plus essentiels que la seule protection repose sur le protocole WPA2.

Les solutions de pare-feu applicatif ainsi que l'installation d'un serveur Radius sont à l'étude pour renforcer le niveau de sécurité.

4.4.2 - Cas de la télémaintenance

Bien que la nouvelle topologie le permette, la télémaintenance sur les automates de sûreté via un accès au service Web des CPU[4] n'est absolument pas envisageable.

Les défaillances sur les installations d'automatisme sont d'origine matérielle dans la majorité des cas comme le montrent les analyses AMDEC réalisées dans le passé et les retours d'expérience. Ces défaillances nécessitent une intervention physique sur l'installation pour la remise en service. Les pannes liées à un « bogue » de programmation sont réduites et nécessitent après intervention une requalification de l'installation. Sur les installations critiques, les modifications même mineures sont soumises à un processus de validation qui ne peut se dérouler à distance.

C'est pour cela que les processus de réception des installations imposent de réaliser des tests d'ensemble sur site, parfois très lourds, afin de s'assurer qu'il ne reste plus d'anomalies.

L'étude de sécurité réalisée conclut que la télémaintenance sur les installations critique n'est pas acceptable compte tenu des risques (difficulté d'établir des canaux sécurisés jusqu'aux installations de procédés, difficulté de garantir l'identité de la personne se connectant, complexité pour définir les limites de responsabilité en cas d'incident...). En revanche il est possible de déployer une solution de télédiagnostic.

Le coordinateur avait expliqué qu'il était nécessaire de déployer des outils d'analyse et de diagnostic. Ceux-ci permettront de centraliser sur un poste situé dans le centre d'exploitation les événements des SCADA et PLC. Ces informations pourront être accessibles via une DMZ pour les équipes de télémaintenance qui pourront qualifier l'incident et organiser plus efficacement l'intervention si besoin.

4.4.3 - Cas des échanges SCADA /GPAO

Les échanges avec le système de GPAO peuvent se réaliser par différents protocoles comme OPC ou SLQ par exemple. L'application SCADA peut écrire des données dans le système de GPAO ou réciproquement. Il est également possible d'utiliser un serveur « *repository* » placé sur une DMZ entre les réseaux ICS et GPAO ce qui serait une solution encore plus sécurisée.

La solution SQL conviendrait mieux aux équipes IT bien qu'elle ne soit pas plus sécurisée que la solution OPC. Cependant les équipes IT connaissent les problématiques associées comme les injections de code, les élévations de privilèges et connaissent déjà les contre-mesures à

4 CPU : Central Process Unit. Il s'agit de la partie de l'automate contenant le processeur et le programme exécuté.

appliquer alors qu'elles ne maitrisent pas la solution OPC.

Le coordinateur explique qu'en général plus les protocoles sont standards et utilisés par une majorité de personnes plus il est facile de les maîtriser et de trouver des compétences sur le sujet. Les vulnérabilités sont également identifiées plus rapidement et les correctifs rapidement disponibles.

5 - LE PLAN D'ACTION

5.1 - Evolution de l'architecture

Toujours avec les personnes de l'IT, il travaille sur une évolution de la topologie qui permettra à la fois de réduire les vulnérabilités en cloisonnant les réseaux et d'intégrer les nouveaux besoins en essayant d'anticiper les futurs :

- l'accès depuis des PC de bureau aux IHM des SCADA ;
- le lien entre les bases de données des SCADA et les applications de GPAO de l'entreprise ;
- la remontée des informations de la zone de stockage vers le centre d'exploitation ;
- le déploiement d'une liaison informatique pour les asservissements des futures installations entre la zone de stockage et la zone de distribution des produits dangereux ;
- potentiellement la télémaintenance.

Ces points seront de plus à étudier avec les personnes en charge de la sureté des installations. D'autant plus que des améliorations sur la protection physique des équipements sont à prévoir.

5.1.1 - Proposition d'architecture

Les travaux réalisés avec les équipes IT et les divers intervenants ont abouti à la proposition d'architecture ci-dessous. Le modèle d'urbanisation du réseau et des systèmes (et ségrégation) offre un découpage en zones et quartiers suivant les criticités et les fonctionnalités.

