



## LES COUPE-FEU DANS LES APPLICATIONS INDUSTRIELLES

# Tenez les visiteurs indésirables à distance

Ing. Xavier De Buyscher, Control & Automation Magazine

Ethernet s'est échappé du bureau et constitue aujourd'hui une alternative à part entière pour la commande machine dans l'environnement industriel et IP67. Outre les nombreux avantages que cela représente, il y a aussi certains risques. Rappelons-nous la conduite de gaz de Gazprom gérée pendant plus de dix heures par des pirates. La protection du réseau est une nécessité absolue!

Le sept février dernier, l'événement High Tech Equipment Engineering s'est déroulé à Eindhoven en collaboration avec les constructeurs de machines et les membres du secteur néerlandais de l'automatisation industrielle. Ce jour-là, les constructeurs de machines et leurs fournisseurs ont discuté du thème 'modulaire ou intégré'. Outre les différents programmes-conférences, plusieurs discussions ont eu lieu à la Chambre des communes. Chacun pouvait y discuter avec les personnes présentes. Une des sessions dirigées par Fred Weggelaar de Hirschmann Automation and Control, traitait de la communication dans la construction de machines modulaire et en particulier de la sécurité du réseau.

La communication dans la construction de machines modulaire connaît plusieurs niveaux: les protocoles propriétaires pour les commandes déterministes, ou la large autoroute des données pour la communication globale. Ethernet s'est échappé du bureau et constitue aujourd'hui une alternative à part entière pour la commande machine dans l'environnement industriel et IP67. On y retrouve divers protocoles qui recourent souvent à un équipement réseau existant.

### Ethernet quitte le bureau

Contrairement aux périodes difficiles qu'a connues le marché de l'automatisation classique ces dernières années, le marché des modules Ethernet industriels a connu une croissance remarquable. L'ARC Advisory Group prévoit dans les prochaines années une croissance annuelle mondiale de 51,4% pour l'Ethernet industriel. Le marché représentait un total de 840.000 unités en 2004 et devrait passer à 6,7 millions d'unités en 2009. Cette étude de marché comprend aussi le marché des commutateurs Ethernet industriels qui représentait un chiffre d'affaires mondial de 124,4 millions de dollars en 2004 et qui augmentera de 49,9% en 2009 pour atteindre un chiffre d'affaires de 939,8 millions de dollars. Ethernet confère aux utilisateurs un réseau industriel dont le coût de gestion est inférieur et qui offre une flexibilité accrue pour s'adapter aux besoins changeants

du business. Sa large diffusion et le caractère familier du marché contribuent à l'augmentation du nombre d'applications Ethernet dans les automatisations industrielles d'un grand nombre de secteurs industriels. L'utilisation de cette technologie prête à l'emploi permet d'appliquer plus aisément Ethernet dans les projets pilotes, les extensions système, les développements d'applications et les nouveaux systèmes d'automatisation. La technologie comprend une variété de produits parmi lesquels des commutateurs, des coupe-feu, des outils de gestion de réseau, des outils de développement et des standards de messagerie.

### Environnement industriel

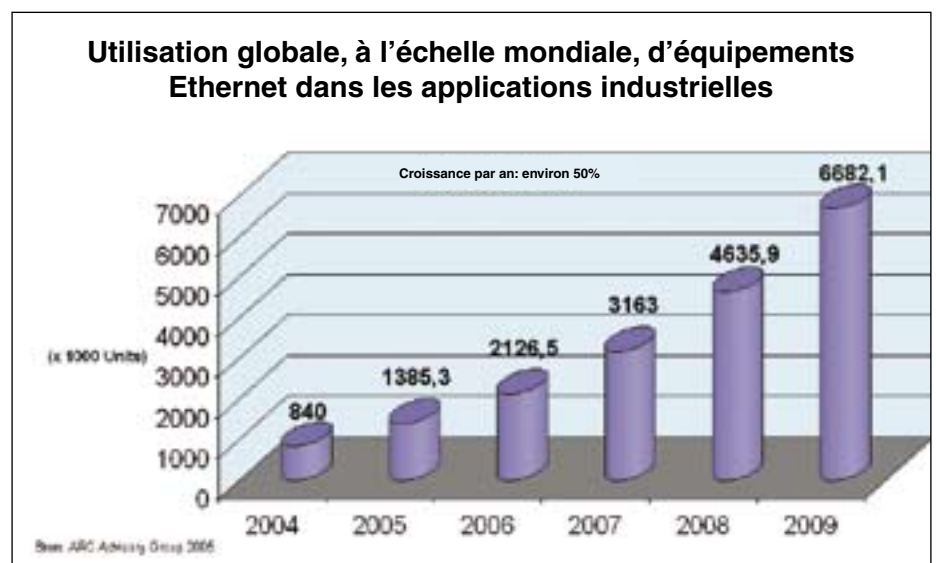
Alors que certains démarrent avec un commutateur bon marché en provenance du monde de la bureautique, acheté dans le magasin informatique du coin, ils apprendront bien vite l'intérêt de la fiabilité et de la protection dans un envi-



