Si on jouait à se faire peur ?

Ouille, ouille, ouille… la dernière journée du Club Automation sur la Cybersécurité n'a pas fait que des heureux. Finie l'époque des gentils pirates qui, encore mineurs, cherchaient à se faire un nom, aujourd'hui ce sont les méchants qui s'intéressent à vous, à votre production.

Ce fut un peu comme l'attaque du Ponant, le bateau de luxe français qui croisait au large de la Somalie. Le réveil pour les participants du Club Automation fut aussi brutal. Les pirates n'ont pas disparu, seuls les moyens ont changé, dans le cas du Ponant, les kalachnikovs ont remplacé les épées et les commandos de la marine ont troqué le mousqueton par un fusil MacMillan apte à tirer avec précision une munition de 12,7 mm à près de 2000 mètres.

Pour Jean-François Pacault, Haut Fonctionnaire de Défense et de Sécurité, il est clair que l'on peut de plus en plus facilement exploiter les vulnérabilités des systèmes industriels d'information et de contrôle, à la fois parce qu'ils sont maintenant connectés au reste de l'entreprise et parce qu'ils utilisent de plus en plus des produits, des protocoles et des logiciels largement répandus et dont les failles sont déjà couramment exploitées en informatique générale.

Exposés maintenant au même genre d'attaques que l'informatique générale, ils font donc courir aux entreprises le même genre de risques, comme des pertes de production, des divulgations d'informations confidentielles, des atteintes à l'image de marque. Ils présentent des risques particuliers puisqu'ils peuvent, en cas de dysfonctionnement, mettre en danger la santé, voire la vie, des employés de l'entreprise.

LA BANALISATION

L'informatisation des systèmes de contrôle/commande des outils industriels a débuté à la fin des années 60. Elle s'est tout d'abord appuyée sur des solutions propriétaires où tout était spécifique à partir de cahiers des charges adaptés à chaque process. Aujourd'hui, bien que les fonctions de bases soient restées les mêmes (programmation d'automates, commandes de machines…), les dispositifs informatiques ont changé. Le réseau utilisé est partagé avec l'informatique de gestion, les ordinateurs fonctionnent sous Windows ou Unix et les bases de données sont des produits du commerce.

Les réticences des premiers temps face à l'introduction de produits banalisés dans un environnement industriel se sont progressivement effacées face à l'attrait que représente le coût relativement bas de ces équipements, bien qu'ils ne soient pas complètement adaptés aux contraintes industrielles.

Malheureusement ces équipements ont amené les faiblesses qui leurs sont propres et ouvrent ainsi la porte à des attaques sur les moyens de production industriels qui, jusque là, étaient protégés par leurs spécificités techniques.

LE POINT DE VULNÉRABILITÉ

Le réseau est l'élément fédérateur des équipements d'un système de commande/contrôle ; il est donc, par nature, le point sensible de l'installation. Mais l'interconnexion avec des réseaux ouverts sur l'Internet, l'usage des liaisons sans fil dans des bandes de fréquences ouvertes à tous, créent de nouveaux points d'entrée qui peuvent être exploités pour initier des intrusions externes ou internes à l'entreprise.

Si les objectifs de ces attaques peuvent être d'origine très diverses (espionnage, hacking, sabotage…), les moyens utilisés sont identiques : ils exploitent les failles des matériels et des logiciels utilisés.

De plus, les systèmes qui gèrent les processus industriels sont souvent interconnectés avec les systèmes support de l'informatique de gestion : une faiblesse dans la protection des uns entraîne, de ce fait, une vulnérabilité dans la protection des autres.

Malheureusement, étant données la complexité et la diversité des systèmes utilisés dans le pilotage des process industriels, il n'est pas possible de transposer simplement les règles et procédures de sécurité aujourd'hui appliquées dans le monde de l'informatique de gestion.