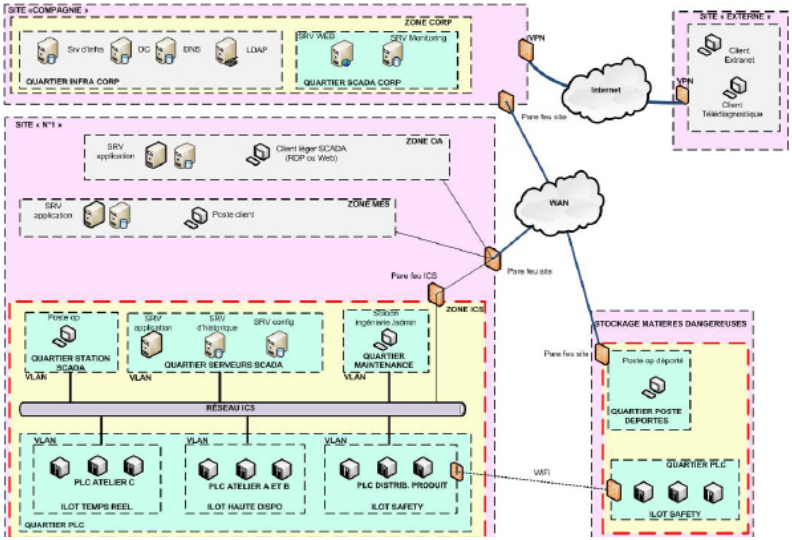

Fig. 4 - Proposition d'une architecture des installations industrielles et des interconnexions

Cette architecture facilitera l'intégration de futures installations et permettra d'appliquer la politique définie ci-dessous.

Les divers réseaux de la zone industrielle (ICS) peuvent être réalisés par des LAN ou des VLAN. Afin d'assurer un haut niveau de disponibilité, les pare-feux pourront être déployés en redondance.

Il est fortement recommandé de créer un VLAN « admin réseau » contenant l'ensemble des équipements réseau ICS (ce VLAN n'est pas représenté afin de ne pas surcharger le schéma).

Les règles présentées ci-dessous fournissent des principes et sont à préciser en fonction des besoins stricts de chaque installation.

Exemple de filtrage :

QUARTIER STATION SCADA : aucun flux entrant

- flux RDP et Web en sortie vers Quartier serveur SCADA ;
- flux WSUS en sortie vers QUARTIER INFRA CORP ;
- flux LDAP, kerberos, autre services d'infra en sortie vers zone Corp en fonction des besoins des applications.

QUARTIER POSTE DEPORTES : aucun flux entrant

- flux Web en sortie vers QUARTIER SCADA CORP ;
- flux WSUS en sortie vers QUARTIER INFRA CORP ;
- flux LDAP, kerberos, autre services d'infra en sortie vers QUARTIER INFRA CORP en fonction des besoins des applications.

QUARTIER SERVEUR SCADA :

- flux RDP et Web en entrée depuis QUARTIER STATION SCADA ;
- flux permettant l'accès au SCADA depuis les postes bureautiques (voir annexe B) : attention, les risques liés à cette règle doivent être clairement identifiés et acceptés en connaissance de cause ;
- protocole de communication PLC en sortie vers QUARTIER PLC ;
- flux SQL en sortie vers le QUARTIER SCADA Corp ;
- flux SysLog et SNMP vers QUARTIER SCADA Corp ;
- flux SQL ou OPC en sortie vers ZONE MES.

Dans les versions actuelles du protocole OPC les flux peuvent être complexes à gérer. Ils s'appuient sur les composants DCOM qui utilisent des ports alloués dynamiquement dans une plage donnée. Les flux peuvent être bidirectionnels. Dans ce cas les risques liés à cette règle doivent être clairement identifiés et acceptés en connaissance de cause.

Les ILOT PLC :

- flux pour les protocoles de communication PLC en entrée depuis QUARTIER SERVERS SCADA ;
- flux SysLog et SNMP en sortie vers QUARTIER SCADA Corp et QUARTIER SERVEURS SCADA ;
- flux NTP (pour la synchronisation des horloges) en sortie vers QUARTIER SERVEURS SCADA.

QUARTIER MAINTENANCE (ou ADMININISTRATION : aucun flux entrant

- flux LDAP, kerberos, WSUS et autre services d'infra en sortie vers QUARTIER INFRA CORP ;
- flux de programmation PLC en sortie vers QUARTIER PLC ;
- flux de programmation SCADA en sortie vers QUARTIER SERVEURS SCADA ;
- flux pour l'administration (HTTPS, SNMP, SSH) en sortie vers VLAN ADMIN RESEAU ;
- flux pour l'administration des serveurs et des applications (RDP par exemple en sortie vers QUARTIER SERVEURS SCADA.

QUARTIER SCADA CORP :

- flux SysLog et SNMP en entrée depuis ZONE ICS ;
- flux HTTPS en entrée depuis SITE Externe.

