Chapitre 4
Les protocoles utilisés et leurs faiblesses

1. Introduction

Dans le milieu industriel, les hommes ont toujours cherché à automatiser les tâches à réaliser. Les premiers systèmes automatisés remontent à l'Antiquité, mais ce n'est que pendant la révolution industrielle au XIX^{e} siècle que l'automatisme s'imposa partout dans l'industrie. Les premiers automates ne communiquaient pas entre eux et étaient cantonnés à la réalisation d'une tâche précise sur une machine. Puis l'arrivée de la production en chaîne, principalement dans le milieu de l'automobile, a fait apparaître le besoin de synchroniser les tâches de production et la mise en place d'une surveillance du processus de fabrication. Il fallait donc que les systèmes automatisés puissent communiquer les uns avec les autres. Il fallait aussi que l'on puisse surveiller les étapes de fabrication, et donc avoir des tableaux de bord pour piloter la production.

À l'heure actuelle, quand on parle de communication, on entend beaucoup parler de réseau, et tout particulièrement du réseau Internet. Au bureau, à la maison, vous disposez d'ordinateurs, d'imprimantes, de tablettes interconnectés en réseau. La communication s'établit pratiquement uniquement à l'aide du réseau de type Ethernet et/ou Wi-Fi, qui n'est qu'une couche physique supplémentaire. De même, l'Internet est régi par des protocoles particuliers mettant en œuvre des processus de routage comme EIGRP (*Enhanced Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*), etc.

La nécessité de communication entre les machines industrielles est apparue bien avant l'avènement d'Internet. D'autres réseaux de communication ont donc été mis en place bien avant les réseaux que vous connaissez actuellement. L'histoire de l'évolution de l'automatisation a laissé des traces. Si les réseaux industriels se dirigent actuellement progressivement vers des méthodes de communication se rapprochant des techniques utilisées dans les réseaux informatiques, il n'en demeure pas moins que des contraintes particulières existent dans le milieu industriel :

– milieu perturbé électriquement principalement par les ondes électromagnétiques émises par les moteurs, les transformateurs, etc. ;
– milieu perturbé mécaniquement : vibration, poussières, etc. ;
– parfois nécessité d'une réponse en temps réel ;
– interconnexion avec des matériels de technologies différentes ;
– etc.

Vous allez voir dans ce chapitre les protocoles mis en œuvre dans le milieu industriel, leurs évolutions et les risques qui sont apparus par la mise en réseau à grande échelle, particulièrement par l'interconnexion avec des réseaux de type Ethernet/Internet. En effet, il est très tentant de pouvoir piloter un système industriel depuis l'autre bout de la planète, par exemple dans des pays sensibles, et parfois la connexion entre le réseau industriel et l'Internet est faite sans penser à la sécurité !

2. L'évolution des communications entre les matériels dans l'industrie

2.1 Problématique de l'évolution des matériels et de la sécurité

L'évolution des API (automate programmable industriel) est un enjeu majeur dans le secteur industriel. La progression des technologies est très rapide dans ce domaine, ce qui, par ailleurs, n'est pas sans poser problème pour la maintenance des parcs d'API. En effet, les automates sont souvent très robustes. Lors de l'installation du système de production, ceux-ci se retrouvent dans une armoire que l'on n'ouvre plus « tant que ça marche ». Cette situation est plus répandue pour les petites entreprises que pour les gros groupes, encore que... Mais que se passe-t-il en cas de panne ? Les pièces sont-elles toujours disponibles ? L'automate est-il toujours fabriqué ? Ces problématiques entraînent des arrêts de production qu'il faut absolument limiter dans le temps pour la survie de l'entreprise. La conséquence est que le problème est traité dans l'urgence et nécessite souvent une migration vers une technologie plus récente. C'est là que la reprise de production prime tellement que les notions de sécurité sont totalement omises. Attention, il faut préciser qu'il s'agit ici de sécurité au sens accès au système automatisé ; la sécurité des matériels et surtout des personnels étant régie par la loi, elle est rarement négligée.