LE RISQUE D'ATTAQUE EST RÉEL

Une augmentation significative des attaques concernant l'informatique industrielle a été constatée aux USA depuis septembre 2001. Parmi les incidents publiés, on peut noter une grande diversité des cibles (centrale nucléaire, unités de traitement des eaux, ports maritimes…) qui laisse envisager une grande diversité d'impacts.

Les conséquences des perturbations d'un système automatisé dépendent de la nature de ce système. Pour les systèmes de gestion, on mesure bien les risques : divulgation d'informations confidentielles, corruption des données, indisponibilité du système…

La nature des process qui pilotent l'informatique industrielle et son fonctionnement en temps réel donnent une autre dimen-

sion à ces risques qui peuvent entraîner des problèmes de santé publique, des dégradations de l'image de l'entreprise, la divulgation de données confidentielles… Ces impacts sont en général bien connus des responsables de l'informatique industrielle et les risques étaient maîtrisés, implicitement le plus souvent, quand les systèmes de contrôle industriel étaient simples, isolés les uns des autres, non connectés aux réseaux informatiques de l'entreprise et rarement connectés avec l'extérieur. Ces systèmes se sont complexifiés, ils ne sont plus isolés et, puisqu'ils utilisent largement des logiciels et des protocoles d'usage courant, ils présentent dorénavant le même genre de vulnérabilités que les systèmes de gestion : les risques se sont aggravés et il est maintenant indispensable, pour les maîtriser, de les analyser méthodiquement.

COMMENT SE PROTÉGER ?

Il est clair qu'il n'existe pas de réponse unique en raison de la variété des contextes (systèmes nouveaux ou amélioration de systèmes existants, diversité des technologies, contraintes opérationnelles…). *« Au final, le choix des solutions résultera d'un compromis entre le coût de développement et les contraintes d'utilisation, d'une part, et celui des conséquences des risques résiduels d'autre part*, explique Jean-François Pacault du Service du Haut Fonctionnaire de Défense et de Sécurité au Ministère de l'industrie. *Ceci étant, la définition d'une politique de protection propre à l'informatique industrielle doit s'inscrire dans le cadre plus général de la politique de protection du patrimoine de l'entreprise. Elle exige une analyse méthodique des risques pesant sur l'ensemble des activités de production industrielle, une prise de conscience de tous les responsables de l'entreprise au plus haut niveau, la sensibilisation de tous les échelons et la diffusion d'instructions aussi opérationnelles que possible. »*

Il est généralement admis que la démarche de sécurisation comprend les étapes suivantes :

- Analyser et comprendre les enjeux ;
- Identifier les éléments sensibles et les systèmes qui justifient une protection (confidentialité de données, disponibilité de processus, intégrité de paramètres techniques…) ;
- Analyser les risques (identifier les menaces et évaluer les vulnérabilités) ;
- Mettre en évidence les contraintes ;
- Déterminer une architecture dont le niveau de sécurité réponde aux risques identifiés ;
- Déterminer l'ensemble des mesures d'accompagnement sous les aspects sécurité physique (protection des locaux, contrôle du personnel, procédures…) ;
- Faire le bilan des risques résiduels.

« Parallèlement à cela, il sera nécessaire de développer des procédures d'alerte et d'intervention en cas d'incidents ou d'anomalies, tout comme de former et entraîner le personnel. Il faut par ailleurs analyser les risques induits par la sous-traitance, les partenariats, la clientèle et les fournisseurs. Plus largement, il convient d'introduire dès le début, pour tout projet d'informatique industrielle, la prise en compte du volet protection contre les risques de malveillance, et définir clairement les rôles et responsabilités de chacun, en particulier pour la validation des moyens de protection. Ces principes généraux sont ceux de la norme SP-99 et des documents qui l'accompagnent. Ce sont les seuls textes disponibles actuellement qui abordent de façon méthodique la sécurité de l'informatique industrielle. Ils constituent un bon point de départ pour prendre en compte la problématique de la sécurisation des systèmes d'information à vocation industrielle. »

Il est donc de la responsabilité des automaticiens de prendre les choses en main avant qu'elles ne leur échappent, car la culture des réseaux ne leur est pas assez connue, la part des automatismes dans les réseaux ne doit plus être négligée. Il n'empêche, conclut Jean-François Pacault du Ministère, *« que les escaliers se balayent par le haut, et qu'il faut donc que la direction de l'entreprise prenne conscience des risques encourus. Et vue la vitesse d'évolution de la technologie chaque minute compte »*.