La majorité des applications SCADA fonctionnent avec un système d'exploitation Microsoft. Il est possible d'utiliser les Group Policy Object (GPO) pour déployer et gérer une partie des configurations systèmes ainsi que les outils Microsoft pour déployer les mises à jour. La gestion centralisée sera plus efficace que la gestion actuelle.

Les postes opérateurs et serveurs ne sont pas en nombre suffisant pour créer et gérer un domaine spécifique au SCADA. En revanche, regroupés avec les machines de la zone MES/GPAO, il deviendrait intéressant de créer un domaine spécifique (domaine Production par exemple) indépendant du domaine bureautique[5]. **Cela suppose que les zones MES et SCADA disposent du même niveau de confiance.** La gestion d'un domaine nécessitant des compétences spécifiques, elle sera opérée par l'IT.

Cette mutualisation facilitera l'administration et en particulier permettra une gestion plus efficace des comptes utilisateur. Cela pourra permettre de résoudre par exemple les problématiques de *logins* génériques.

5 La gestion des domaines peut se révéler complexe et être source de vulnérabilités importantes si elle est mal maitrisée. L'annexe C fournit quelques explications complémentaires sur les architectures de domaines.

5.1.2 - Proposition de la nouvelle topologie physique du réseau

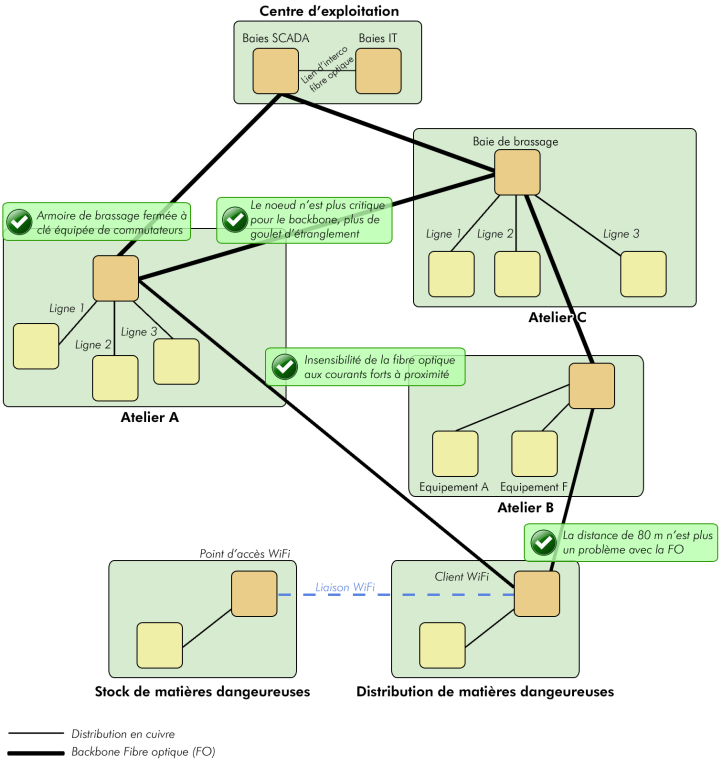

Fig. 5 - Proposition d'une nouvelle topologie physique du réseau industriel

Chaque atelier et unité sera raccordé au réseau SCADA par une baie de brassage intégrée dans une boucle afin d'améliorer la disponibilité. Les baies de brassage seront fermées à clés et un contact sec permettra de remonter sur le SCADA une alarme en cas d'ouverture.

Les équipements (PLC, Op, Postes SCADA) seront connectés en liaison cuivre sur les commutateurs dans les baies de brassage.

Plusieurs VLAN seront crées afin de respecter la ségrégation proposée précédemment. Le routage entre les VLAN sera complété par un filtrage.

L'interconnexion avec le réseau bureautique sera également réalisée au travers d'un pare-feu.

Cette topologie facilitera l'ajout de futures installations.

5.2 - Adaptation de la PSSI

Parallèlement aux mesures techniques un gros chantier de méthode et de définition de responsabilités pour l'exploitation et la maintenance des SCADA est à mettre en place (procédures d'exploitation, procédures d'intervention pour les sous-traitants par exemple).

Il se pose également la question du niveau d'implication des équipes IT qui disposent de compétences utiles et peuvent apporter un support efficace aux utilisateurs. Ces équipes pourront également aider au déploiement de la PSSI en prenant bien en compte les adaptions métier nécessaires.