Dans le cas d'une entreprise qui a pris conscience qu'il était nécessaire de faire évoluer son parc d'automates, il sera de toute façon impossible de tout changer en une fois. Il faudra en outre convaincre sa hiérarchie du bien-fondé de cette évolution. Là encore, c'est le gain de production engendré par la mise en service de nouveaux matériels qui va primer. La migration va donc se faire progressivement, avec un minimum d'arrêt de production. Des technologies différentes vont alors devoir cohabiter. Cet état peut là encore conduire à des problèmes de sécurité. Si par exemple une entreprise décide de mettre en place un système d'indicateurs de production accessible depuis son réseau intranet, comment chaque automate va communiquer avec ce réseau ? Une fois mis en place, il est alors intéressant de modifier ce système d'indicateurs, pour pouvoir piloter la production. Et d'un système initialement conçu pour donner des informations, on passe à un système envoyant des ordres aux automates !

Il faut que les entreprises pensent sécurité du système à chaque étape, mais ce n'est pas dans leur culture, car les réseaux industriels étaient au départ isolés de tout, et il n'y avait donc pas de risque de prise de contrôle à distance. Les entreprises pensent fréquemment production et fonctionnalité, pas sécurité.

Vous venez de voir que les réseaux d'automates remontent progressivement vers les réseaux informatiques, mais les automaticiens et les informaticiens ne parlent pas toujours le même langage. La frontière entre les droits des uns et des autres sur le réseau de l'entreprise devient floue. L'automaticien veut voir son automate sur l'intranet, mais il veut aussi accéder à la partie administrative de l'entreprise. L'informaticien lui explique qu'il faut séparer les choses pour des raisons de sécurité. Mais l'automaticien rétorque qu'il lui faut aussi un accès à Internet, car la mise à jour de son automate se fait à présent par téléchargement directement chez le constructeur et que cela peut avoir des conséquences sur la production. Ce dialogue de sourds conduit souvent à des situations de conflit, et c'est souvent la production qui prime sur la sécurité. L'effet est que l'on finit par bouger les frontières en termes de sécurité. Parfois même, il n'y a pas du tout de concertation. Combien d'automaticiens ou de responsables de production n'ouvrent-ils pas une porte vers l'extérieur afin d'avoir un regard sur leur système de production ? Ceci est parfois fait sans en informer la direction du système d'information, quand il y en a une. Et l'entreprise se retrouve dans une situation où une liaison est établie entre son réseau intranet et l'Internet !

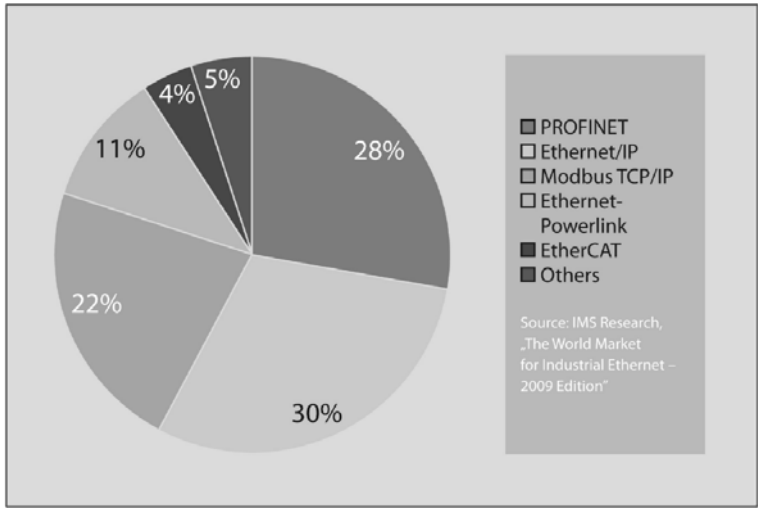
Il arrive que le danger vienne d'un manque de connaissances ou de prise de conscience. L'automaticien remplace un automate sur la chaîne de production, et le commercial lui vante les avantages de ce nouveau petit bijou. Plus besoin de descendre dans l'atelier avec une console pour reprogrammer l'automate, tout cela peut se faire depuis un bureau à l'aide d'une interface web. Comment ne pas être séduit ? Et l'automate se retrouve sur le réseau informatique de l'entreprise. Bien entendu, cet accès peut être protégé par un mot de passe, mais comme cela complique les choses, c'est rarement un argument du vendeur. De plus, si vous avez 60 automates sur une chaîne de production, difficile d'avoir un mot de passe par automate. C'est donc généralement toujours le même. Là, deux situations sont possibles : soit le mot de passe est simple et tout le monde pourra le trouver facilement, soit il est compliqué et vous le retrouvez sur des post-its collés sur les écrans des ordinateurs.

Dans tous les cas, une personne mal intentionnée de l'entreprise peut mettre en péril le système de production. Or, il est démontré qu'un grand nombre d'attaques contre les entreprises viennent de l'intérieur.

2.2 Évolution des communications et des interfaces de programmation

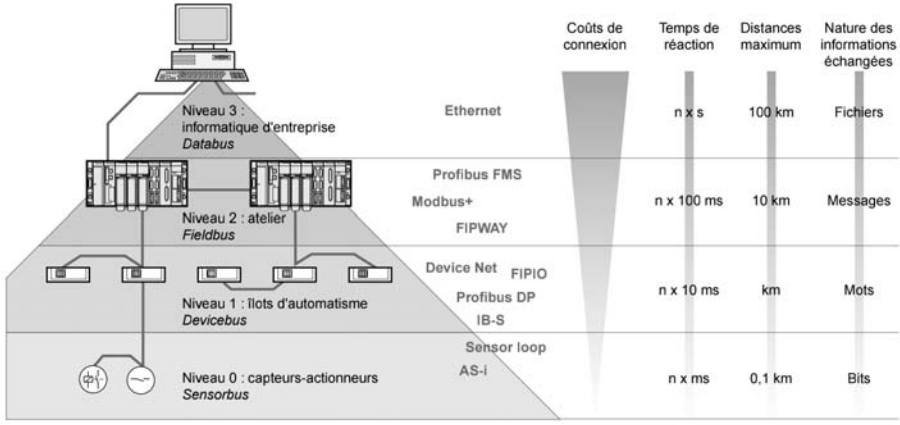
L'évolution des communications avec les automates va de pair avec les mécanismes mis en jeu pour leur programmation. Si nous prenons par exemple un bon vieux TSX17 de chez Schneider, pas grand risque de prise de contrôle à distance. Celui-ci se programme en effet à l'aide d'une console directement connectée à l'automate. Il faut donc un accès physique à celui-ci. De plus, le langage de programmation est spécifique : du PLC7. Par contre, dans le cas d'un S7-200 de chez Siemens, même s'il existe des protocoles propriétaires comme PROFIBUS, un module permettant une communication Ethernet est proposé.

Les industries comme Siemens, Schneider, etc. font évoluer leurs automates pour qu'ils puissent communiquer de plus en plus via le réseau Ethernet de l'entreprise. En 2009, IMS Research publie une statistique sur les types de réseaux de terrain les plus utilisés dans l'industrie :



Vous voyez ici clairement la domination du réseau Ethernet avec plusieurs protocoles présents sur celui-ci. Cette progression d'Ethernet n'a cessé d'évoluer jusqu'à nos jours et Ethernet devient progressivement un protocole incontournable.

Attention néanmoins, toutes les communications dans un système automatisé ne peuvent pas être en Ethernet, il y a des contraintes liées au milieu industriel qui font que beaucoup de protocoles et de modes de communication existent. D'autre part, un système automatisé est découpé en couches suivant le niveau de l'information, le traitement qui en est fait et le pouvoir de décision de l'organe sur le système automatisé. Voici un exemple de représentation de la hiérarchisation d'un système automatisé. Cette organisation est appelée pyramide CIM (*Computer Integrated Manufacturing*) et a été développée dans les années 1980 pour appréhender la position de l'information dans les systèmes automatisés.



Vous constatez que le temps de réponse du système est un élément majeur et qu'il faut mettre en place le bon réseau de terrain à chaque niveau de la pyramide pour répondre à cette contrainte.

Les niveaux 0, 1 et 2 sont utilisés par les systèmes automatisés.

Les niveaux 3 et 4 se trouvent au niveau du système d'information et de communication de l'entreprise. Le niveau 4, qui représente la gestion globale de l'entreprise, n'est pas représenté ici.