Ethernet s'est échappé du bureau et constitue aujourd'hui une alternative à part entière pour la commande machine dans l'environnement industriel et IP67. On y retrouve divers protocoles qui recourent souvent à un équipement réseau existant.

ronnement industriel. Une petite visite au plant manager pour s'entendre dire qu'un commutateur 'du monde bureautique' à vingt euros a mis l'usine à l'arrêt pendant un certain temps, vous apprendra très vite qu'il vaut mieux recourir à du matériel industriel. La protection contre l'environnement industriel intègre les problématiques de chaleur, de vibrations, d'EMC et de poussière ainsi que d'autres facteurs. Les modules Ethernet industriels sont réalisés de série avec des degrés de protection IP20 et IP40. On constate même un glissement vers l'IP67 et l'IP68, au fur et à mesure que l'on avance sur le terrain et que l'on

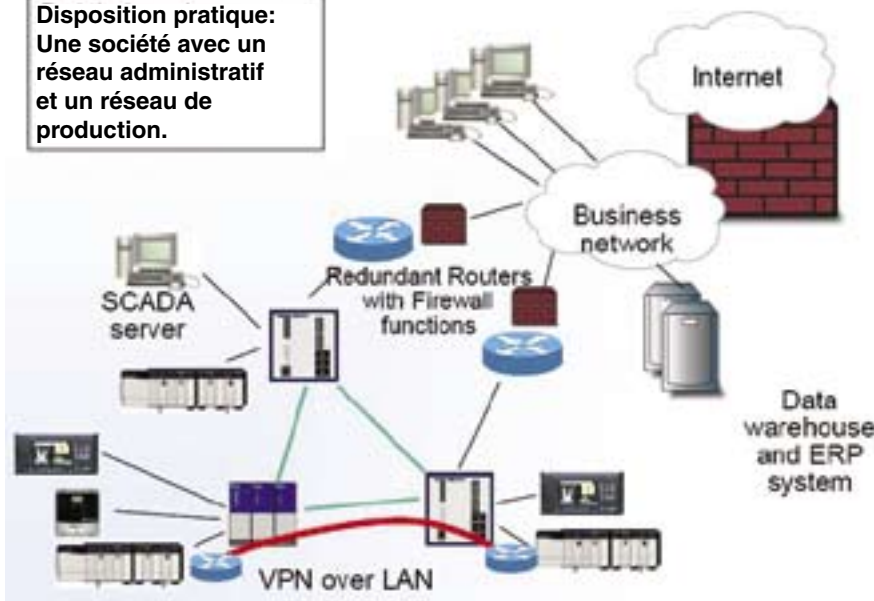
### Utilisation globale, à l'échelle mondiale, d'équipements Ethernet dans les applications industrielles



L'ARC Advisory Group prévoit dans les prochaines années une croissance annuelle mondiale de 51,4% pour l'Ethernet industriel. Le marché représentait un total de 840.000 unités en 2004 et devrait passer à 6,7 millions d'unités en 2009.



**Disposition pratique:  
Une société avec un  
réseau administratif  
et un réseau de  
production.**



*Au fur et à mesure qu'augmentent les liens entre les réseaux d'usine et les réseaux de bureau, les risques d'arrêt de ces réseaux augmentent aussi. La prise de conscience du problème doit conduire à la prise de mesures adéquates, comme l'application d'une protection appropriée.*

implémente davantage d'applications dans des environnements de processus. Cependant, outre la protection physique, il faut aussi prendre les mesures de sécurité nécessaires en matière de protection des données et de visiteurs indésirables.

## Des situations vécues

Il y a quelques années, des pirates ont été en mesure d'accéder au réseau de Gazprom. Pendant une douzaine d'heures, ils ont été les 'maîtres' d'une conduite de transport de gaz. En Australie, un employé licencié s'est vengé en 'piratant' le réseau de son employeur pour ensuite faire couler des eaux d'égout, notamment au rez-de-chaussée d'un hôtel. Un gestionnaire de réseau d'une société d'aliments pour bétail a nettoyé, un vendredi midi, des adresses étrangères des tables d'un routeur. Il ne savait pas que le personnel de production venait d'introduire ces adresses. La production a été à l'arrêt pendant un shift complet. En 1998, le NIST (National Institute of Standards and Technology) a catégorisé et analysé des attaques informatiques publiées sur Internet (choisies parmi une offre de quelque 400 attaques). 29% de celles-ci concernaient un hôte Windows, 20% concernaient des composants de réseau (routeurs, commutateurs, coupe-feu), 3% des manipulations de sites web, 4% des scans de réseau à la recherche d'hôtes fragiles.

## Quatre règles de base

La réalisation d'un réseau protégé requiert une approche par étapes. Il faut tout d'abord établir une stratégie ou ligne de conduite. Il est primordial d'impliquer le management et d'intégrer ce point dans un système de qualité. Ensuite, il faut définir l'architecture du réseau. Sur le plan

physique, il faut déterminer qui peut entrer dans l'espace serveur et sur le plan technique, il faut déterminer les séparations, les sous-réseaux ou les VLAN. Tertio, il faut organiser de bonnes sessions d'information pour tous les collaborateurs. Durant celles-ci, vous les informez des dangers et vous leur expliquez les règles relatives à l'utilisation de CD et de cartes mémoires, aux PC de visiteurs, au comportement sur Internet... Finalement, il faut exercer un contrôle. La confiance c'est bien, mais le contrôle c'est mieux, tant que vous expliquez aux collaborateurs la raison d'être de ce contrôle.

## Quel est le degré de sécurité de notre réseau?

Le bâtiment est entouré d'une clôture avec une porte et un contrôle d'accès! Par contre, quel est le degré de sécurité de notre réseau bureautique, de notre réseau de commande de processus, des accès à distance, d'Internet et de la connexion VPN? Le plus sûr serait naturellement de ne rien relier ou de relier un minimum en ne connectant l'équipement que lorsque cela s'avère nécessaire. Cependant, ceci n'est pas vraiment l'objectif car quid alors des diagnostics à distance et comment les constructeurs et intégrateurs systèmes peuvent-ils se connecter dans ce cas? On peut alors choisir d'établir la connexion la plus sûre à l'aide d'un coupe-feu ou d'utiliser les connexions d'accès à distance les plus sûres possibles, par exemple avec un modem de retour d'appel ou une connexion VPN. Une règle s'impose toutefois: ne jamais relier directement un réseau de production à Internet. Utilisez au moins un coupe-feu et de préférence en passant via le réseau bureautique. Outre l'aspect technique, il faut aussi définir de bons accords et règles organisationnels. Une

bonne concertation entre la production et l'IT est fondamentale. Gardez la communication essentielle au sein d'une partie du réseau sous la responsabilité d'une seule personne. Qui est responsable du réseau de production? Posez-vous la question: si la technique n'était pas Ethernet, qui serait-ce? Si l'IT est responsable de tous les composants réseau et PC, est-elle également responsable des PLC?

## Coupe-feu

Selon le spécialiste des réseaux industriels Fred Weggelaar de Hirschmann, la 'prise de conscience et la prévention' sont les clés de la protection des réseaux informatiques, ce qui est de plus en plus vrai aussi dans l'industrie. «Au fur et à mesure qu'augmentent les liens entre les réseaux d'usine et les réseaux de bureau, les risques d'arrêt de ces réseaux augmentent aussi. La prise de conscience du problème doit conduire à la prise de mesures adéquates, comme l'application d'une protection appropriée « remarque-t-il. L'intégration des deux réseaux est selon lui parfaitement logique. Au bureau, le management souhaite profiter de la meilleure vue possible sur la qualité et la quantité de production, les besoins de maintenance des machines... On travaille de plus en plus à partir du réseau d'usine dans un environnement Web, ce qui rend les programmes de navigateur web actifs. L'intégration de plus en plus grande des deux réseaux est totalement liée aux exigences d'efficacité et de transparence. Ceci s'appelle aussi l'intégration verticale. Pensez à l'impression des données du produit dans le processus de production, qui est pilotée à partir du réseau bureautique.

## Des murs et des tunnels

Chez Hirschmann, le matériel nécessaire pour protéger la communication entre le réseau de bureau et le réseau d'usine porte le nom d'Eagle. Outre un coupe-feu, Eagle dispose aussi d'un scanner de virus intégré et d'un serveur VPN (Virtual Private Network). Ce dernier constitue pour ainsi dire un tunnel via lequel le trafic bureautique peut être guidé en toute sécurité à travers l'usine. Eagle protège le réseau de production des influences indésirables (conscientes ou inconscientes), comme les virus et les diffusions générales, provenant du réseau bureautique. En outre, Eagle rend quasiment impossible tout 'piratage' par des étrangers des données échangées. Dans la pratique, Hirschmann peut aujourd'hui se targuer d'une expérience de deux ans avec Eagle. Ce temps a surtout été consacré à accroître la prise de conscience auprès des entreprises quant à la nécessité d'une protection. Les coûts liés à la recherche des causes de pannes dans un réseau de production surclassent en effet largement les frais d'implémentation d'Eagle. <<

 Vous pouvez télécharger cet article sur [www.engineeringnet.be](http://www.engineeringnet.be)