Il conviendra en effet d'adapter la PSSI et plus particulièrement de :

- définir une politique pour la gestion des médias amovibles ;
- définir une politique de gestion des mots de passe y compris pour les comptes génériques (avec des restrictions), pour les automates, pour les sous-traitants ... ;
- mettre en place une gestion et surtout une traçabilité des évolutions des applications et de la documentation ;
- définir une politique de monitoring (qui ?, comment ?, quoi ?) ;
- définir une politique d'analyse des journaux d'événements ;
- définir un processus de traitement d'incident ainsi qu'une chaîne d'alerte ;
- définir une politique pour la protection antivirale est plus complexe car les applications sont sensibles. Les interactions négatives entre l'antivirus et les applications (souvent d'ancienne génération) qui n'ont pas été conçues pour cela sont prévisibles. Le coordinateur préfère travailler sur le durcissement des configurations pour les systèmes en production et limiter le déploiement des antivirus aux stations d'ingénierie et consoles de programmation ;
- définir une politique de sauvegarde des données et les procédures de restauration associées. Cela sera nécessaire pour l'élaboration du DRP.

5.3 - Évolution des applications

Enfin des évolutions des applications de SCADA sont à prévoir. Certaines sont simples comme:

- intégrer les déconnexions automatiques ;
- améliorer la traçabilité de l'utilisation des modes dégradés permis par les écrans tactiles dans les ateliers de production.

En revanche fusionner les applications SCADA des unités de production A et B avec l'unité C semble plus complexe. Les automates sont d'ancienne génération et le protocole de communication est propriétaire.

Le fabriquant de ces automates propose depuis peu de temps des convertisseurs de protocoles intégrant un serveur OPC. Cette solution permettrait à l'application SCADA de l'unité C de dialoguer avec les automates des unités A et B sans migrer les équipements (OPC UA) vers de nouvelles générations.

Ce protocole est connu pour être vulnérable même si des évolutions intégrant des mécanismes de sécurité sont en cours. La mise en place d'une politique de filtrage ainsi que le durcissement des configurations seront des mesures temporaires possibles en attendant ces évolutions.

5.4 - Audits et tests d'intrusion

Le coordinateur propose de demander à une société externe de réaliser un audit ainsi que des tests d'intrusion sur l'installation une fois que l'ensemble des évolutions auront été réalisées. Afin d'éviter de nouveaux impacts sur les installations lors des tests d'intrusion, le protocole d'audit sera validé en amont.

QUELQUES MOIS PLUS TARD...

Pour le coordinateur le bilan des actions conduites se révèle positif.

Les utilisateurs accèdent de manière plus sécurisée aux données des SCADA depuis leurs postes bureautiques ce qui leur simplifie de nombreuses tâches. La reprise et la fusion sur une même application des SCADA des ateliers A, B et C fournit une meilleure visibilité des installations pour les opérateurs et les responsables d'atelier. Le protocole OPC utilisé pour cela comporte des vulnérabilités mais les mesures de durcissement des machines et le cloisonnement des réseaux limitent considérablement les risques. La remontée des informations de l'unité de stockage a considérablement simplifié le travail des personnels de maintenance et d'exploitation. Les dysfonctionnements sont détectés plus rapidement.

Les réseaux « process » se limitent aux flux entre automates et entrées /sorties déportées. La mise en place de filtrage entre ces réseaux fournit des informations de diagnostic utiles et a permis de détecter de nombreux problèmes de configuration d'équipements (émissions de trames *broadcast* et *multicast* parasites, conflit d'adresses IP...). Les temps d'arrêt de la nouvelle chaîne de production ont été réduits. Les nouveaux tests d'intrusion réalisés ont été négatifs. Les scans réalisés sur le réseau bureautique puis étendus au réseau SCADA n'ont pas eu d'impact sur les réseaux d'automates. Les tentatives d'intrusion du réseau bureautique depuis le réseau SCADA n'ont pas réussi.

Comme l'a fait remarquer la direction du site, le plus important est sans doute que les utilisateurs ont compris l'intérêt de la SSI en général, dans leur vie de tous les jours mais surtout pour le domaine industriel. Ils ont compris qu'elle est un outil pour la disponibilité et la sûreté de fonctionnement indispensable avec l'utilisation des nouvelles technologies.

L'entreprise s'est « réappropriée » ses installations. Grâce aux études nécessaires pour mener ce projet les utilisateurs disposent d'une meilleure connaissance des installations et des procédures à respecter. Ceci, ainsi que le télé-diagnostic, a réduit les coûts de maintenance.

