Sécurité des systèmes informatiques industriels

3ème partie

La normalisation

Martin Naedele, Dick Oyen

La 2ème partie de notre dossier s'intéressa aux divers types de malveillance visant les systèmes d'automatisation et à leurs éventuelles parades.

Cet ultime volet passe en revue les efforts accomplis ces deux dernières années par différents organismes de normalisation en vue de créer un référentiel commun de sécurité des automatismes industriels. Leurs initiatives et le résultat de leurs travaux sont abordés, dont ceux du groupe de travail WG10 du comité d'études CE 65 de la CEI visant à instaurer une démarche de sécurisation de certains scénarii de contrôle-commande.

Qui n'est pas aujourd'hui inondé d'informations sur la sécurité informatique, relayées par moult «livres blancs» de fournisseurs d'automatismes nous expliquant l'art et la manière de verrouiller leurs systèmes? Mais dispose-t-on pour autant de guides impartiaux et accessibles sur la sécurisation systématique des systèmes d'automatisation et d'instrumentation face à une cyberattaque?

Nul doute que la normalisation profitera à la fois aux offreurs et aux utilisateurs d'automatismes soucieux:
- d'évaluer l'effort de mise en œuvre, de maintien et d'exploitation des mécanismes et procédures de sécurité;
- de définir les objectifs de sécurité pour leur site et le cahier des charges des fonctionnalités et mesures relevant des fournisseurs et intégrateurs;
- de comparer la couverture de sécurité et le coût des solutions offertes;
- de mettre en œuvre et d'exploiter des mécanismes de sécurité multisites, efficaces et rentables;
- de s'assurer que leurs parades correspondent aux meilleures pratiques de gestion du risque et de la sécurité informatique.

De même, fabricants et intégrateurs pourront:
- anticiper les exigences de sécurité et développer les fonctionnalités ad hoc;
- bâtir des architectures de sécurité réutilisables pour de multiples projets et clients afin d'abaisser les coûts de rédaction des offres et de développement, ainsi que les frais d'achat de dispositifs et d'applications de sécurité tiers.

Deux grandes initiatives de normalisation

Cette étude des travaux de normalisation sur la sécurité industrielle s'inspire des sources [1] et [2].

ISA S99

Le comité SP99[1)] de l'ISA (*Instrumentation, Systems, and Automation Society*) est à l'origine de recommandations, de guides et du standard S99 pour la mise en place d'un cycle de vie de la sécurité dans les systèmes d'automatisation du manufacturier et du process.

L'ISA est l'organisme de normalisation du contrôle-commande et de l'instrumentation aux Etats-Unis. Nombre de ses standards (S88 et S95, par exemple) font figure de meilleures pratiques et de référentiels internationaux.

Des normes sur la cybersécurité des automatismes industriels profiteront à la fois aux offreurs et aux utilisateurs.

Les travaux du SP99, débutés en 2002, ont abouti à deux premiers rapports publiés au printemps 2004. Le premier, intitulé *«Technologies de sécurité»* [3], fait le tour des techniques et mécanismes de sécurité informatique en vigueur, et de leur mise en œuvre dans l'atelier: y sont notamment abordées les questions d'authentification et d'autorisation, de filtrage/blocage/contrôle d'accès logiques, de cryptage et validation des données, d'audit, mesure, surveillance et détection, de systèmes d'exploitation et logiciels d'application, de sécurité physique. Chaque technique est étudiée sous plusieurs angles: analyse de vulnérabilité, déploiement type, connaissance des points faibles, utilisation en automatisation, orientations futures, recommandations et sources bibliographiques.

Le second, *«Intégration de la sécurité informatique dans les systèmes manufacturiers et de contrôle-commande»* [4], préconise une architecture de sécurité et décrit les aspects organisationnels, sociaux et juridiques de l'introduction de la gestion de la sécurité de l'information en milieu industriel, sur la base de la norme ISO/IEC 17799:2000 [5]. Au chapitre des recommandations figurent l'élaboration d'un programme et d'une politique de sécurité, l'analyse de risques, l'audit et le test, le développement, le choix et la réalisation de contre-mesures, ainsi que des exemples de politiques et de documentation.

Depuis l'été 2004, le SP99 travaille sur le standard S99 et ses deux points fondamentaux:
- adaptation des mécanismes de sécurité informatique aux sites industriels existants moyennant des composants banalisés, sans préconiser d'architecture précise;
- exploitation du système de gestion et des processus administratifs sous-jacents.