PIRATE OU CORSAIRE ?

Revenons à notre histoire du Ponant, le bateau croisière. Il s'agissait bien de pirates, des hors-la-loi qui pillaient pour leur besoin propre. La différence avec le corsaire, c'est que ce dernier est mandaté par une personne physique ou morale pour effectuer des opérations malhonnêtes. Et à en croire, l'intervenant de la DST à ces journées organisées par le Club Automation, ce ne sont plus de jeunes pirates qui s'attaquent aux technologies et aux industries, mais bel et bien des corsaires organisés, qui reçoivent des « commandes » pour voler des informations et déstabiliser une entreprise ou des individus clés de cette entreprise.

Certes le représentant de la DST est arrivé « masqué » (interdiction de prendre des photos, de citer son nom, d'enregistrer ses dires – c'est tout juste si l'amphithéâtre n'a pas été mis en quarantaine), mais au bout de quelques minutes les participants ont compris pourquoi : il n'était pas venu les mains vides, la DST était en représentation et ne voulait pas s'en tenir à de simples paroles affolantes. Le matériel était sur la table.

Un matériel somme toute commun à tout le monde. Il n'avait pour bagage que son modeste PC portable payé par le contribuable, une vulgaire clé USB et une boîte de Ricoré. Une façon de démontrer que ce sont souvent les grands classiques qui sont toujours employés.

Plusieurs centaines de PC ont été volés dans les TGV et autres lieux publics, et trop souvent les personnes annoncent que le PC portable ne contenait que des données anodines. Difficile à croire pour notre expert de passage. Démonstration, devant la salle, de récupération d'informations dans un PC ordinaire, tous les mots de passe et autres données soi-disant formatées remontent à la surface en quelques secondes. D'ailleurs, insiste l'intervenant, lorsque vous jetez un PC, ne laissez pas le disque dur à l'intérieur, et sachez que même, théoriquement cassé, un disque dur parle toujours, seul l'acide peut le faire taire à jamais. *« Lorsque l'on voit des grandes entreprises qui donnent leurs vieux PC avec un disque dur, théoriquement formaté, à toutes sortes d'association, il y a de quoi s'inquiéter »*. Et cette réserve est bien entendu valable pour les PC, mais également pour tous les composants informatiques qui partent en destruction ou en maintenance,

un photocopieur inclus le plus souvent un disque dur, duquel il sera aisé de sortir l'ensemble des dernières impressions.

Et parfois le PC ne vous est même pas volé, c'est la douane ou une autorité d'un pays « lambda » qui, pour des raisons de sécurité, embarque quelques instants votre PC dans un lieu tenu secret, inutile de vous demander ce qu'ils en font. Alors règle numéro un, tellement évidente qu'elle n'est pas respectée : Ne jamais mettre d'indication sur le PC ou la clé USB, *« coller un autocollant arborant fièrement le logo de votre entreprise Airbus ou Total ne peut qu'inciter les prédateurs »*.

PC, CLÉ USB... MÊME COMBAT

Evidemment dans le cas d'un emprunt de votre PC durant quelques instants, il n'aura pas servi qu'à récupérer des informations, il est peut-être devenu, à son insu, un PC qui dans l'avenir parlera, se mettra en relation avec le réseau d'entreprise et transmettra des informations à l'heureux mandataire du corsaire.

C'est à cet instant que le représentant de la DST, sort de sa poche une clé USB, semblable à celles du commerce, et demande dans l'assistance si quelqu'un veut bien lui prêter un PC. Il essuie un refus, bien mérité. Car, en deux secondes, il l'introduit dans un PC portable, ce dernier ne reconnaissant pas la clé USB, il l'enlève, fait mine d'un dysfonctionnement, s'excuse et part avec sa clé, qui, pour la démonstration, était vierge avant l'introduction et pleine deux secondes plus tard. Pleine de données spécifiques, tous les fichiers texte et autres tableurs, mais surtout pleine de l'ensemble des mots de passe utilisés. En retour la clé USB a laissé un cheval de Troie dans le PC, histoire de suivre ce dernier à la trace.

Mais que faire ? Des mots de passe codés ? Il ne faudra également que quelques secondes pour les voir apparaître en direct sous les yeux incrédules des participants. Bien entendu, l'inverse reste vrai. Vous introduisez votre clé USB dans un PC, chez un client pour uniquement visualiser un fichier, et le PC en profite pour pirater le contenu de votre clé et introduire des éléments. Et inutile de croire qu'un formatage de la clé efface les données. Devant les participants, c'est ce qui fut fait à maintes reprises sur la clé USB présente, et en quelques secondes les informations réapparaissaient.

Le pire dans toute cette démonstration, c'est que l'ensemble des logiciels permettant ces tours de passe-passe se trouvent en libre service sur Internet, disponibles pour le commun des mortels.

IMAGINEZ VOTRE SMS ENVOYÉ À TOUT LE MONDE

Et s'il n'y avait que les intrus physiquement reconnaissables, ce serait simple. Car aujourd'hui on ne parle que de sans-fil, et alors tout devient encore plus amplifié. Les virus destinés aux mobiles communiquant sur Bluetooth seraient aujourd'hui au nombre de 350, avec plus de 800.000 codes malveillants, normal il existe déjà 500 millions d'objets dialoguant avec Bluetooth. C'est ainsi que Paris Hilton a découvert vingt minutes après une intrusion sur son portable, l'ensemble de son carnet d'adresses disponible sur Internet. Et le petit malin qui avait réussi l'opération avait 17 ans.

Le dernier virus pour mobile, envoie votre dernier message envoyé à l'ensemble de votre carnet d'adresses. *« Imaginez votre dernier SMS envoyé à tout le monde »*.

Certes, si mobile et Bluetooth restent des technologies utilisées dans le monde industriel, elles ne le sont pas pour le contrôle/commande qui reste la priorité des automaticiens. Seulement, les autres communications sans-fil sont également visées. C'est ainsi que la boîte de Ricoré reste l'une des meilleures antennes pour capter vos communications ADSL. Et ne croyez pas les distances annoncées par les opérateurs, elles peuvent largement être multipliées par 10, 100 voire 1000 pour atteindre plusieurs kilomètres. Le signal ne s'arrête pas à la porte de votre bureau, il « bave » forcément, il suffit alors de le récupérer. C'est un peu comme si l'on donnait le volant d'une Formule 1 à des utilisateurs qui n'ont même pas le permis. Il suffit dans un aéroport de connecter son PC pour voir le nombre de PC qui sont prêts à rentrer en communication avec vous. Si vous ramenez votre PC de bureau chez vous, pour continuer un travail en utilisant votre connexion ADSL sans-fil, pensez aux données qui sont présentes dans le PC.

Bien entendu, la récupération d'informations n'est pas que le seul motif. Il reste des méthodes simples et toujours efficaces, comme la saturation d'un réseau. Il suffit d'un virus qui infecte des milliers de machines dans le monde et qui, à un instant donné, vont toutes vouloir se connecter sur un site ou un serveur, et c'est le blocage de la communication assuré. Imparable.

Surtout que les pirates, ou plutôt corsaires, peuvent aller plus loin. Ils peuvent ne rien prendre sur votre PC mais au contraire y introduire, sans que vous le sachiez, des données qui ne seront même pas des virus mais des photos compromettantes. Des cas existent de personnes physiques ayant été discréditées par des éléments compromettant trouvés par la police lors d'une perquisition. Il aura fallu six mois pour remonter la source et s'apercevoir que la personne soupçonnée n'y était pour rien. Et six mois dans ces conditions, c'est long.

Pourtant la loi est intransigeante. Le code pénal est sans ambiguïté, le vol reste du vol, l'extorsion de fond ou le faux mail peuvent valoir six mois de prison. La DST recommande de toujours se connecter en mode VPN (infos cryptées) aux points d'accès Wi-Fi public, et de préciser pour ceux qui l'auraient oublier la loi de Gilb qui veut que *« Tout système dont la fiabilité dépend d'un être humain n'est pas fiable »*.

Et ne croyez pas que les spécialistes soient eux-mêmes à l'abri de toutes erreurs. Sachant que les fichiers Word conservent l'ensemble des informations, même celles effacées, les spécialistes n'envoient jamais de fichiers Word mais uniquement un fichier Pdf du texte. Seulement faut-il encore paramétrer correctement son fichier Pdf et ne pas faire de modifications. C'est ainsi que la CIA s'est faite prendre la main dans le sac avec des fichiers confidentiels en Pdf sur lesquels les noms des personnes ayant fourni les informations étaient masqués

par des pavés noirs. Seulement, le paramétrage avait été mal fait, et il suffisait de faire glisser le pavé en dehors du texte pour récupérer le texte complet. Ce qui a valu un incident diplomatique entre deux pays.

LES UTILISATEURS SONT D'ACCORD

Pour Stefan Lueders, consultant sécurité pour le CERN, le problème est réel. Beaucoup trop de systèmes de contrôle/commande sont interconnectés par le réseau Ethernet en utilisant la couche TCP/IP. *« Ils héritent des avantages de l'IT standard, les automates programmables peuvent maintenant envoyer des mails, mais est-ce vraiment raisonnable ? »*

Le projet de collisionneur de hadrons est le plus grand et le plus puissant des accélérateurs de particules au monde avec 27 kilomètres de circonférence, il permettra de faire progresser notre compréhension de l'Univers. Une machine qui accélère deux faisceaux de particules à plus de 99,9 % de la vitesse de la lumière avant de les projeter l'un contre l'autre. Pour cette application, le CERN se retrouve à la tête de 125 systèmes de contrôle en provenance de fournisseurs différents qu'il faut faire dialoguer. Et les problèmes ne manquent pas, entre les fournisseurs qui livrent des produits intégrant des fonctions de communication avec des mots de passe vides, permettant à tout le monde de rentrer dans le système.

Pour Stefan Lueders, trop souvent les systèmes sont construits sur des châteaux de sable. Pourtant, il existe des outils développés pour l'informatique bureautique qui permettent de valider chaque automate programmable. Le CERN n'a reculé devant aucun sacrifice, plus de 50 automates programmables ont été testés avec le logiciel Nesus qui effectue des milliers de tests tournant autour de la communication. Résultat, seulement 17 % des automates du commerce étaient configurés correctement, pour le solde la moitié ne marchait plus à la fin des tests. *« La réponse des fournisseurs nous a laissé sans voix, ils n'avaient pas détecté de demandes importantes de la part de leurs clients. La seule solution, c'est la vérification automate par automate, matériel par matériel car mêmes des oscilloscopes qui intègrent des composants PC peuvent être mal paramétrés »*.

Alors faut-il revenir aux méthodes d'antan ? Arrêter toute communication et installer des automates programmables propriétaires avec des ports de communication propriétaires, sur un bus propriétaire ? Telle est la véritable question. Si vous croyez qu'en passant de Microsoft à Unix vous prenez moins de risques, il n'en est rien. L'on n'est peut-être pas obligé d'aller jusque là, précise l'intervenant de la DST, *« évitez déjà de coller un post-it avec votre mot de passe sur l'ordinateur, ce sera un bon début ! »*.

MÉTHODE À SUIVRE

Pour conclure cette journée, sur une note plus optimiste, c'est Jean Pierre Dalzon, de l'ISA qui décrit les travaux du comité ISA SP99 qui visent à permettre la

ET VOUS ?

IDÉES REÇUES ET QUESTIONS QUI FONT PEUR

Les attaques courantes sur la bureautique sont impossibles sur l'informatique industrielle (virus, exploitation de vulnérabilité, malveillances internes...).

Faux : l'une et l'autre utilisent les mêmes produits (Windows, Unix...) et les mêmes protocoles (IP en général). Elles présentent donc le même genre de vulnérabilité et les mêmes malveillances qui auront les mêmes effets informatiques (mais pas les mêmes conséquences sur l'entreprise).

C'est ainsi qu'en janvier 2003, le ver Slammer s'est introduit dans les ordinateurs de commande de la centrale nucléaire américaine Davis Besse par une connexion non sécurisée avec le réseau bureautique. Conséquence : un système de contrôle de la sûreté de la centrale est resté indisponible pendant près de cinq heures !

Mon système n'intéresse pas les pirates qui prolifèrent sur internet.

Faux : ces pirates sont en permanence à l'affût des systèmes vulnérables et les détectent. Ils les attaquent dès qu'ils en ont la possibilité.

Mes concurrents n'auraient pas les compétences nécessaires pour attaquer mon système, et d'ailleurs ils n'oseraient pas recourir à de telles pratiques.

Faux : il serait imprudent de l'affirmer. D'une part, il est facile de louer les services de pirates compétents, notamment à l'étranger. D'autre part, comme les attaques informatiques restent souvent anonymes, ce n'est pas la crainte d'être découvert qui dissuade beaucoup les malveillances. Enfin, puisqu'on voit régulièrement, en informatique générale, des exemples d'attaques informatiques de la part de concurrents peu scrupuleux, il n'y a pas de raison qu'il ne s'en produise pas visant l'informatique industrielle, si elles sont, pour l'attaquant, moins difficiles à perpétuer et plus rentables – récupération d'informations confidentielles, par exemple sur les procédés et secrets de fabrication, perturbations des chaînes de fabrication, atteintes à l'image de la société…

Aucune attaque interne n'est à craindre

Faux : D'abord les employés peuvent parfois causer des dommages importants parce qu'ils sont mal formés, inconscients ou négligents : il faut donc prendre soin de leur formation comme de leur sensibilisation, promulguer une carte d'utilisation des moyens informatiques et veiller à ce que les procédures appliquées minimisent les risques de négligence.

Ensuite, il peut arriver que certains employés, mécontents ou soumis à des pressions externes, commettent des malveillances, et la tentation est grande s'ils pensent qu'ils ne seront pas identifiées : une précaution indispensable est que les actions critiques ne puissent être effectuées que par certaines personnes et soient commodément imputées à leurs auteurs.

Savez-vous si vos réseaux d'informatique industrielle sont bien protégés du reste de l'entreprise et du monde extérieur ? Etes-vous certain que les connexions vers l'extérieur de votre système de contrôle de processus, et notamment les accès Wi-Fi, sont correctement recensées et sécurisées ?

Sur une durée d'un an environ, en 2006, des pirates ont espionné les connexions Wi-Fi des caisses de la chaîne de supermarchés américains TJX qui n'étaient pas sécurisées. Ils ont ainsi récupéré des millions de numéros de cartes bancaires qu'ils ont utilisés au détriment des clients de TJX.

Il n'est pas rare de découvrir par hasard des bornes Wi-Fi et des modems reliés au réseau téléphonique public dont les administrateurs système ignorent l'existence.

Dans la centrale nucléaire Davis Besse, le ver Slammer s'est introduit par une connexion non sécurisée alors que les équipes croyaient être protégées par un pare-feu.

Autres questions à se poser

Etes-vous certain que les ordinateurs portables et PDA qui se connectent occasionnellement au système de contrôle de processus, ou les clés USB qui y sont parfois introduites, ne peuvent pas y introduire de code malveillant, au moins sans détection immédiate ? Cette cause d'infection est de plus en plus fréquente sur les réseaux bureautiques : pourquoi pas sur l'informatique industrielle ?

Etes-vous certain que les connexions temporaires du système de contrôle de processus (pour des mises au point diverses, pour des mises à jour, pour la télémaintenance…) vers l'extérieur sont surveillées quand elles sont établies et sont désactivées quand elles ne sont plus nécessaires ?

Savez-vous si tous les équipements actifs qui le supportent sont équipés d'un antivirus et s'il est tenu à jour quotidiennement ? Le cycle de parution des virus n'est pas régulier, plusieurs mises à jour des signatures peuvent intervenir dans la même semaine.

Vos procédures de mise à jour et de configuration de votre système de contrôle de processus permettent-elles de retracer l'origine des éventuels incidents ultérieurs ?

Etes-vous certain que seules des personnes autorisées se connectent aux systèmes industriels de votre entreprise ?

Savez-vous ce que deviennent les disques durs de vos systèmes lorsqu'ils sont mis au rebut ?

Pensez-vous qu'en cas de dysfonctionnement de votre informatique industrielle, qu'il soit accidentel ou dû à une malveillance, vos équipes sauraient réagir promptement et efficacement pour en limiter les conséquences néfastes ?

Par **Jean-François Pacault**,
Service du Haut Fonctionnaire de Défense et de Sécurité
au Ministère de l'industrie.

conception et l'implémentation d'une politique optimale de protection des systèmes de contrôle contre les cyber-attaques, en bénéficiant de l'effort de recherche US et des travaux de normalisation sectorielle.

Les réflexions ont démarré en 2001 et les premiers rapports techniques ont été publiés en 2004. Il existe des techniques et outils en informatique potentiellement utilisables dans les systèmes de contrôle. Le rapport recense plusieurs catégories de technologies de sécurité, discute pour chaque catégorie leurs applications industrielles, leurs points faibles en environnement de contrôle et émet des recommandations d'utilisation.

La première partie du standard ISO99 (Concepts, Terminology and Models), publiée à la fin 2007, décrit le contenu du standard, elle définit la terminologie, propose une double modélisation (physique et fonctionnelle) des systèmes de contrôle vis-à-vis de la sécurité, et introduit un concept de découpage des systèmes de contrôle en « zones de sécurité », avec identification des « conduits » d'information à protéger entre ces différentes zones.

La seconde partie (ISA99 Part. 2) comprend les champs d'application du standard, les références normatives utilisées, les termes et abréviations, en complément de la Partie 1. Mais aussi, les éléments constitutifs d'un système de gestion de la cyber-sécurité pour l'automatisation industrielle et les systèmes de contrôle. Les prescriptions pour la mise en place d'un programme de sécurité (analyse de risque et vulnérabilité, cycle de vie de la sécurité, contremesures et défense en profondeur, traitement des incidents, processus d'amélioration permanent). Cette section étant normative.

Reste à bâtir un programme de gestion de la cyber-sécurité. Pour Jean Pierre Dalzon *« il n'existe pas de recette unique en raison de la variété des contextes (système nouveau ou amélioration des systèmes existants, niveau de maturité et de diversité des technologies…et des intervenants). La réponse ne peut être que relative et s'intégrer dans la politique générale de l'entreprise. La sécurité parfaite est un idéal et une solution de compromis est à rechercher en considérant le coût du développement face au coût des conséquences des risques potentiels »*.

En conclusion, la norme SP99 décrit un objectif de « meilleure pratique possible » pour évaluer et classer les risques pour calibrer les précautions en fonction du niveau de risque et pour chaque type d'applications. Avec ces réflexions sectorielles, il constitue une synthèse de l'état de l'art en ce début de 2008.