La SSI est un processus continu. Il reste de nombreux axes d'amélioration possibles. D'autres projets sont envisagés :

- l'analyse des données statistiques (sur les capteurs, actionneurs et alarmes par exemple) pour détecter des comportements aberrants ;
- la poursuite du développement des fonctions de « monitoring système » des SCADA et PLC ;
- le déploiement d'une solution centralisée pour les mises à jour des PLC, écrans tactiles et autres composants d'automatisme ;
- la création d'un plan de gestion de l'obsolescence afin de progressivement remplacer les équipements et logiciels les plus anciens et les plus vulnérables ;
- la création de plans de tests réguliers de non régression ;
- la création d'un plan d'audit établi sur la base de scénarios d'attaques ou de négligences ;
- la planification d'exercices pour tester la chaîne d'alerte et les procédures de traitement des incidents ;
- l'étude de solutions de virtualisation pour les applications serveurs, qui associées

à des clients légers, peuvent apporter des solutions pour améliorer la disponibilité ou pour restaurer rapidement des configurations en cas de sinistre. Ces solutions facilitent également le déploiement des mises à jour système.

L'ensemble de ces projets sera piloté par le coordinateur qui devient le correspondant SSI des utilisateurs du domaine industriel. Il est garant du respect des règles déployées et de la cohérence des actions avec le service IT.

ANNEXE A : SIGLES ET ACRONYMES

ADSL	Asymmetric Digital Subscriber Line
AMDEC	Analyse des Modes de Défaillance de leurs Effets et Criticités
API	Automate Programmable Industriel (PLC en anglais)
CPU	Central Process Unit
DoS	Denial of Service (Déni de Service)
DRP	Disaster Recovery Plan
EIA	Electrical Industry Association
ERP	Entreprise Resource Planning
FMDS	Fiabilité, Maintenabilité, Disponibilité et Sécurité
FMEA	Failure Mode and Effects Analysis
FAT	Factory Acceptance Test
GSM	Global System for Mobile
GPAO	Gestion de Production Assistée par Ordinateur
GTC	Gestion Technique Centralisée (SCADA en anglais)
GTB	Gestion Technique de Bâtiment
HAZOP	HAZard & OPerability method
ICS	Industrial Control System
MES	Manufacturing Executive System
MTBF	Mean Time between Failure
OPC	OLE for Process Control
OPC UA	OLE for Process Control Unified Architecture
OLE	Object Linked & Embedded
P&ID	Process & Instrumentation Diagram
PID	Proportionnel Intégral Dérivé
PLC	Programmable Logic Controller
RTC	Réseau Telephonique Commuté
RDP	Remote desktop Protocol
SAT	Site Acceptance test
SCADA	Supervisory Control And Data Acquisition
SdF	Sureté de Fonctionnement (= FMDS)
SPC	Statistical Process Control
SNCC	Système Numérique de Contrôle Commande
SNMP	Simple Network Management Protocol
SIL	Safety Integrity Level
SOAP	Service Object Access Protocol
SQL	Structured Query Language
SIS	Safety Instrumented System
VFD	Variable Frequency Drive
WSUS	Windows Server Update Services

ANNEXE B : ACCÈS AU SCADA DEPUIS DES POSTES BUREAUTIQUES

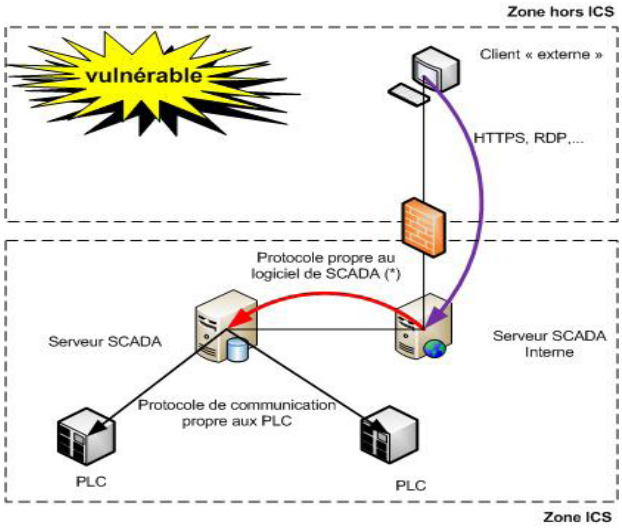

Fig. 6 - Accès aux données SCADA par un filtrage simple (solution fortement déconseillée)[1]

Avantages :

Les logiciels de SCADA du commerce permettent souvent de réaliser cette architecture.

Inconvénients :

- introduit des connexions entrantes dans la zone ICS ;

- une vulnérabilité dans le filtrage du pare-feu donne accès à toute la zone ICS ;

- une vulnérabilité dans le serveur « Interne » peut conduire à la prise de contrôle de toute la zone ICS.

ATTENTION : La prise de contrôle du client (compromission possible si le poste se connecte à Internet, utilise une messagerie, ne dispose ni de durcissements de sa configuration ni des bonnes mises à jour) fournit un accès légitime au serveur Web SCADA.