L'architecture et les processus de sécurité réels seront vraisemblablement adaptés aux besoins de chaque unité.

IAONA

Association d'utilisateurs et de fournisseurs de réseaux de communication industriels, l'IAONA (*Industrial Automation Open Networking Alliance*) et son groupe de travail sur la sécurité[2)] ont édité une fiche type permettant aux constructeurs de systèmes et équipements d'automatisation de docu-

tableau 1 L'état de la normalisation

CIDX (http://www.cidx.org/CyberSecurity/): organisme de normalisation des échanges de données informatiques pour la chimie (surtout actif aux Etats-Unis) éditant un guide de procédures de sécurité, dans la droite ligne des travaux de l'ISA SP99.

NAMUR (http://www.namur.de/en/694.php): organisme de normalisation surtout actif en Europe, notamment en Allemagne, éditant un guide sur l'usage sécurisé des technologies réseau dans l'industrie de process.

NERC (http://www.nerc.com/): instance régulatrice des entreprises énergétiques américaines pour lesquelles la conformité aux normes NERC 1200 et CIP 002…009 sur la gestion de la sécurité (très orientées processus et documentation) est obligatoire.

CIGRE (www.cigre.org): Comité International des Grands Réseaux Electriques dont un certain nombre de groupes de travail se consacre à la sécurité informatique.

PCSRF (http://www.isd.mel.nist.gov/projects/processcontrol/): forum sur les exigences de sécurité en contrôle de processus visant à promouvoir la certification «Sécurité» des futurs composants de système de contrôle-commande suivant l'ISO/IEC 15408 (Critères communs), sous l'égide de l'organisme de certification américain NIST.

PCSF (https://www.pcsforum.org/): forum sur les systèmes de contrôle de processus encourageant, depuis 2004, le partage d'informations à grande échelle entre les instances normalisatrices de la sécurité informatique.

menter les caractéristiques et exigences de sécurité et de communication de chacun de leurs produits : des données précieuses pour l'architecte de la sécurité des automatismes qui peut ainsi concevoir et configurer les mécanismes de sécurisation de l'installation industrielle. Cette « fiche sécurité » a l'avantage de centraliser une somme d'informations concises et pertinentes, qui serait sinon difficilement récupérable de la documentation fournisseur.

La CEI

C'est au début 2004 que le sous-comité SC 65C de la CEI spécialisé dans les communications numériques, sous la houlette de son groupe de travail WG13, s'attaque aux questions de cybersécurité auxquelles il consacre la partie 4 (*« Profils de communication sécurisés »*) de la norme CEI 61784 sur les bus de terrain et autres réseaux de contrôle-commande industriels.

Ces travaux révélèrent une évidence : impossible de régler les problèmes de sécurité rencontrés en automatisation en se contentant de protéger la communication, ni en se cantonnant au niveau terrain. Le WG13 s'attacha plutôt à spécifier des réalisations sécurisées, dans les règles de l'art, de certains scénarii courants de mise en réseau d'automatismes, comme les accès à distance par RTC. Ces descriptions ou « ensemble d'exigences » constituent à la fois un recueil de mécanismes techniques, indépendant du produit, dans le cadre d'une architecture mettant en œuvre les meilleures pratiques de sécurité, et un guide sur la configuration et l'exploitation de ces mécanismes. Cette démarche est approfondie ci-après.