1 Ces protocoles intègrent peu d'éléments de sécurité, ce qui les rend vulnérables.

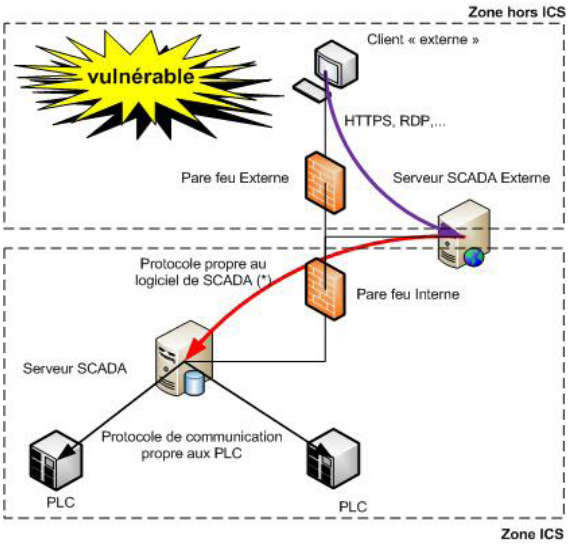

Fig. 7 - Accès aux données SCADA par une zone intermédiaire : (solution fortement déconseillée)[1]

Avantages :

Idem que la solution précédente.

Inconvénients :

- introduit des connexions entrantes dans la zone ICS ;

- le filtrage du flux pour le pare-feu interne peut être « laxiste » suivant le protocole propre au SCADA (ports dynamiques par exemple) ;

- la prise de contrôle du serveur « Externe » pourra permettre d'envoyer des télécommandes vers les PLC. Si le protocole propre au SCADA est vulnérable et permet l'exécution de code arbitraire, cela fournira un accès complet à la zone ICS. Les protocoles utilisés par les SCADA n'ont pas été conçus à l'origine pour faire face à des attaques informatiques et peuvent donc être très vulnérables.

ATTENTION : la prise de contrôle du client (compromission possible si le poste se connexte à Internet, utilise une messagerie, ne dispose ni de durcissements de configuration ni des bonnes mises à jour) fournit un accès légitime au serveur Web SCADA.

1 Ces protocoles intègrent peu d'éléments de sécurité, ce qui les rend vulnérables.

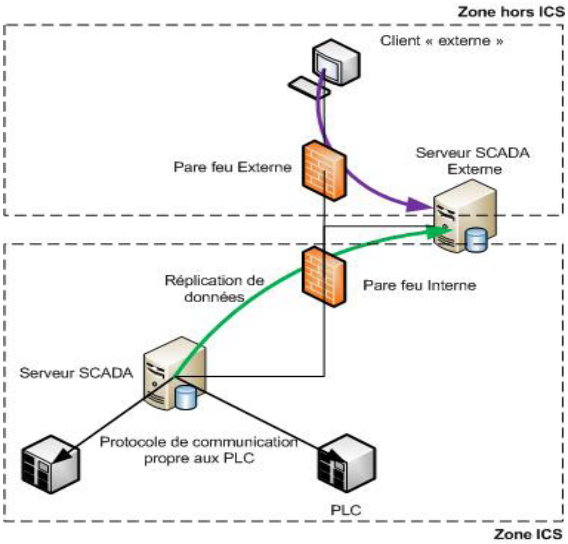

Fig. 8 - Accès au données SCADA au travers d'une zone démilitarisée : SECURISE

Avantages :

Pas de connexion entrante vers la zone ICS ce qui complique les tentatives d'accès malveillants à cette zone.

Inconvénients :

- peu de logiciels de SCADA du commerce permettent de réaliser cette architecture. Des développements spécifiques peuvent être nécessaires ;

- si le protocole utilisé pour « répliquer » les données vers le serveur « externe » présente des vulnérabilités il sera possible de prendre la main sur le réseau ICS.

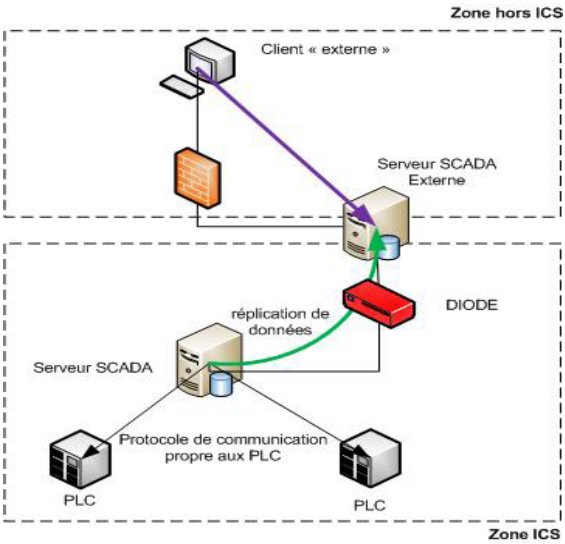

Fig. 9 - Accès au données SCADA au travers d'une diode : TRES SECURISE (solution préférée)

Avantages :

Aucune donnée provenant de la zone hors ICS ne peut entrer dans la zone ICS.

Inconvénients :

Peu de logiciels de SCADA du commerce offrent aujourd'hui la possibilité de réaliser cette architecture. Des développements spécifiques peuvent être nécessaires.

ANNEXE C : RESTRICTION DES FONCTIONNALITÉS LIÉES À L'EMPLOI DE MÉDIAS AMOVIBLES

L'usage de CD-ROM, de DVD ou de périphériques de masse USB (disque dur externe, clé USB, PDA, téléphone, appareil photographique, lecteur MP3, etc.) est aujourd'hui largement répandu. Ces médias, facilement transportables et difficilement contrôlables, peuvent être utilisés pour sortir illégitimement des données d'un système d'information et constituent un vecteur important d'introduction de codes malveillants.

Or, si les lecteurs CD et/ou DVD peuvent être supprimés (comme les lecteurs de disquettes en leur temps), il est moins évident de se passer des connecteurs USB, ceux-ci étant aujourd'hui employés par des périphériques légitimes tels que les claviers ou les souris.

Des mesures logiques peuvent toutefois être mises en œuvre sur le système d'exploitation Windows afin de couvrir les menaces d'introduction de codes malveillants et de fuite d'information.

Blocage de la détection des périphériques de stockage USB

Si aucun périphérique de stockage USB n'a été préalablement installé sur le poste (action à réaliser sur un « master »), il suffit d'attribuer à l'utilisateur les autorisations « Refuser » pour les fichiers suivants :

- %systemroot%\Inf\Usbstor.pnf
- %systemroot%\Inf\Usbstor.inf

Désactiver le pilote de gestion des périphériques de stockage USB

Pour empêcher d'utiliser des clés USB, il faut positionner à 4 la valeur Start de la clé de registre suivante (effectif après redémarrage du poste) :

HKLM\SYSTEM\CurrentControlSet\Services\UsbStor

Les claviers, souris et autres périphériques USB fonctionneront toujours. Pour plus d'informations, se reporter au site de Microsoft1.

Blocage de l'écriture sur les périphériques USB

A partir de Windows XP SP2, il est possible de connecter les périphériques USB en lecture seule. Il faut pour cela créer ou modifier la valeur dénommée WriteProtect (de type DWORD), en lui affectant la donnée 1, dans la clé :

HKLM\System\CurrentControlSet\Control\StorageDevicePolicies

Désactiver l'exécution automatique

Les fonctionnalités autorun et autoplay peuvent être complètement désactivées pour tous les types de lecteurs en modifiant les stratégies de groupe. Le paramètre se trouve dans la Configuration ordinateur, Modèles d'administration, Système et est dénommé « Désactiver

le lecteur automatique ». Il doit avoir la valeur «activé», en spécifiant « tous les lecteurs ».

Les correctifs de sécurité Windows doivent également être appliqués pour corriger les vulnérabilités liées aux supports USB. Les stratégies de restriction logicielle peuvent également être configurées pour interdire l'exécution de programmes depuis d'autres lecteurs que les lecteurs de disques durs.

ANNEXE D : LES 10 RÈGLES POUR L'UTILISATION DES SCADA

Exemple des 10 règles d'utilisation des SCADA à afficher dans le centre d'exploitation et dans les différentes zones du site :

1 - Verrouiller ou fermer les sessions lorsque vous quittez une station ou un écran tactile ;

2 - Ne pas « prêter » ses identifiant /mot de passe à ses collègues ;

3 - Ne pas connecter de clés USB, disques durs externes, téléphones portables ou autres périphériques sur les machines ;

4 - Utiliser les sas pour importer ou exporter des données depuis ou vers l'extérieur ;

5 - Ne pas sortir les consoles de programmation et de maintenance et ne pas les connecter sur d'autres réseaux que ceux des SCADA. Les stocker dans le centre d'exploitation ;

6 - Ne pas conserver de données sur les stations et consoles de programmation. Utiliser les espaces de stockages partagés prévus à cet effet ;

7 - Refermer à clé les armoires PLC, compartiments courants faibles et baies de brassage après les interventions ;

8 - Ne pas redémarrer un équipement défaillant (Station SCADA, OP, PLC…) sans l'intervention d'un spécialiste ;

9 - Ne pas connecter d'équipement non sûr sur le réseau SCADA ;

10 - Signaler toute situation anormale au responsable du centre d'exploitation.