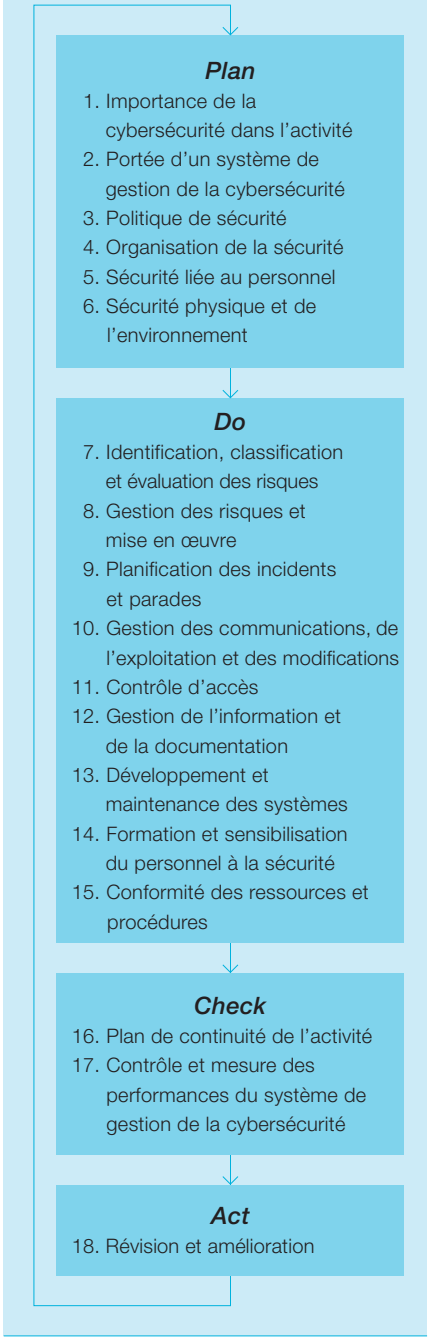
Le WG13 passa la main à un autre groupe de travail, le WG10, pour que ces recommandations et principes directeurs soient en phase avec la mission du CE 65. La norme finalisée 62443, prévue pour 2006, s'intitulera *« Sécurité pour la mesure et la commande dans les processus industriels – Sécurité des systèmes et réseaux »*, sa validation internationale devant être votée au premier semestre 2007.

D'autres approches normalisatrices sont résumées au tableau 1.

Gestion de la sécurité industrielle normalisée ISA S99

Le premier rapport technique de l'ISA SP99 [3] est un guide sur la mise en œuvre d'une gamme complète et variée de techniques et moyens de sécurité, s'appuyant sur l'expérience conjointe de spécialistes de la sécurité chez les offreurs et utilisateurs d'automatismes industriels. Cette information étant de nature analytique, il ne s'agit pas d'un document normatif auquel on peut confronter un produit et en mesurer la conformité. Il incombe au lecteur de juger de l'adéquation de l'information à son cas de figure. C'est un excellent document pour commencer à définir des mesures de sécurité, que l'on soit débutant ou initié. Le TR99.00.01 est en permanence mis à jour, mais son contenu ne sera pas repris dans les normes S99.

1 Système de gestion de la cybersécurité



Depuis octobre 2005, les projets des deux premières parties de la S99 sont à la disposition du public.

La partie 1 définit la terminologie et décrit les modèles utilisés en matière de sécurité des systèmes d'automatisation ; la partie 2 donne des conseils sur la mise en place d'un système de gestion de la cybersécurité dont les 18 points fondamentaux sont organisés selon un « cycle de vie de la sécurité », intégré autour du modèle PCDA (*Plan-Do-Check-Act*). C'est une émanation du CIDX [7] qui a adapté ces 4 phases de la norme britannique BS 7799-2:2002 [6] aux systèmes d'automatisation et en a défini les 18 étapes clés (1). La nature cyclique de la démarche est manifeste au point 18 avec la modification du programme de sécurité suivant les enseignements tirés des 17 étapes précédentes.

Définition (*Plan*)

Cette première phase échafaude la ligne stratégique de la Direction pour définir clairement une politique générale de sécurité chapeautant le programme de sécurité.

Cette organisation de la sécurité tient compte de tous les acteurs du système de contrôle-commande dont elle identifie les rôles et responsabilités en la matière.

La sécurité étant affaire d'hommes (qu'ils soient détenteurs d'actifs à protéger, gardiens de ce patrimoine ou éventuelles menaces), le volet « Personnel » définit les politiques et méthodes d'évaluation et de maintien de la fiabilité des personnes ayant largement accès à ces actifs. S'y ajoutent les aspects « Sécurité physique » et « Sécurité de l'environnement », partant du postulat qu'il existe d'importantes, mais somme toute relatives, barrières à la cyberattaque physique.

Comprendre

C'est aussi là que sont répertoriés, classés et valorisés les risques liés à la sécurité, la S99 et sa bibliographie donnant le détail de la méthode ; une évaluation qui aboutit directement à la phase suivante.

Mise en œuvre (*Do*)

L'analyse des risques permet d'appliquer des parades efficaces à la réalité des vulnérabilités.

Des procédures sont établies pour contrecarrer d'éventuels incidents ; cette planification de la riposte doit notamment préciser le moment où il convient d'alerter les autorités des lourdes menaces pesant sur la collectivité.

Des politiques et procédures de gestion globales sont définies pour prendre en compte les communications, l'exploitation des systèmes et la gestion des modifications.

Le point 11, *Contrôle d'accès*, stipule les droits de chacun en fonction de sa mission, mais aussi les procédures limitant l'accès logique des personnes aux activités et informations de leur ressort. Sont ainsi définis des moyens d'authentification pour garantir qu'un utilisateur donné (humain ou logiciel) est bien habilité à accéder à l'information.

Le point 12, *Gestion de l'information et de la documentation*, identifie le classement «sécurité» des données et en précise les protections. Les problèmes de sécurité de développement et de maintenance du système font aussi l'objet de politiques et de procédures.

Le personnel doit être formé aux procédures correspondantes, chacun de ses membres étant régulièrement sensibilisé et rôdé aux précautions de sécurité générales. Il faut constamment veiller au respect des politiques et procédures de sécurité par les services et effectifs de l'entreprise, ces dernières étant périodiquement auditées. A cette conformité s'ajoute la prise en compte d'exigences «externes» que constituent les clients et partenaires de l'organisme, ainsi que les instances régulatrices.

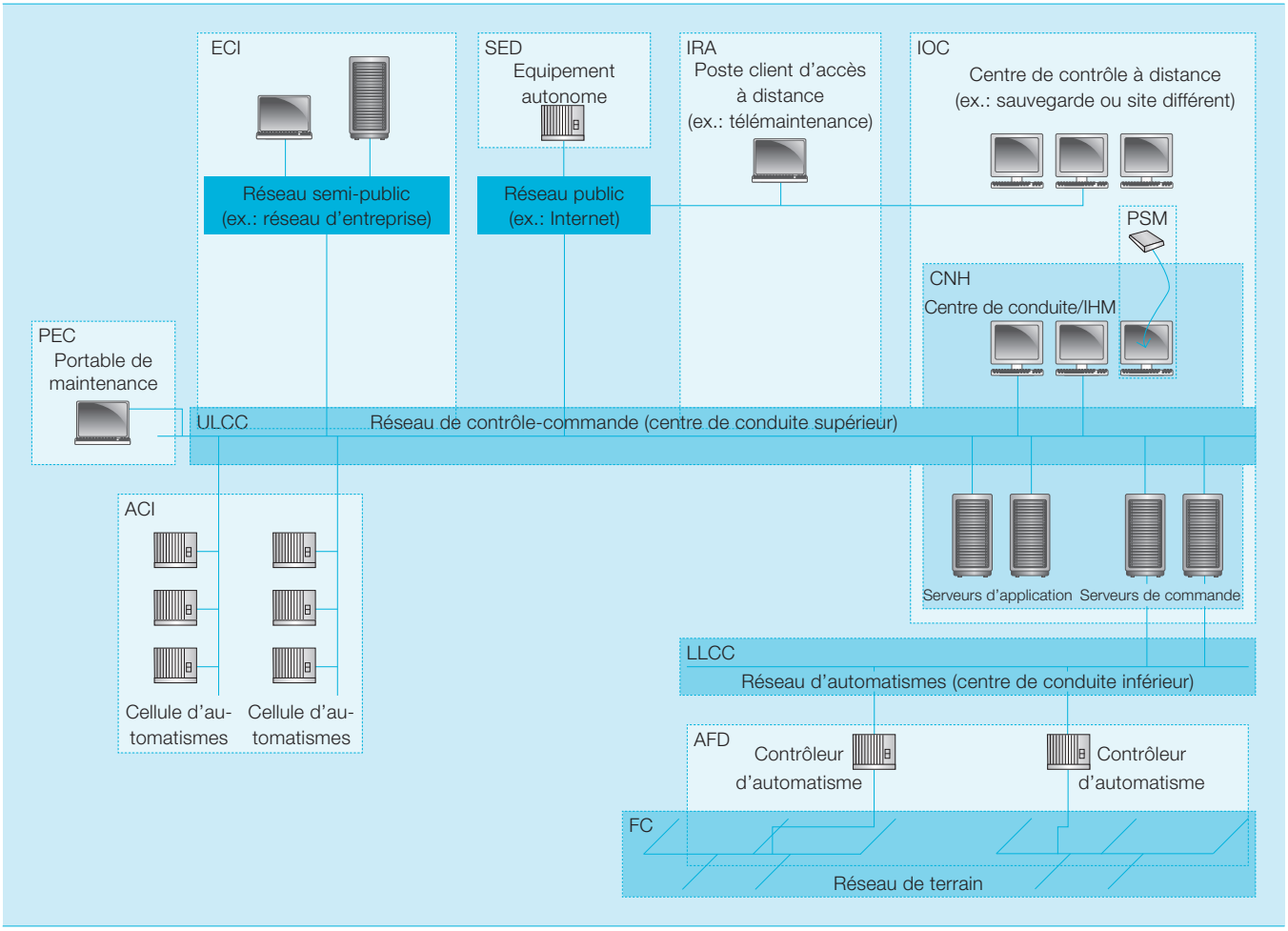
Evaluation et mesure (*Check*)

Cette phase prévoit l'établissement et le suivi d'un plan de continuité de l'activité précisant la capacité de l'organisme à répondre rapidement aux interruptions de ses fonctions critiques résultant de pannes, d'incidents, de sinistres ou de catastrophes. C'est aussi l'occasion de mesurer les performances du système de gestion de la cybersécurité par rapport aux objectifs et expériences pratiques.

Révision et amélioration (*Act*)

Cyclique, le programme de sécurité est révisé en fonction des résultats de la phase précédente.

2 Architecture de sécurité modulaire : chaque module est adaptable à certains constituants du système d'automatisation et de son réseau.



La partie 2 de la S99, plus détaillée, instaure un système de gestion de la cybersécurité en 19 points ; la partie 3 explique comment l'exploiter.

Architecture de sécurité normalisée CEI 62443

La CEI 62443 porte principalement, au niveau système, sur les aspects techniques de l'architecture de sécurité, complétant à ce titre les initiatives orientées produits (IAONA) et processus (SP99 et NERC).

Grâce aux efforts continus de normalisation des processus et architectures de sécurité informatique pour les systèmes industriels, les responsables de production disposent d'outils modernes, efficaces et rentables pour sécuriser leur système d'information.

La démarche de la CEI se fonde sur une architecture de sécurité *modulaire* dans laquelle chaque module correspond à un scénario donné d'exploitation ou de communication, est applicable à certains constituants du système d'automatisation et de son réseau 2, et est représenté par un ensemble d'exigences spécifiées dans la norme. Quelques-unes de ces exigences, de même que les constituants physiques et logiques afférents, sont communes à de multiples modules. Ces derniers peuvent et doivent se combiner pour répondre à un usage et à une menace spécifiques du système d'automatisation. La norme indique les modules prioritaires lorsque son respect global est impossible en raison des contraintes budgétaires pesant sur la mise en place et la maintenance du projet.

Ces exigences seront formulées de façon à servir de base aux appels d'offres et offres, ainsi qu'aux audits sécurité, tout en autorisant différentes solutions techniques. L'un des buts recherchés est la possibilité de satisfaire aux exigences de la norme avec des produits et technologies du commerce. De même, ces exigences sont à la fois applicables à l'existant et révisables «à la baisse» pour les systèmes qui, après analyse, font courir peu de risques à l'entreprise et à la collectivité.

Dans cette optique, les modules suivants sont envisagés :

Interconnexion réseau de contrôle-commande -> réseau d'entreprise (ECI) : définit l'architecture de sécurité des flux de données, autres que temps réel et de préférence unidirectionnels, entre un réseau de contrôle-commande et un réseau d'entreprise.

Accès à distance interactif (IRA) : précise l'architecture de sécurité nécessaire pour accéder à distance à des segments du système de contrôle-commande (par RTC ou Internet), à des fins de télémaintenance ou de télédiagnostic.

Interconnexion des centres de conduite (ICC) : explique comment sécuriser les communications entre centres de conduite fixes sur réseaux publics.

Equipement embarqué autonome (SED) : énonce les exigences de sécurité d'un automatisme situé hors zone sécurisée, pour lequel un périmètre de sécurité complet ne serait pas rentable (dispositif électronique intelligent monté sur poteau, par exemple).

Ordinateurs portables industriels (PEC) : définit les protections d'un système de contrôle-commande pour contrer les menaces liées à l'itinérance des ordinateurs portables entre réseaux publics et système de contrôle-commande.

Mémoires de masse amovibles (PSM) : explique les méthodes de protection d'un système d'automatisation contre les risques d'infections informatiques par des moyens de sauvegarde de type clés ou cédéroms.

Interconnexion de cellules d'automatismes (ACI) : décrit l'architecture de sécurité nécessaire à l'établissement d'une communication protégée entre cellules d'automatismes du réseau de contrôle-commande.

Centre de conduite supérieur (ULCC) : énonce les mécanismes de sécurité du segment de réseau de contrôle-commande relié aux postes de conduite, logiciels d'historisation, serveurs d'application et serveurs de connectivité.

Centre de conduite inférieur (LLCC) : énonce les mécanismes de sécurité du segment de réseau de contrôle-commande relié aux contrôleurs d'automatisme.

Conduite du terrain (FC) : énonce les mécanismes de sécurité du segment de réseau de contrôle-commande relié aux équipements de terrain.

Conduite du réseau de contrôle-commande (CNH) : explique les modes de sécurisation des postes et serveurs de conduite et de développement des automatismes contre les attaques de l'intérieur et les malveillances informatiques, par exemple.

Equipements de terrain (AFD) : explique les modes de sécurisation des appareils de terrain et contrôleurs embarqués.

Chaque module décrit le cas d'emploi auquel il s'applique, les menaces contrées ou non, les hypothèses sous-jacentes, les exigences et le responsable (fournisseur d'automatismes, intégrateur système, exploitant du site) du respect de chacune de ces 20 à 50 exigences, selon le module.

Chaque exigence se compose d'une référence normative, éventuellement revue à la baisse, d'une justification et, dans bien des cas, d'une ou de plusieurs notes applicatives. La justification est essentielle dans la mesure où elle permet au lecteur de décider en toute connaissance de cause de l'importance et de la pertinence de l'exigence. Les notes applicatives, quant à elles, renseignent sur la réalisation de cette exigence.

La CEI 62443 donne les tenants et aboutissants de l'architecture de sécurité, sans toutefois expliquer comment procéder ; cette question étant spécifique à chaque site et système, elle est laissée à l'appréciation technique des experts de l'installation et de l'intégrateur du système d'automatisation et des technologies de l'information.

Bilan

Grâce aux efforts continus de normalisation des processus et architectures

Notes

1) http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

2) http://www.iaona.org/home/jtwg-se.php

Comprendre

de sécurité informatique pour les systèmes de contrôle-commande et d'automatisation industriels, les responsables de production disposent aujourd'hui d'outils modernes, efficaces et rentables pour sécuriser leur système d'information.

Les initiatives de normalisation décrites dans cet article reconnaissent toutes le besoin de pragmatisme des solutions industrielles et la nécessité d'une collaboration résolument constructive entre fournisseurs et utilisateurs d'automatisme.

ABB y contribue amplement en dotant sa clientèle de produits et solutions normalisés, et en l'aidant à mettre en œuvre cet arsenal normatif en sites industriels.

Martin Naedele
ABB Switzerland, Corporate Research
martin.naedele@ch.abb.com

Dick Oyen
ABB US, Corporate Research
dick.oyen@us.abb.com

Bibliographie

[1] Naedele, M.: Standardizing Industrial IT Security – A First Look at the IEC approach, 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 05), Catania, September 2005

[2] Dzung, D., Naedele, M., von Hoff, T., Crevatin, M.: Security for industrial communication systems, Proceedings of the IEEE, Vol. 93 (6), June 2005, pp 1152–1177

[3] ISA SP99: Security Technologies for Manufacturing and Control Systems, Instrumentation, Systems, and Automation Society, ISA-TR99.00.01-2004, March 2004

[4] ISA SP99: Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems, and Automation Society, ISA-TR99.00.02-2004, April 2004

[5] Technologie de l'information – Code de pratique pour la gestion de la sécurité de l'information, ISO/IEC 17799:2000, décembre 2000

[6] British Standards Organization: Information security management systems – Specification with guidance for use, BS 7799-2:2002, September 2002

[7] Chemical Industry Data Exchange (CiDX): Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.0, December 2004.

INDEX 2005

1/2005
Esprits pionniers

3/2005
Développement durable

2/2005
Collaboration université-industrie

4/2005
L'innovation, notre A.D.N.