En cas de doute, s'adresser à son responsable hiérarchique.

ANNEXE E : DOMAINES MICROSOFT WINDOWS

Plusieurs architectures de domaines sont possibles. Chacune présente des avantages et des inconvénients. Il est important de choisir l'architecture qui respecte les exigences de sécurité et les besoins fonctionnels.

Les schémas ci-dessous présentent les principales caractéristiques de solutions couramment répandues.

Domaines et sous domaines (architecture fortement déconseillée) :

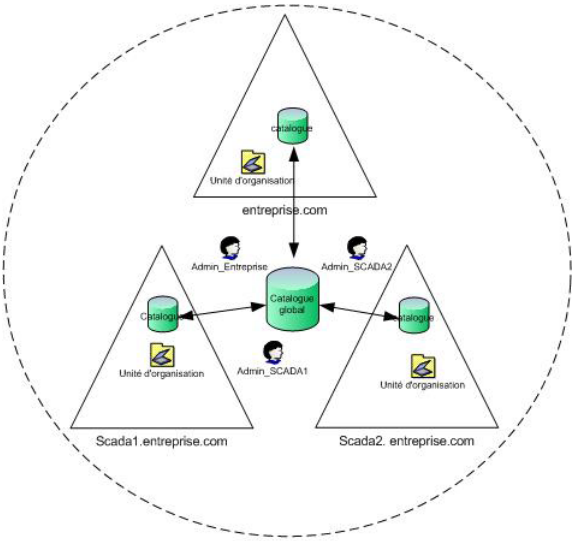

Fig 10 - Schéma de principe domaines et sous domaines

Les relations d'approbation entre l'ensemble des domaines sont créées automatiquement par le système lors de leur création. Par défaut, elles sont bidirectionnelles.

Il existe un catalogue global pour tous les domaines ainsi qu'un catalogue par domaine avec mécanismes de réplication de certains objets.

Les *policies* du domaines entreprise.com s'appliquent implicitement aux domaines SCADA1.entreprise.com et SCADA2.entreprise.com

L'utilisateur d'un domaine peut accéder aux autres domaines dès qu'il est authentifié sur l'un d'eux.

La compromission d'un domaine compromet tous les autres. Exemple : la prise de contrôle de l'utilisateur Admin_SCADA1 permet d'exécuter des taches d'administration dans les autres domaines.

Domaines indépendants (architecture préférée) :

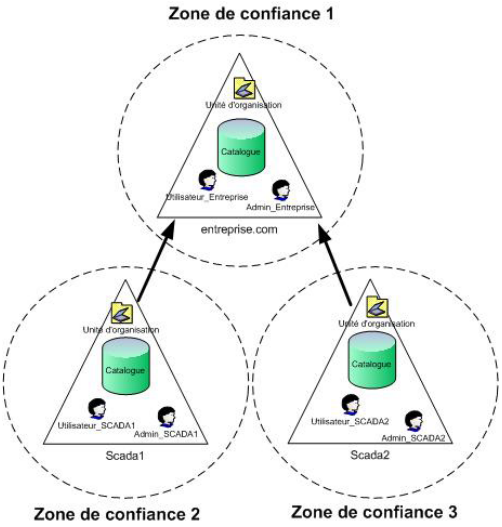

Fig. 11 - Schéma de principe domaines indépendants

Les relations d'approbation sont déclarées manuellement par les administrateurs des domaines. Elles peuvent être unidirectionnelles ou bidirectionnelles.

Il existe un catalogue global indépendant par domaine.

Les *policies* du domaine entreprise.com ne s'appliquent pas aux domaines SCADA1 et SCADA2.

L'utilisateur d'un domaine n'accède aux autres domaines que si des droits lui sont explicitement accordés dans les autres domaines.

La compromission d'un domaine se limite à ce domaine.

ATTENTION : si l'utilisateur admin_entreprise est déclaré comme membre des groupes d'administration dans les domaines SCADA, sa compromission entraine la compromission des domaines SCADA.

THÈMES ABORDÉS

Ce guide sur la cybersécurité des systèmes industriels a été réalisé par l'agence nationale de la sécurité des systèmes d'information (ANSSI)

avec le concours des ministères suivants :

et des sociétés suivantes :

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Version 1.0 - Juin 2012

Agence nationale de la sécurité des systèmes d'information

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr