République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche Scientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTROTECHNIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Option : **Electrotechnique industrielle**

Présenté par
Smail HEMADI

Younes HATEM

Thème

Etude d'un système de télémaintenance Solution TeamViewer

Mémoire soutenu publiquement le 10/07/ 2018 devant le jury composé de :

M. Salah HADDAD
Professeur, UMMTO, Président

M. Ahmed NAHI
MAA, UMMTO, Encadreur

M. Lhacene ARAB
MAA, UMMTO, Examinateur

M. Arezki FEKIK
Docteur, UMMTO, Examinateur

M. Remdane AMMOUR
Ingénieure, Co-Encadreur, gérant de l'EASM IDUSTRIEL

La politique des gouvernements impose le développement et la collaboration entre les entreprises industrielles, cette alliance tire parti de la révolution industrielle. Cella permettra aux entreprises d'accroitre leur compétitivité en repensant leurs modèles d'affaire et en se repositionnant sur le marché grâce à l'innovation. De ce fait, les industriels ont de plus en plus recours à l'automatisation afin d'accélérer leurs processus industriels et à la communication afin de relier leurs réseaux. La grande majorité des interconnexions utilise des équipements et des réseaux acquis auprès de fournisseurs différents, ce qui explique la diversité du choix.

De nos jours il est impossible de réaliser une installation de production sans le contrôle par l'outil informatique qui permet la flexibilité, la souplesse d'utilisation et le déploiement facile et rapide sans câbles. Cette opportunité informatique offre aussi aux entreprises le privilège de télé-maintenir leurs installations : Au lieu de faire venir sur place une personne aux compétences rares et de payer des frais de déplacement (trajet aller et retour, hébergement), il est plus économique de la laisser sur son lieu habituel de travail et de l'autoriser, grâce aux réseaux existants et aux logiciels de prise de contrôle à distance, à effectuer les mêmes opérations qu'elle serait amenée à réaliser si elle se trouvait sur le site de l'entreprise.

Les protocoles TCP et IP dominent les réseaux de télécommunications contemporains. Ils ont été conçus pour répondre à ces objectifs d'harmonisation des échanges d'informations entre systèmes différents. C'est dans ce contexte qu'a émergé le standard IEEE 802.11 pour les réseaux locaux sans fils.

Remerciements

Avant toute chose, nous remercions Dieu de nous avoir donné la force physique et morale pour accomplir ce travail.

Nos remerciements s'adressent en tout premier lieu à notre promoteur Monsieur *NAHI Ahmed* pour le formidable encadrement qu'il nous a accordé tout au long de ce travail. Nous avons grandement apprécié ces conseils judicieux, sa sagesse et son orientation bénéfique, ainsi que pour sa constante disponibilité,

mais aussi pour son soutien psychologique et ses encouragements.

Nous tenons également à remercier spécialement Mr *FEKIK Arezki* d'avoir partagé ses compétences avancées avec nous au sein du laboratoire LATAGE.

Nos vifs remerciements vont aussi à Mr *AMMOUR Remdane* Co-promoteur et gérant de L'EASM industriel nous avoir ouvert ses portes afin de réaliser ce que la formation universitaire nous a fait rater.

Nos remerciements s'adressent aussi à Mr *CHALAL Samir* surnommé Akli qui nous a aidés par son expérience professionnelle.

Nos remerciements vont également aux membres du jury pour l'honneur qu'ils nous font en acceptant la charge de juger ce travail.

Je dédie ce modeste travail :

Á Vava NAGH Azizen et à Yemma NAGH Ghelayen

Á mon petit frère rebelle **Aghilas.**

Á notre cadet **Nassim**

Á l'unique Wetma Tamectuht **Litticia**

Á mon cousin espoir **Momoh**

Á Vava amuqran et Yemma Tameqrant

Á mes amis frères : Hamid SOLO, Sofiane OKLM, Wally ihedadhen, Hcen ihachouren, Jigo l'architecte n Cosider, Belaid l'écrasé, Momoh Tmizar, Nacer Dumber, Remdhane pharmacien, l'équipe B27, B01, C30, les résidants ex habitat, mon bînome Fellaini, Idir selvatory. Walid delci, Ami Said , Nassim Medjedoub, Imoune Lamine, kechemi Abed NOUR, mon frère Lyes Hatem.

Á mes amies sœurs : Nadia Abbas, Dyhia imine, Nora Iwadhiyen, Djidji, Karima Fareb, Hrouze Samira, Ghenima Kana.

Dédicace Spéciale *: ma louve R.S*

Hemadi et Hatem

Introduction

L'objectif d'une communication est essentiellement de permettre à deux systèmes distants de dialoguer entre eux, d'échanger des informations. Pour cela les deux systèmes doivent parler le même langage, c'est pourquoi on établit des règles de communication. L'ensemble des ces règles constitue le protocole de communication. Le réseau doit également assurer la stabilité du transport des données.

Pour répondre à ces différents impératifs, de manière fiable et évolutive on choisit de décomposer le lien entre deux clients, en fonctions. Ces fonctions constituent des couches successives qui prennent en charge les données applicatives, et assurent leur acheminement à travers le réseau vers leur destination.

I.1. Définition d'un réseau informatique

Selon AFNOR « ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques ». (norminfo.afnor.org)

I.2. Classification des réseaux informatique

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que des stations de travail ou des serveurs. Dans un premier temps, ces communications étaient destinées au transport de données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo sur ces réseaux informatique devient naturelle, même si cela ne va pas sans difficulté.

On compte généralement quatre catégories de réseaux informatiques, ils peuvent être classifiés selon leurs étendue (éloignement maximal entre systèmes informatiques) :

- RLI (Réseaux Locaux Industriels) : Un réseau local industriel est en première approximation un réseau local utilisé dans une usine ou tout système de production pour connecter diverses machines afin d'assurer la commande, la surveillance, la supervision, la conduite, la maintenance, le suivi de produit, la gestion, en un mot, l'exploitation de l'installation de production.
- LAN (local Area Network) : réseau local pour des systèmes informatique appartenant à la même entreprise (Ethernet, AppleTalk….) son étendue est entre 10m et 1Km.

- MAN (Metropolitan Area Network) pour les réseaux des villes étendue entre 1Km et 10Km.
- WAN (Wide Area Network) : large réseaux national ou international. échelle de la terre. (Laissus, Version du 25 f˝evrier 2009)

I.3. Protocoles de communication du réseau local industriel :

Un protocole de communication est un ensemble de règles permettant à plusieurs ordinateurs ou appareils informatiques de dialoguer entre eux. A la manière des humains, les appareils doivent parler le même langage afin de se comprendre. (Jean-François Hérold, juin 2015)

I.3.1. La nécessité de la normalisation

La normalisation est un acte primordiale dans le domaine de la communication, en effet, il faut que tout utilisateur connecté au réseau soit apte à recevoir et à transmettre des informations destinées à l'ensemble des participants, c'est-à-dire qui faut se mettre d'accord sur l'ensemble des éléments nécessaires à la communication pour que des échanges puissent s'effectuer. L'établissement d'une architecture de communication est indispensable pour permettre à des applications informatiques de coopérer sans avoir à tenir compte de l'hétérogénéité des moyens et procédés de transmission tel que la topologie du réseau, les caractéristiques des équipements ou des supports d'accès.

I.3.2. La norme EIA RS-232

L'EIA (Electronics Idusteries Association): la norme est créée en 1962 dans le but de normaliser l'interface entre les équipements de traitement de données et les dispositifs de transmission de données appelés ''modem''. L'interface RS-232 permet la mise en œuvre d'une communication série dite asynchrone (car il n'ya pas de signal d'horloge commun aux deux dispositifs communicants) et '' asymétrique'' : un seul conducteur utilisé pour la transmission des données. Cette méthode d'interconnexion présente l'inconvénient de créer un couplage parasite important ce qui va limiter la longueur et de la vitesse de transmission. Ainsi la norme donne comme vitesse maximales de transmission de données la valeur 20 Kbit/s pour une longueur de câble de 15m. (Jean-François Hérold, juin 2015)

I.3.2.1. La transmission asynchrone des données

Dans le mode de transmission asynchrone, la transmission des données se fait sans signal d'horloge commun à l'émetteur et au récepteur. Le récepteur échantillonne la ligne de réception de données afin d'identifier les bits de la donnée reçue.

Pour faciliter ce travail d'identification, la procédure utilisée pour la transmission de donnée est la procédure dite '' star-stop'' qui correspond au chronogramme suivent :

Figure I.1 : **Transmission asynchrone des données.**

Chaque transmission est précédée d'un bit dit de ''Start'' qui permet de repérer le débit de la donnée (entre 5 bits et 8 bits) et suivi d'un ou plusieurs bits de ''stop'' qui permet au récepteur d'identifier la fin de la donnée.

I.3.2.2. Utilisation de l'interface RS-232 en configuration restreinte

Cette dernière est élaborée pour connecter un modem à un système informatique, Sa grande popularité dans le monde industriel a étendu son utilisation pour établir des liaisons autres que celle prévue initialement. Dans ce cas, on utilise une connexion en configuration dite '' restreinte'' ou encore appelée '' liaison à trois fils'' en référence aux trois signaux de l'interface qui sont utilisés TD (transmission de données) RD (réception de données) et GND (le potentiel zéro).

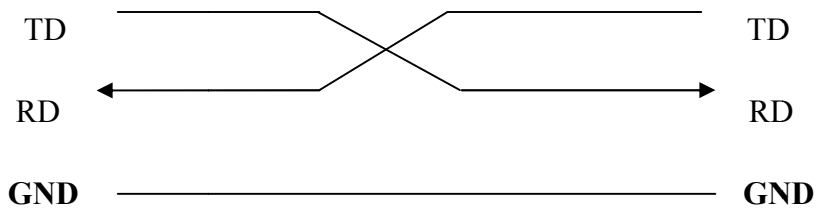


Figure I.2 : **Connexion en configuration à trois fils.**

I.3.3. Norme EIA RS-485

Il s'avère habituellement difficile de transmettre des données à grande vitesse, sur de grande distance et parfois dans des conditions de bruit élever, entre des parties d'un système

informatique et des périphériques en utilisant une interface asymétrique. Pour remédier à ce problème des interfaces dites ‘’ symétriques’’ sont proposées. C’est le cas notamment de l’interface RS-485 que l’on retrouve dans de nombreux réseaux d’automates. (Jean-François Hérold, juin 2015)

I.3.3.1. Principe de fonctionnement d’une interface symétrique

L’image du bit à transmettre est une différence de potentiel entre deux fils de liaison comme le montre la figure suivante :

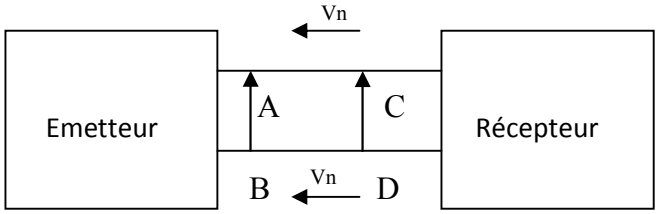


Figure I.3 : **Principe d’une interface symétrique.**

Vn : représente la tension de bruit affectant les lignes de transmission.

On peut établir :

$$V_A - V_B = V_n + (V_C - V_D) - V_n \Leftrightarrow V_A - V_B = V_C - V_D$$

De par sa structure, l’interface symétrique permet d’éliminer la tension de bruit.

Remarque

1- Dans la réalité, ce n’est pas tout à fait le cas : en effet, la tension de bruit affectant les lignes de transmission n’est pas strictement identiques aux deux conducteurs.de ce fait il ya toujours une limite physique à la longueur de câble et pour la vitesse de transmission.

2- Comparaison entre les normes EIA RS-232 et EIA RS-485 :

Paramètres	RS-232	RS-485
Mode de fonctionnement	Asymétrique	Différentiel
Longueur max du câble	15 m	1200 m
Vitesse max de transmission	20 kbit/s	10 Mbit/s

3- De nombreux constructeurs d’API (automates programmables industrielles) ont adopté l’interface RS-485 pour la mise en œuvre de leurs bus d’automates.

I.4. Protocole de communication TCP/IP sur Ethernet

La mise en œuvre des réseaux en automatisme industrielle se fait par une adoption progressive des protocoles standards mondiaux Ethernet et TCP/IP

(TCP : transmission Control Protocol. IP : Internet Protocol)

Ces technologies, associées à internet, permettent un accès aux données de l'automatisme en tout lieu, à toute personne autorisée. On assiste alors au développement de nouveaux services comme la gestion de production, la supervision des procédés, la maintenance à distance (télémaintenance).

I.4.1. Ethernet

Est un réseau de type LAN il apparait comme un support de transmission de données et supporte plusieurs protocoles réseaux tel que le TCP/IP, Appel, Talk, DECnet. Son architecture est la plus répondue au monde.

I.4.1.1. Caractéristiques du réseau ETHERNET

Ethernet est un réseau local à bus partagé : une machine émet des trames sur le bus et aucune autre machine n'émet un contrôle sur cet accès au bus. Cette caractéristique implique la mise en place d'un protocole de gestion des accès afin de ne pas occuper le bus par plusieurs machines à la fois. Ce protocole de gestion porte le nom de CSMA/CD pour '' Carrier Sense Multiple Acces /Collition Detection'' ou accès multiple avec écoute de la porteuse et détection de collision. Le principe du protocole est le suivant :

1- Une machine détecte que le bus est libre (il y'a pas de porteuse)
2- La machine émet ses données (envoie des trames au format Ethernet)
3- Si des données se trouve sur le bus (détection d'une porteuse), aucune autre trame ne peut être émise tant que le bus n'a pas était libéré.
4- Si deux machines envoient des données sur le bus au même instant, il y aura une collision (superposition de deux trames lorsque deux stations émettent simultanément). En pareil cas, les machines détectent la collision, cessent d'émettre pendant une durée aléatoire puis elles essaient de reprendre la transmission.

I.4.2. Protocol TCP/IP

La pile de protocole TCP/IP est non-propriétaire permettant l'interconnexion des systèmes d'exploitation par le réseau. C'est donc une architecture multiplateforme qui s'appuie sur le principe du model client/serveur.

I.4.2.1. Principe du modèle Client/serveur

Dans le modèle Client/serveur en réseau, le terme serveur fait référence à toute application informatique qui reçoit une demande de service via le réseau sous forme de requête prévenant d'une application dite client, traite cette donnée et renvoi le résultat à l'application client.

L'exemple typique est le navigateur web, qui demande au serveur de lui envoyer une page. La demande se fait sous la forme d'une chaîne de caractères :

« http://www.google.fr/télémaintenace ». Le serveur (en l'occurrence la machine qui a pour nom « www » dans le domaine « google.fr ») renvoie le contenu de la page «télémaintenance », et le logiciel client l'interprète et l'affiche en retour.

Le modèle Client/serveur en réseau se présente comme une relation entre des applications informatique qui peuvent s'exécuter sur des machines séparées, reliées par réseau, relation dans laquelle l'application serveur et fournisseur de service et l'application client est consommatrice de service.

De ce fait, le terme serveur s'applique à tout programme qui offre un service pouvant être utilisé via un réseau. Un programme devient client lorsqu'il émet une requête vers un serveur et qu'il attend une réponse. Les communications entre clients et serveurs s'effectuent toujours à l'initiative des clients, jamais à celle des serveurs et attendent passivement les requêtes des clients.

I.4.2.2. Modèle architectural TCP/IP

Comme Il est difficile à un groupe de personnes de s'entendre du moment qu'ils ne parlent pas le même langage, ça l'est aussi pour un réseau informatique qui ne suit pas les mêmes règles de communications. Un modèle de référence était élaboré au début des années 1980 par ISO (International Standards Organisation).

Ce modèle s'appelait OSI (Open System Interconnexion) propose aux fournisseurs un ensemble de normes assurant une compatibilité et une interopérabilité accrues entre divers types de technologies réseau produites par de nombreuses entreprises à travers le monde.

La normalisation mise en place définit un modèle théorique à 7 couches où chacune des couches est définie de façon à travailler avec la couche directement au dessus ou au dessous d'elle, comme l'indique la figure suivante :

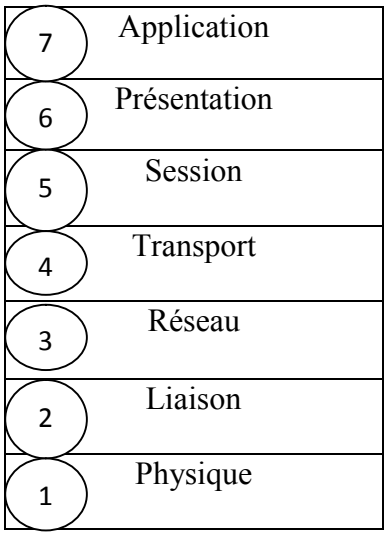


Figure I.4 : **Les sept couches du modèle OSI.**

a- **La couche physique** : Fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de liaison de données.

b- **La couche liaison :** Fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions de liaison de données entre entités du réseau. Elle détecte et corrige, si possible, les erreurs dues au support physique et signale à la couche réseau les erreurs irrécupérables. Elle supervise le fonctionnement de la transmission et définit la structure syntaxique des messages, la manière d'enchainer les échanges selon un protocole normalisé ou non.

c- **La couche transport :** Assure un transfert de données transparents entre entités de session et en les déchargeant des détails d'exécution. Elle a pour rôle d'optimiser l'utilisation des services de réseau disponibles afin d'assurer au moindre coût les performances requises par la couche session.

d- **Les couches session, présentation et application** : Constituent les couches hautes du modèle OSI et offrent des services orientés vers les utilisateurs alors que les couches basses sont concernées pas la communication fiable de bout en bout. Elles considèrent que la couche transport fournit un canal fiable de communication et ajoutent des caractéristiques supplémentaires pour les applications.

En 1983 le protocole TCP/IP est devenu un standard de communication, après la déclaration du ministère de la défense américain. La guerre froide a engendré le besoin de concevoir un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire.

Dans un monde connecté par différents types de médias de communication tels que les fils de cuivre, micro-ondes, fibres optiques et liaisons satellite, le ministère de la défense souhaitait une transmission de paquets capable d'aboutir à coup sûr et sous m'importe quelle condition. Ce problème de conception extrêmement ambitieux a conduit à la création du modèle TCP/IP.

Contrairement aux technologies réseau propriétaires mentionnées précédemment (OSI), le protocole TCP/IP a été développé en tant que norme ouverte. Cela voulait dire que n'importe qui pouvait utiliser TCP/IP. Cela contribua à accélérer le développement de TCP/IP en tant que norme. Ce modèle est composé des quatre couches suivantes :

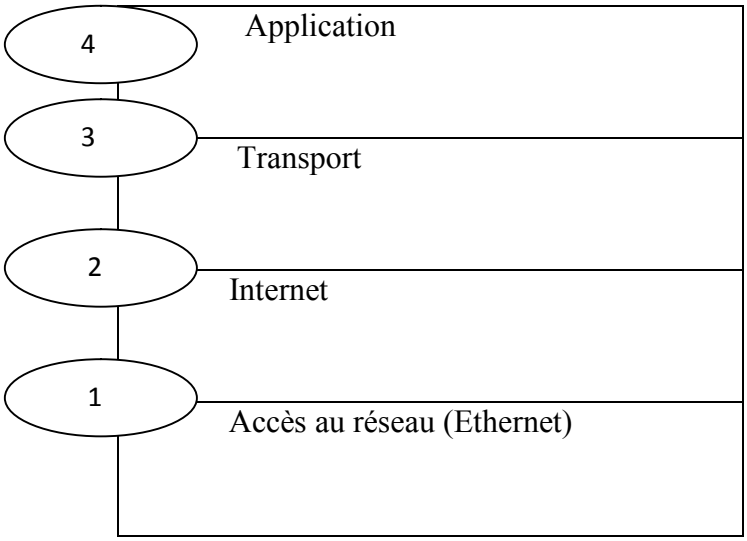


Figure I.5 : **Les quatre couches du modèle TCP/IP.**

Remarque

Bien que certaines couches du modèle TCP/IP aient le même nom que les couches du modèle OSI, elles ne correspondent pas exactement. Il est à noter que la couche application assure différentes fonctions dans chaque modèle.

La couche Application

- Assure le langage de communication entre les clients et les serveurs
- Assure les transferts bidirectionnels des fichiers binaires

- Permet un accès aux fichiers d'un équipement de stockage distant tel qu'un disque dur, dans un réseau.
- Permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité.

La couche transport

- Chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs.
- Fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé.

La couche Internet

- Responsable d'adressage, fragmentation et réassemblage des paquets.
- Chargé de la résolution de l'adresse de couche Internet en adresse physique.
- Protocole de « gestion » de réseau. Son rôle est d'exécuter les fonctions de diagnostic et d'établir un rapport d'erreurs suite à la transmission des paquets.

La couche physique (Ethernet)

Les pilotes d'application, les cartes modem et les autres équipements s'exécutent au niveau de la couche d'accès au réseau. Cette dernière définit les procédures utilisées pour communiquer avec le matériel réseau et accéder au média de transmission.

I.5. Les supports physiques des communications

Un protocole de communication nécessite forcement une liaison, ou bien un support physique capable d'assurer l'interconnexion des appareils industriels. Les données vont transiter sur un câble au moyen d'un signal, il est nécessaire de choisir un support de transmission apte à transférer les nombreuses applications dont les câbles métalliques ou la fibre optique.

Le signal peut se détériorer à cause des perturbations électromagnétiques ou d'une distance trop longue à parcourir. Il est alors tellement affaibli ou déformé qu'il n'est plus exploitable. Il est donc nécessaire de connaître les caractéristiques principales du câble utilisé afin de préserver la qualité du signal émis sur toute la longueur du câble. Un câble de transmission ou une fibre optique sont caractérisés par :

- l'atténuation qu'il impose au signal par mètre.
- la vitesse de transmission maximale.
- la sensibilité aux interfaces.
- le coût.
- la flexibilité et la facilité de l'installation.

- L'impédance ou résistance du câble en fonction de la fréquence. (SUPINFO)

I.5.1. Principaux câbles utilisés

Deux types de câblage sont possibles, soit à base de câble métallique, soit à base de fibre optique. Au niveau d'un réseau local, les câblages sont essentiellement mis en œuvre à l'aide des câbles métalliques. On distingue deux types de câbles métalliques dans le domaine des réseaux industriels :

a- câbles coaxial : est un câble monobrin, le conducteur de données est entouré d'un diélectrique servant d'isolant, d'un blindage composé de tresses métalliques pour s'affranchir des perturbations d'origine électromagnétiques et d'une gaine extérieure en PVC. Il répond à la norme RG58, il doit posséder une impédance de 50 ohms dont la structure est donnée par la figure suivante :

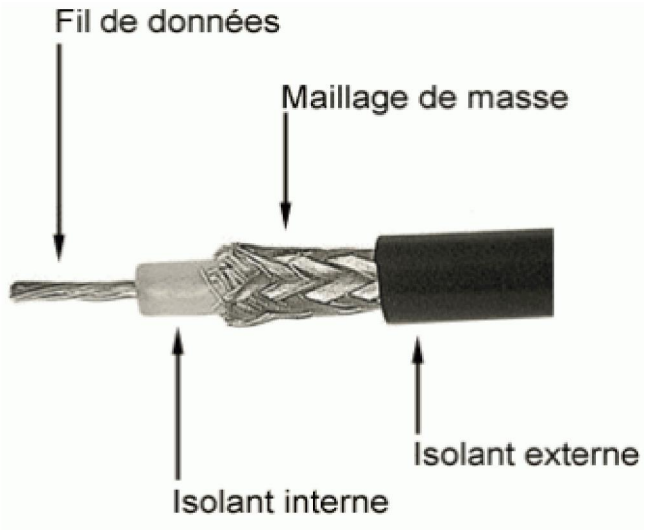


Figure I.6 : **Structure d'un câble coaxial RG58.**

Remarque

Lors du passage d'un signal électrique de haute fréquence, les électrons vont plutôt s'agiter en surface du conducteur qu'en profondeur, les signaux de basses fréquences passeront dans tout le conducteur contrairement aux signaux de haute fréquence qui passeront dans la peau du conducteur ce phénomène est appelé ''effet de peau'' .

b- Câbles torsadés

Pour contrer l'effet de peau, l'astuce consiste à faire passer le signal dans de multiples conducteurs fins isolés individuellement, cette idée simple est appelée la mise en ''fils de Litz''.

Un câble torsadé est un ensemble de lignes symétriques formées par plusieurs pairs de fils conducteurs enroulées en hélice l'une autour de l'autre.

Un code de couleurs est normalisé repère chaque fil, les torsades permettent de limiter l'effet de diaphonie. Les branchements aux machines se fait à l'aide de la prise RJ45.

Figure I.7 : **Mâle et femelle de la prise RJ45.**

N.B :

Pour pouvoir relier plusieurs machines entre elles sur un réseau il faut utiliser un matériel de connexion, il s'agit du hub ou le concentrateur, le hub est composé de plusieurs prises RJ45 femelle qui a le rôle de relier les machines entre elles.

Un Hub

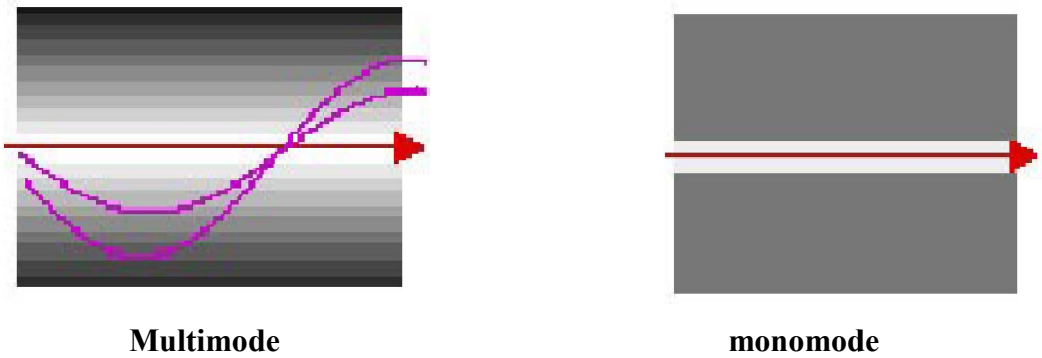
Figure I.8: **Un hub**

Le fonctionnement du hub est particulier, imaginons qu'il ait cinq machines branchées au hub A, B, C, D, E. Si A veut communiquer avec C elle va envoyer l'information au hub, mais lui ne sait pas lire, il va envoyer l'information à toute les machines en se disant qu'il y en aura bien une des machines qui sera la bonne. Les machine B, D, E vont voir que l'information n'est pas pour elles et vont la jeter tandis que la machine C va pouvoir la lire.

c- La fibre optique

Son nom scientifique est 1000BF, avec la fibre optique nous transportons des 0 et des 1 non avec l'électricité mais avec de la lumière, il existe deux type de fibre optique, la fibre monomode et multimode.

La fibre monomode fait passer une seule longueur d'onde lumineuse d'une seule couleur elle fonctionne avec un laser qui peut être vert, bleu, rouge… La fibre miltimode fonctionne avec de la lumière blanche donc toutes les longueurs d'onde, car la lumière blanche est la somme de toutes les couleurs.



Multimode **monomode**

Figure I.9 : **Principe multimode et monomode – principe.**

Avoir deux types de fibres différentes, c'est par rapport à la distance parcourue et le débit qui diffère d'une application à une autre. En effet la fibre monomode est beaucoup performante que la multimode .la lumière blanche, elle va être reflétée à l'intérieur de la fibre mais chaque couleur va se refléter légèrement différemment. Comme vous lanciez une poignée de cailloux, ces derniers sont bien regroupés au lancement mais plus ils avancent et plus ils s'éparpillent alors que si nous lançons un seul caillou il arrive groupé vu qu'il est seul. On pourra parcourir une distance plus longue avec la fibre monomode.

- 2 km pour la fibre multimode.
- 60 km pour la fibre monomode.

Remarque

Même si les distances parcourues aujourd'hui peuvent être beaucoup plus grandes (le record étant de l'ordre de 8000 km). C'est ainsi que l'on a relié les États-Unis et l'Europe, en passant de la fibre monomode dans l'Atlantique, et en répétant le signal lumineux tous les 60 km.

Conclusion

Dans un transfert de données la nécessité de coder puis décodé l'information ralentit toujours l'opération, le challenge était donc d'établir des protocoles développés afin de transférer un maximum de données en réduisant le temps de traitement. La norme RS-232 permet une communication en **Duplex** c'est-à-dire en un seul fil le transport de l'information se fait dans un seul sens et non les deux en même temps, contrairement à la norme RS-485 peut être en mode **Full Duplex (**sur quatre fils) ou en mode **Half Duplex** (sur deux fils) Ceci signifie que les informations sérielles sont véhiculées sur une même ligne tantôt dans une direction, tantôt dans l'autre. Puis vient Ethernet qui s'adapte à tous types de topologie (nature de la connexion) et qui a généralement quatre paires de fils Chaque pair est identifié par une clé, appelée adresse MAC (Média Access Control), pour s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes sans configuration préalable.

La nature et le matériau des câbles jouent un rôle important dans la transmission, le passage de l'électron au photon ou bien du cuivre à la lumière était la réponse à la problématique de temps de transmission des données.

Introduction

Les réseaux locaux industriels ont été introduits petit à petit dans les systèmes automatisés, à des stades divers selon les domaines d'application. Ils sont nés avec le développement de l'électronique et des matériels numériques programmables. L'apparition des régulateurs numériques et des automates programmables a conduit les offreurs à mettre sur le marché des réseaux pour les interconnecter et rapatrier à moindre coût de câblage les informations nécessaires à la conduite par les opérateurs dans les salles de commande. C'est ainsi qu'est né le réseau WDPF de Westinghouse (Jeumont- Schneider en France) dans les années 1970. Ce réseau était essentiellement utilisé dans les processus continus, les premiers à être automatisés et à innover dans les nouvelles technologies de l'automatique et de l'informatique industrielle. Puis est né le réseau MODBUS (MODicon BUS) de Gould MODicon, pour coordonner les activités sises sur plusieurs automates. Dans les processus continus, des calculateurs dits d'optimisation étaient utilisés de longue date pour envoyer des consignes sous forme d'aides aux opérateurs. Il est apparu utile de les connecter d'une part aux stations de travail des opérateurs et d'autre part aux équipements qui pilotent les machines de production. Le grand développement des réseaux locaux industriels date du début des années 1980.

Ces réseaux utilisaient certains des protocoles développés pour les télécommunications avec quelques adaptations aux contextes de réseau local et du milieu industriel. Par exemple le protocole TCP/IP; les concepts de station maître et de station esclave étaient directement repris des réseaux de transmission de données des années 1960. La principale innovation de ces réseaux fut d'introduire la notion de « données globales ». Ces informations répertoriées issues de chacune des stations étaient transmises périodiquement à toutes les autres de façon à maintenir un état global approché du système. Le fonctionnement des équipements raccordés qui étaient essentiellement des automates programmables à système exécutif mono tâche périodique (on dit aussi parfois synchrones). Le réseau tentait de reproduire le système d'entrées-sorties.

Parallèlement à ces projets de réseaux ouverts, donc ayant vocation à devenir des normes internationales, en l'absence de normes, et devant l'intérêt croissant des réseaux, de nombreux réseaux locaux industriels privés voyaient le jour chez tous les constructeurs et chez des offreurs indépendants. Les services fournis par les premières versions de ces réseaux étaient le rapatriement d'informations vers des postes de commande centralisée, la lecture et

l'écriture de variables, le démarrage ou la gestion de programmes, leur téléchargement et quelques fonctions de service que l'on placerait maintenant dans la gestion de réseau. Certains peuvent être considérés comme les ancêtres des réseaux de terrain quand ils offraient la possibilité de connecter des entrées/sorties déportées. Chaque constructeur choisissait son profil à partir de normes existantes dans les couches basses et définissait des services et protocoles que l'on peut qualifier d'application adaptés à ses clients et à ses marchés.

II.1. Définition du terme « réseau »

Un réseau est un système de mise en commun de l'information entre plusieurs machines. Les machines peuvent être des automates programmables industriels « API », des ordinateurs, imprimantes, pupitre de commande, variateur de vitesse.

Les informations échangées entre les équipements sur un réseau sont variées. Un automate programmable peut par exemple échanger avec un variateur de vitesse des mots et des bits dans le but de donner des consignes de vitesse ou des modes de marche. Un ordinateur peut échanger des fichiers ou des ensembles de mots pour une recette de production.

II.2. Exigences globales d'un réseau local industriel « RLI »

L'environnement industriel où doivent opérer les réseaux locaux industriels a des besoins très particuliers par exemple:

- Un processus de fabrication nécessite le téléchargement d'un programme sur un automate programmable ; il doit être transmis sans erreur le plus rapidement possible, toutefois un léger retard n'est pas trop préjudiciable si le processus physique pendant ce temps est dans un état stable. L'opération n'est pas critique du point de vue temporel, mais elle doit être effectuée sans erreur.
- Un processus de régulation doit recevoir la valeur d'une mesure toutes les 50 ms, cette valeur peut être erronée une fois de temps en temps, mais pas de manière consécutive, et la période doit être respectée. Les sécurités de transmission porteront non seulement sur la protection contre les erreurs éventuelles, mais aussi sur les instants où les mesures sont produites, transmises, consommées. Dans ces deux exemples, les mécanismes de traitement des erreurs ne seront pas les mêmes ; dans le premier on choisira des acquittements et un contrôle de flux ; dans le second, et en général pour les trafics périodiques, on fera le choix de communication sans acquittement, avec un contrôle de la reprise en cas d'erreur par les processus d'application.
- Un contrôleur de cellule doit pouvoir gérer les tâches (les activer, les arrêter, leur transmettre des paramètres) sur les commandes numériques, les commandes de robot, les automates programmables. On identifie ainsi des services de niveau application qui devront être disponibles sur les machines concernées.

- Si plusieurs automates doivent éditer un journal, ou afficher des messages sur une station opérateur, on aura besoin de services de partage de ressources, comme les sémaphores, pour ne pas mélanger les messages.
- Un processus de supervision doit être averti des dysfonctionnements du processus physique dans des délais raisonnables qui dépendent des constantes de temps des variables physiques. Il faudra pouvoir garantir que des contraintes de temps seront respectées.
- Au niveau physique les réseaux locaux industriels doivent être dotés de moyens résistant aux perturbations, aux chocs, à la chaleur, …etc. tel que les câbles et les connecteurs blindés. Les moyens de communication utilisés à chaque niveau doivent répondre en termes de débit aux besoins de ce niveau. (Abdelhamid, 2010-2011)

II.3. Caractéristiques d'un réseau local industriel

contrairement à un réseau local de bureau où les messages ont la même priorité, les données échangées dans réseau local industriel varient selon leurs priorité en terme d'urgence et de la taille.

a- La nature du message échangé: Un retard de transfert de données peut engendrer des dégâts catastrophiques, à cet effet les messages échangés peuvent être :

✓ **Urgent** : tel que le transfert d'une information d'alarme ou l'ordre de fermeture d'une vanne.

✓ **Non urgent** : tout autre type de messages tel que le chargement d'un programme exécutable sur une machine.

b- Taille des messages : La charge du trafic peut être très irrégulière en taille de message et en leur nombre ; tout dépend du niveau concerné. Ces messages peuvent être :

✓ **Courts :** tel que la valeur d'une mesure envoyée depuis un capteur, ou un ordre de démarrage d'une machine.

✓ **Longs :** tel qu'un fichier à un programme.

c- Qualité requise

✓ **Fiabilité** : la plupart des machines industrielles représentent des sources sérieuses de perturbations des communications ;On parle même de pollution magnétique dans les environnementsindustriels. Si on ajoute les risques auxquels sont exposés les moyens de communication dans une usine, on aperçoit rapidement quel message acheminénécessiteun

très haut degré de fiabilité pour pourvoir être transmis sans erreur, sans perte, et sans retard tant au niveau physique qu'au niveau protocole.

✓ **Performance** : Il faut garantir la continuité du fonctionnement même enrégime dégradé il faut garantir la continuité du fonctionnement même en régime dégradé c'est-à-dire en cas de panne de certains composants. Il faut avoir une bonne tolérance aux pannes et pouvoir reprendre certaines activités après les anomalies.

d- Services spécifiques : Un réseau local industriel peut être caractérisé par plusieurs phénomènes de communication spécifiques dont la prise en compte et l'apport de solution permet de garantir le bon fonctionnement du réseau :

✓ **Diffusion :** la diffusion peut être simultanée c'est-à-dire que plusieurs émetteurs doivent pouvoir envoyer vers plusieurs récepteurs en même temps. Le transfert simultané, par exemple, de plusieurs ordres à plusieurs actionneurs.

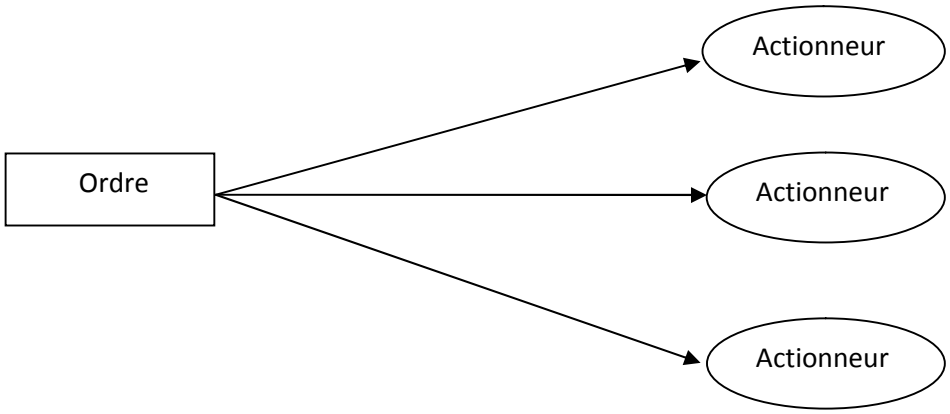


Figure II.1 : La diffusion dans un RLI

✓ **Concentration** : Plusieurs équipements peuvent demander la prise en compte en même temps, tel qu'une requête de prise de mesure simultanée de plusieurs capteurs

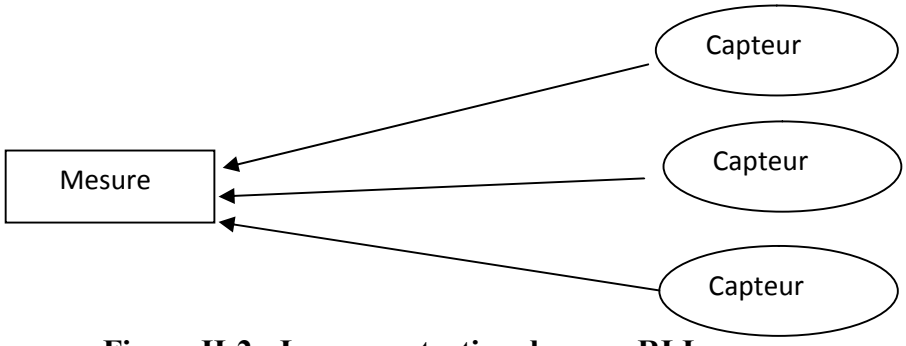


Figure II-2 : La concentration dans un RLI.

II.4. Architecture d'un réseau industriel

Un réseau local industriel, en une première approximation, est un réseau local utilisé dans une usine ou tout système de production pour connecter diverses machines afin d'assurer la commande, la surveillance, la supervision, la conduite, la maintenance, le suivi de produit, la gestion, en un mot, l'exploitation de l'installation de production.

Néanmoins, à chaque niveau d'abstraction, dans un environnement industriel, correspond un réseau permettant de relier ses différents éléments. Entre deux niveaux différents il doit y avoir une passerelle si les deux réseaux sont hétérogènes. On distingue donc trois types de réseaux :

a- Les réseaux de terrain (niveau capteurs) : connectent les capteurs, les actionneurs et les dispositifs comme les automates, les régulateurs et plus généralement tout matériel supportant des processus d'application ayant besoin d'avoir accès aux équipements de terrain. Ils doivent offrir au minimum les mêmes services que les systèmes d'entrées/sorties industrielles, mais d'autres très importants (de synchronisation par exemple) seront aussi définis pour faciliter la distribution des applications.

b- Les réseaux d'atelier (niveau machines) : connectent, dans une cellule ou un atelier, les dispositifs de commande de robots, de machines-outils, de contrôle de la qualité (lasers, machines à mesurer). Ces réseaux se rencontrent essentiellement dans les industries manufacturières.

c- Les réseaux d'usine (niveau entrprise) : un réseau qui irrigue l'ensemble de l'usine, interconnectant des ateliers, des cellules avec des services de gestion, les bureaux d'études ou des méthodes.

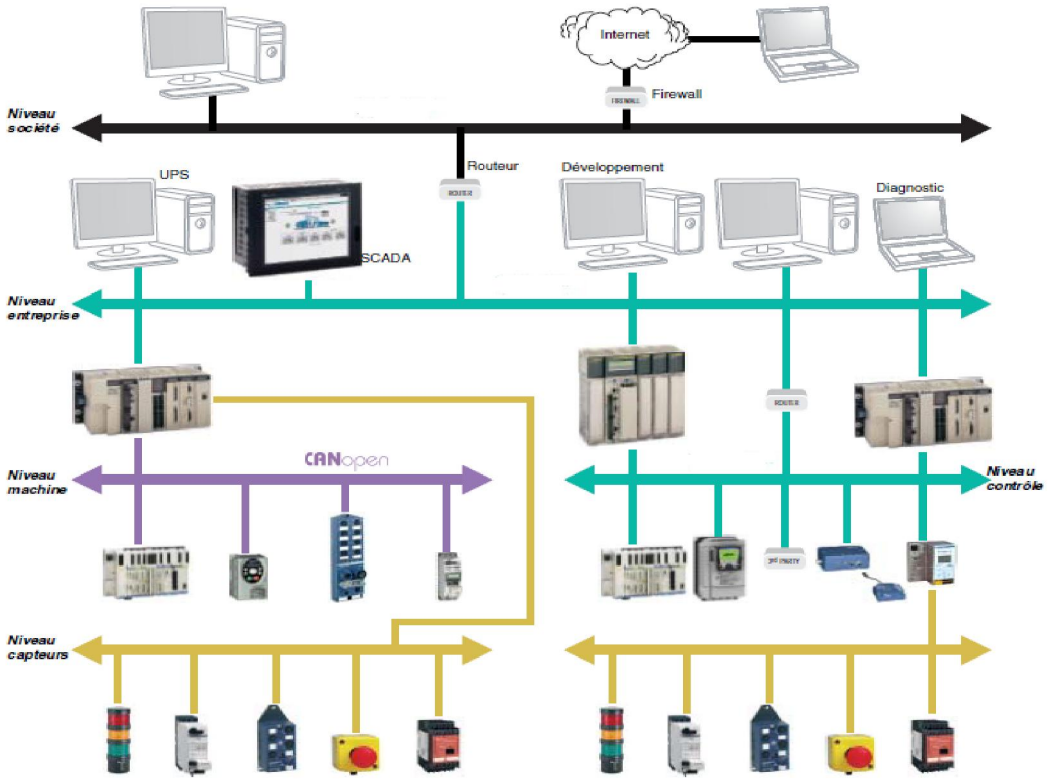


Figure II.3 : Architecture d'un réseau local industriel.

II.5. Le rôle de l'informatique dans un réseau local industriel

Le besoin d'assurer une communication entre le monde informatique et l'automatisme est devenue indispensable du fait de la nécessité d'augmenter la productivité (fiabilité, pérennité…) des usine de fabrication. Le RLI d'automatisme propriétaire ont rapidement bénéficier des grands standards développés sur les architectures informatiques. La communication entre ces deux mondes d'abord fut d'être assuréepar des liaisons séries (RS), puis par des produits issus de partenariats entre les constructeurs d'automates programmables et les grands de l'informatique, ces derniers ont proposé dans leurs catalogues une offre de coupleurs RLI plus avancés.

II.5.1. La segmentation des réseaux et bus

Le modèle CIM (Computer Integrated Manufacturing), qui se voulait être la réponse à la quête de performance, a réussi à créer une segmentation verticale des réseaux et des bus.

Le CIM décrit les différents niveaux de communication sous une forme quantitative des données à véhiculer. Le niveau 0, niveau capteur/actionneur, nécessite un transfert performant (quelques millisecondes) mais concernant peu d'informations (données binaires), alors que le niveau 4 nécessite quant à lui de véhiculer de gros paquets de données, des fichiers et la performance n'est plus forcément un critère prédominant.

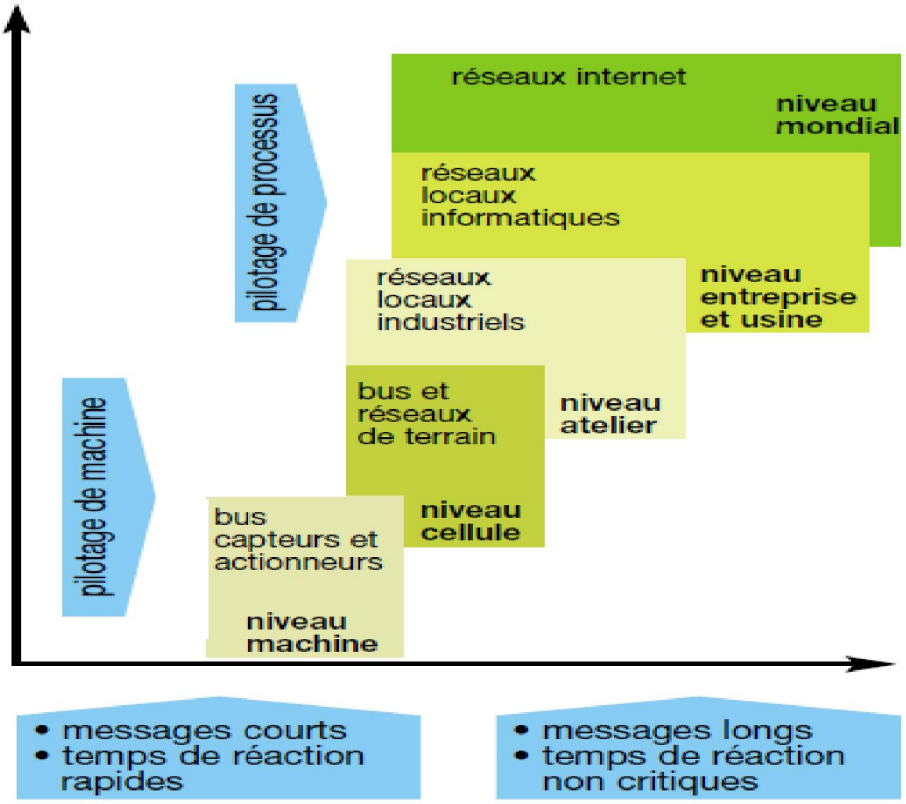


Figure II.4 : La segmentation CIM par de réseau ou bus.

Remarque

Avec l'adoption de la segmentation, les mécanismes d'échanges traditionnels ont évolué.Les offreurs adaptent les performances de leurs réseaux en fonction des niveaux du CIM, mais cela ne résout pas donc la problématique de gestion de l'augmentation du trafic sur les médiums. Les constructeurs des automates programmables ont créé des réseaux et des bus adaptés au besoin, par exemple le ''sensor bus'' est un bus capteurs et actionneurs unitaire simple, ''field bus'' réseau de communication entre l'unité de traitement, les l'automates programmables, les superviseurs, la commande numérique, ''device bus'' bus et réseaux pour périphériques : variateurs, robots, axes…

II.5.2 De l'automatisme centralisé à l'automatisme décentralisé

a- Les automatismes centralisés : Dans les années 1980, les automatismes, s'appuyant sur des API, traitaient essentiellement des fonctions séquentielles, autrement dit, elles géraient des demandes d'exécution (à l'image des entrées), ainsi élaboraient des demandes d'exécution d'actions(positionnement des sorties).Par la suite, les API ont été amenés à gérerde nombreuses fonctions de métier tel que la variation de vitesse, le dialogue homme/machinecomplémentaire commele diagnosticdes systèmes d'applications.Les automatismes, géraient toutun ensemble de fonctions qui n'avaient pasforcement d'interactions entre elles.Lorsqu'il y avait déjà un automate dans l'usine,les automaticiens qui devaient intégrer une fonctionsupplémentaire se posaient simplement la question :l'automate ou le système d'automatisme en placepeut-il gérer les E/S supplémentaires et quelle estla capacité de mémoire disponible ?

Bien souvent, l'automatisation supplémentaire étaitréalisée avec cet automate existant, même si ellen'avait aucun rapport avec l'automatisme résident.

Ces automatismes centralisés amenaient denombreuses contraintes :

- aucune autonomie des différents sous-ensembles,
- mise en service et maintenance lourdes et difficilesà effectuer du fait de la quantité d'E/S gérées,
- arrêt de l'ensemble des fonctions gérées par l'APIen cas de défaut système de cet API ou d'arrêt pourla maintenance du moindre élément de l'outil deproduction.

b- Les automatismes décentralisés : Du fait des contraintes imposées par les systèmescentralisés, les utilisateurs se sont orientés vers unesegmentation de l'architecture. Celle-ci a été faite endécoupant l'automatisme en entités fonctionnelles.Elle permet de simplifier les automatismes enréduisant le nombre d'E/S gérées et présente doncl'avantage de faciliter la mise en service et lamaintenance. Cette segmentation a généré le besoin de communication entre les entités fonctionnelles. La fonction de communication est devenue la clef de voûte de la conception des architectures d'automatismes. Les bus de terrain ont permis de gérer dans un premier temps des E/S décentralisées par la périphérie d'automatisme.Ces réseaux de terrain contribuent à réaliser des gains de câblage importants et surtout ils permettent de rendre accessible des services sur tout le site. **(Scheinder électrique et Télémécanique, Mai 2007)**

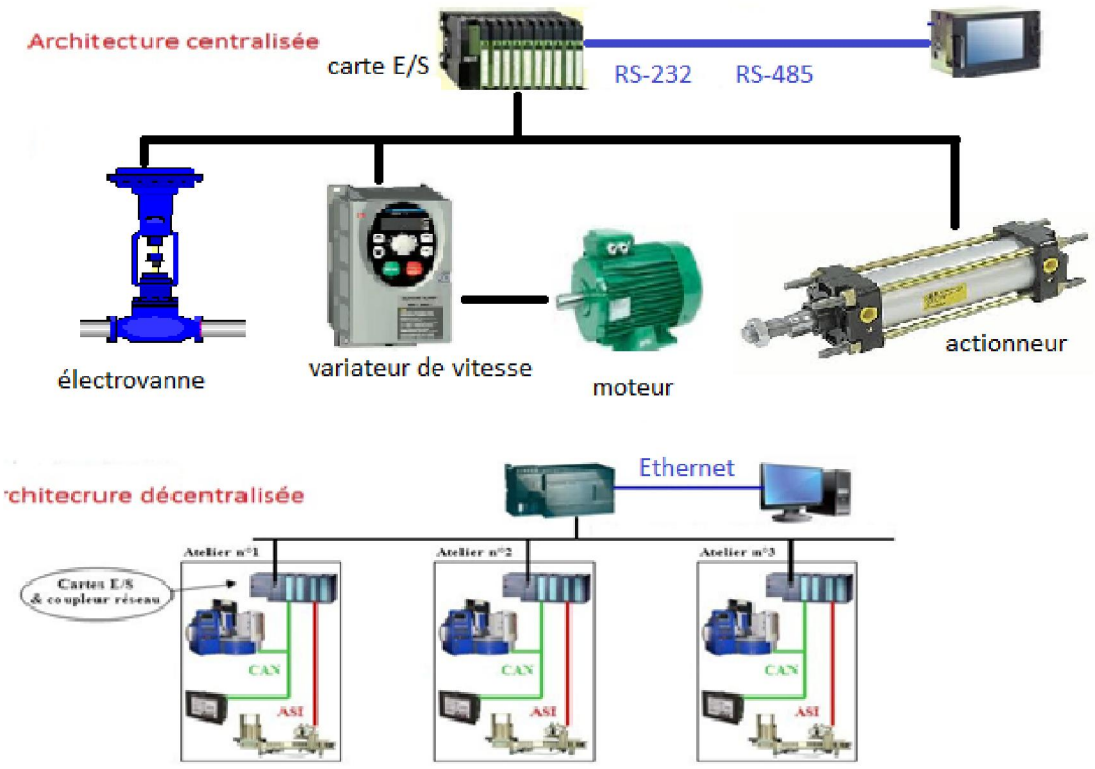


Figure II.5: au automatisme centralisé etdésenctralisé

II.6. Les bus et réseaux de terrain dans les machines industerielles

II.6.1. Le réseau TCP/IP dans les machines industrielles

La reconnaissance d'Ethernet TCP/IP, aussi bien dans les organisations que sur internet, en fait aujourd'hui le standard de communication. Sa large utilisation conduit à une diminution des coûts de connexion, à une augmentation des performances et à l'ajout de nouvelles fonctionnalités, tout en garantissant sa pérennité. Ethernet TCP/IP satisfait aux exigences de connexions de chaque application :

- ✓ Câbles cuivre en paire torsadée pour la simplicité et le coût.
- ✓ Fibre optique pour l'immunité aux parasites et pour les grandes distances.
- ✓ Redondance des communications, native au niveau IP (*Internet Protocol*).
- ✓ Radio ou satellite pour supprimer les contraintes de câblage.
- ✓ Accès distant en point à point via le réseau téléphonique ou par Internet au prix d'une communication locale.

Ethernet TCP/IP ouvert, par excellence, supporte tous types de communication :

- ✓ Pages Web.
- ✓ Transfert de fichiers.
- ✓ Messagerie industrielle…

Grâce au haut débit, le réseau ne limite plus les performances de l'application. L'architecture évolue sans remise en cause. Les produits ou les équipements restent compatibles, assurant la pérennité du système.

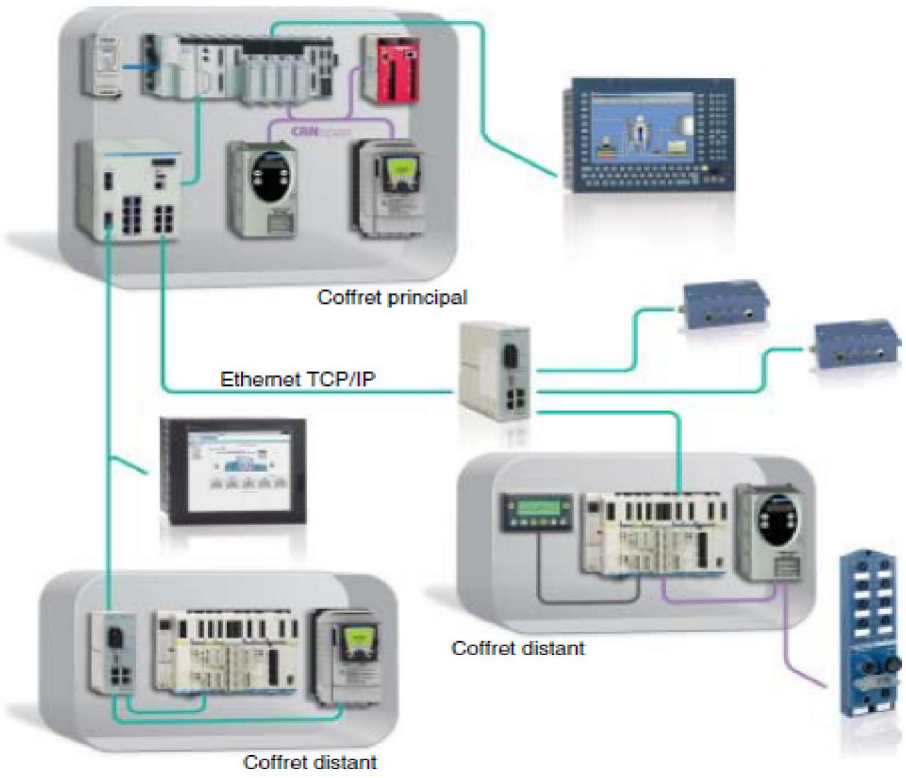


Figure II.6 : Ethernet TCP/IP dans les machines industrielles.

Ce moyen de communication est dédié aux machines et aux installations complexes et de grande taille nécessitant modularité et transparence ainsi que des fonctions avancées. Les contraintes de cette solution de communication sont Les variateurs et les périphériques E/S ont un degré de protection IP 20**.** Les coffrets et les boîtiers doivent impérativement respecter un niveau de protection supérieur (par exemple, IP 50 ou IP 66).

II.6.2. Les bus CAN dans les machines industrielles

Grâce aux trames courtes (CAN open) et la connexion à la terre (CAN grounds) le bus a une grande immunité aux perturbations électromagnétiques. Le bus CAN permet à la machine ou à l'installation d'effectuer un travail précieux point de sélectionner un boîtier de petite taille dans un environnement de fortes interférences.

Sa performance réside dans sa flexibilité. La réponse du réseau est rapide; en moins de 1 ms, 256 points d'entrées/sorties numériques peuvent être traités à 1 Mbit/s. Le CAN est un système de communication, en temps réel, par liaison série conçu pour relier des composants intelligents ainsi que des capteurs et des actionneurs dans une machine ou un procédé. Il possède des propriétés multi-maître, c'est-à-dire que plusieurs nœuds peuvent simultanément demander l'accès au bus. Le CAN ne possède pas de système d'adressage mais plutôt un système d'allocation de priorités aux messages basé sur l'identificateur attribué à chaque message. Un émetteur transmet un message sans indication de destinataire ; sur la base de l'identificateur associé à ce message, chaque nœud décide de traiter ou d'ignorer ce message.

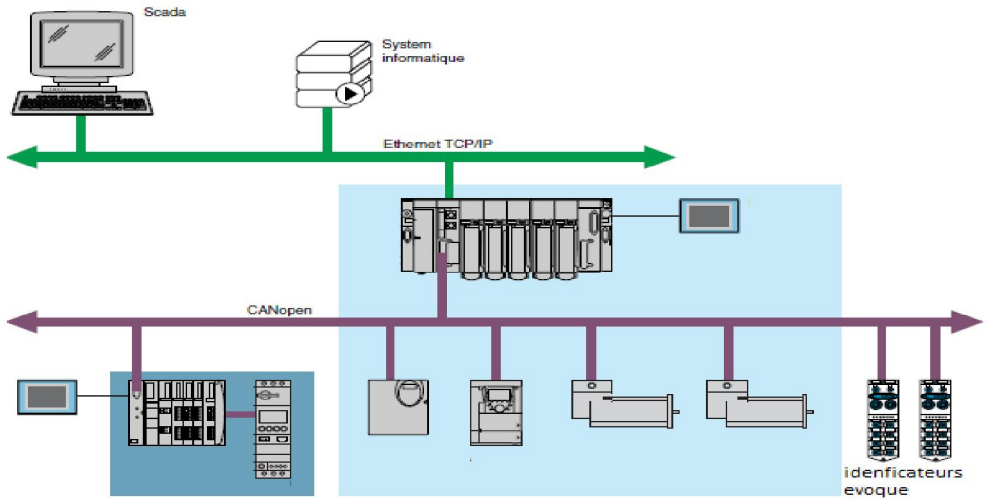


Figure II.7 : Le bus CAN dans les machines industrielles

II.6.3. Les bus ASI dans les machines industrielles

Le bus ASI est un système de câblage rapide et évolutif, dans lequel un câble unique sert à raccorder tous les composants d'un automatisme. Cela contribue améliorer nettement la fiabilité et la disponibilité des automatismes en réduisant les erreurs de câblage et en offrant une plus grande résistance aux interférences électromagnétiques (CEM). Le câble ASI est très facile à identifier et à connecter. Sa forme empêche toute connexion inversée de ses fils ASI+ et ASI-.

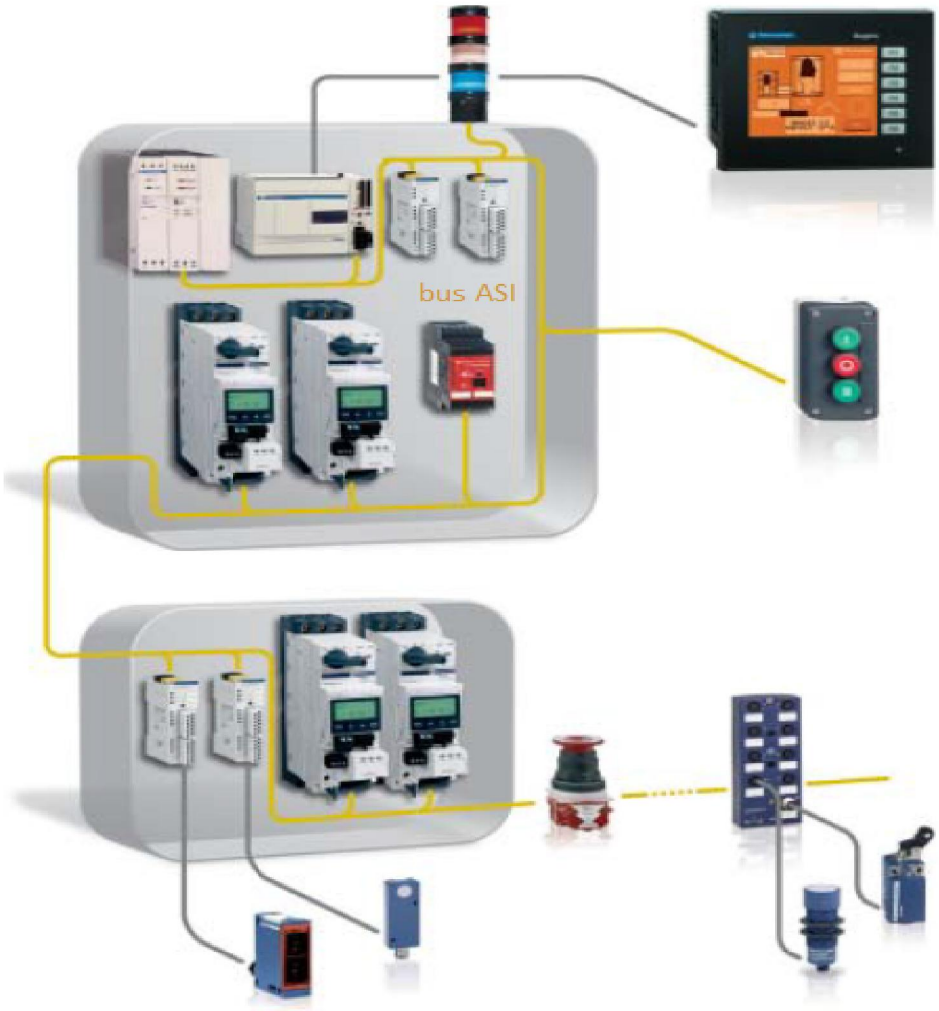


Figure II.8 : Les bus ASI dans les machines industrielles.

Les installations ASI sont très faciles à étendre. Inutile d'insérer un connecteur de chaînage ou d'installer un concentrateur afin d'ajouter un esclave supplémentaire à votre installation. Il vous suffit simplement de raccorder le connecteur de l'esclave au câble ASI. La technologie ASI ne requiert aucune terminaison de ligne. La fonction d'adressage automatique permet de remplacer un esclave par un nouvel esclave du même type, ce qui s'avère aussi simple que de désinstaller l'ancien esclave pour installer le nouveau, ce qui améliore la capacité de maintenance. Il prend en charge toutes les topologies, telles que les topologies en bus, en bus avec boîtiers de dérivation, arborescentes, maille, en anneau ou en étoile. La seule restriction concerne la longueur totale du câble.

II.7. Le besoin de protections des systèmes électriques industriels

Les systèmes industriels sont confrontés à des risques nouveaux, allant jusqu'à la destruction de l'appareil de production, la pollution de l'environnement ou la perte de vies humaines. Les industries sont aujourd'hui largement pilotées par des moyens numériques. Ceux-ci forment des réseaux industriels qui s'interconnectent : automates programmables industriels (API), stations de supervision, systèmes de régulation numérique et plus généralement quantité de capteurs, actionneurs et calculateurs.

Quel que soit le secteur d'activité, un incident cyber aux multiples conséquences impactera la performance économique. Mais beaucoup d'entreprises mettent en jeu des machines ou des produits dangereux pour l'homme ou pour l'environnement, et une attaque informatique aura des conséquences sur la sécurité des biens et des personnes. D'autres encore ont des activités qui sont critiques pour le reste des acteurs économiques ou pour le fonctionnement de la société au service de laquelle elles opèrent. Le risque devient alors systémique et concerne la société dans son ensemble. Le déploiement puis la gestion de la sécurité devraient être organisés afin de protéger l'installation des conséquences d'incidents de sécurité. Les activités peuvent être organisées selon les phases présentées ci-dessus. Il s'agit d'un processus continu, demandant des efforts permanents

II.7.1. Approche globale à la sécurité industrielle

- ✓ **Sélectivité :** détecter et isoler uniquement l'élement défaillant.
- ✓ **Stabilité :** laisser intacts les circuits en bon état pour assurer la continuité du fonctionnement
- ✓ **La vitesse :**un système de protection doit opérer aussi vite que possible en cas d'appel, pour minimiser les dommages et les chutes de production et pour garantir la sécurité du personnel.
- ✓ **Sensibilité :** détecter y compris la plus petite défaillance, les anomalies du système et opérer correctement après sa configuration.
- ✓ **Sensibilisation des personnels** : Une partie importante des incidents est liée à une méconnaissance par les intervenants des risques sur l'installation. Leur sensibilisation aux règles d'« hygiène informatique » contribue à réduire les vulnérabilités et les opportunités d'attaques. La sensibilisation doit être régulière car les risques évoluent en permanence.

✓ **Cartographie des installations et analyse de risque :** L'analyse des risques, le contrôle de la production et la distribution, aboutissent à la définition des mesures de sécurité adéquates, afin de réduire les surfaces exposées. Celles-ci peuvent être techniques mais aussi organisationnelles.

✓ **Veille sur les menaces et les vulnérabilités :** Les mises à jour des micro-logiciels des API et autres équipements, correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis. Elles permettent souvent d'obtenir l'information rapidement. Il peut être utile de demander à ses fournisseurs, au travers des contrats, d'être tenu informé des vulnérabilités ou bien figer les entrées/sorties des API pendant la mise à jour. L'activité de veille sera d'autant plus efficace que la cartographie sera exhaustive.

✓ **Réseau industriel isolé d'internet est-il sûr ?** Si le réseau industriel est relié de près 'ou de loin au réseau de gestion, alors les risques sont identiques. Une infection virale peut être transmise physiquement via un périphérique externe (une clé USB par exemple), ou via la console de maintenance des équipements. Enfin, un réseau industriel totalement isolé du net devient de plus en plus rare, du fait de l'interconnexion de plus en plus fréquente avec des logiciels de gestion.

✓ **Contrôle d'accès physique aux équipements et aux bus de terrain :** Identifier qui a besoin d'accéder aux équipements, pourquoi et à quelle fréquence. Installer les serveurs dans des locaux fermés sous contrôle d'accès (si possible dans les salles informatiques). Placer les unités centrales des stations, les équipements réseaux industriels et les automates dans des armoires fermées à clé. Protéger l'accès au câble réseau et aux prises de connexion. Maintenir l'autorisation d'accès en cas d'urgence.(Dalzon, 2004)

II.7.2 : Sécurité avancée informatique

a- Cryptographie : Etude des procédés permettant d'assurer la confidentialité, l'intégrité et l'authentification. Elle a pour but de garantir la protection des communications transmises sur un canal public contre différents types d'adversaires. La protection des informations se définit en termes de confidentialité, d'intégrité et d'authentification. Le système DQC (Distribution Quantique de Clés Cryptographiques) établis un secret partagé entre deux participants qui communiquent sur un canal non sécurisé. Ce secret sert généralement à générer une clé cryptographique commune.

Parmi les propriétés fondamentales sur lesquelles s'appuie l'échange de clé quantique, il y a notamment le théorème de non clonage, qui garantit qu'il est impossible pour un adversaire de créer une réplique exacte d'une particule dans un état inconnu.

Ainsi il est possible sous certaines conditions de détecter une tentative d'interception des communications.

b- Stéganographie : La stéganographie se réfère à la dissimulation de messages, c'est-à-dire la dissimulation avec pour but la confidentialité de l'existence de la communication. Son objetif est de faire passer inaperçu un message dans un autre message.L'inconvénient de la méthode est que le message est relativement limité en taille.

c- Les réseaux privés : Couramment utilisés dans les entreprises, les réseaux privés entreposent souvent des données confidentielles à l'intérieur de l'entreprise. De plus en plus, pour des raisons d'interopérabilité, on y utilise les mêmes protocoles que ceux utilisés dans l'Internet. On appelle alors ces réseaux privés « intranet ». Des serveurs propres à l'entreprise ysont stockés. Pour garantir cette confidentialité, le réseau privé est coupé logiquement du réseau internet. En général, les machines se trouvant à l'extérieur du réseau privé ne peuvent accéder à celui-ci. L'inverse n'étant pas forcément vrai.

d- Les réseaux privés virtuels (VPN) : Le but d'un réseau privé virtuel (Virtual Private Network ou VPN) est de fournir aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur un réseau privée. En d'autre terme, on veut regrouper des réseaux privés, séparé par un réseau public (internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés, et toute en gardant l'aspect sécurisé qui était assuré par de la coupure logique au réseau Internet.

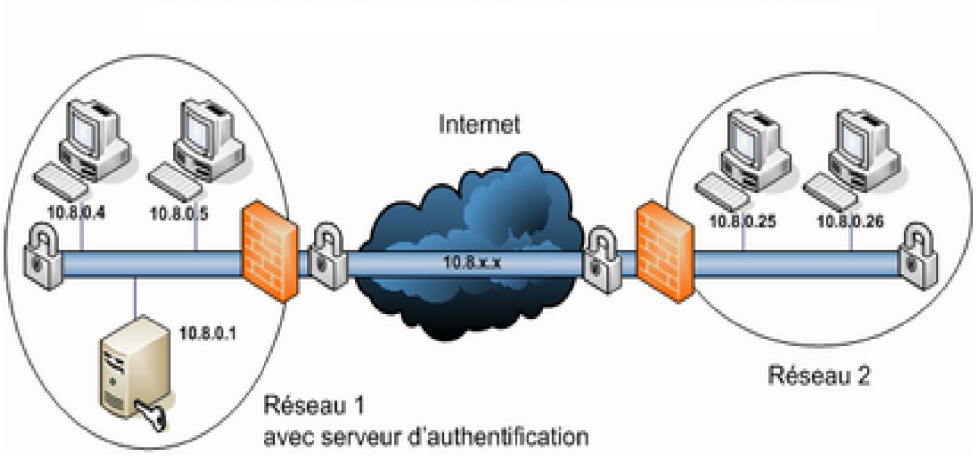


Figure II.9 : principe de fonctionnement d'un réseau privé virtuel (VPN).

II.7.3. Pricipe de fonctionnement des VPN :

Un reseau VPN repose sur un protocole appelé <<protocole de tunneling >> . ce protocole permet de faire circuler les informations de l'entrprise de façon cryptées d'un bout à l'autre du tunnel.ce principe consiste à constuire un chemin virtuel après avoir identifié l'emmeteur et le destinataire. Afin d'assurer un acces aisé et peut coûteux aux internets et aux extranets d'entreprise, les reseaux VPN simmulent un reseau privé, alors qu'ils utilisent en realité une infrastructure d'acces partagé comme internet .

Avantages et contraintes d'un VPN :

- Avantages :

✓ **Securité** : assure des des communications securisées et chiffrées.

✓ **Simplicité** : utilise les circuits de communication classique

✓ **Econnomie** : utilise internet en tant que média principal de tranport, ce qui évite les coûts liés à une ligne dédiée.

Les clefs de cryptage pour le client et le serveur doivent pouvoir être générées et regénérées.

✓ La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux public en particulier le IP.

Conclusion

Depuis que les automatismes sont réalisés à la base d'unités de traitement, les architectures ont fortement évolué et sont passés par differents stades (centralisé et décentralisé) pour arriver au architectures actuelles. Les réseaux locaux industriels d'automatisme ont rapidement bénéficié des standards de communications .

La communication entre le monde informatique et celui de l'automatisme a réussi l'adoption du modèle CIM afin de décentraliser les Entrées/sorties des équipements et autorise l'acces aux données en temps réél en tout lieu et à toute personne autorisé. Naturellement, nous assistons à une augmentation des flux d'échanges inhérente à l'augmentation des capacités de traitement des composants d'automatismes et ce besoin de transfert de volume d'informations important migre vers le bas des architectures. Il devient donc obligatoire d'augmenter les capacités et les performances des réseaux de communication essentiellement la communication via internet.

Les entreprises ont besoins d'échanger des données avec des succursales ou des employés travaillant à l'extérieur de l'entreprise. Le VPN est un moyen sécurisé pour échanger, à travers Internet, des données informatiques.

Introduction

Pendant deux millénaires, l'interface homme-machine fut simple. La visualisation était le processus lui-même et l'interface était la machine en elle-même. Les instruments de mesure étaient constitués conformément aux sens de l'opérateur. L'interprétation de l'information était faible. La commande manuelle était la seule utilisée et se bornait à quelques leviers. L'opérateur assurait également lui-même la maintenance.

En 1960, on assiste à l'apparition des machines individuelles monoblocs. La technologie utilisée à cette époque était de type pneumatique et électronique. La coordination et la commande étaient strictement à la charge de l'homme. Puis, étape significative, les années 70 qui ont vu apparaître les premières tentatives de régulations pilotées par calculateurs. Dans les années 1975 à 1980, sont arrivés les systèmes numériques distribués de la première génération. L'expérience vécue avec le pilotage des régulateurs par calculateur a montré l'intérêt de prendre en compte, dans le traitement, les relations qui existent entre les variables. La structure de coopération horizontale qui en résulte comprend désormais deux décideurs. Une relation entre un humain et une machine permet d'effectuer les décisions. L'interprétation de l'information devient forte. Dans les années 1986-1987, de nouvelles exigences apparaissent, concernant la productivité, la qualité, la flexibilité, la sécurité, induisant une complexité croissante qu'il faut maîtriser. Les installations se sont structurées pour que les machines et sous-machines restent simples à exploiter. Cette coordination est assurée par un système de supervision. (Jean-Marc Charte)

III.1. La supervision

La supervision industrielle, consiste à surveiller l'état de fonctionnement d'un procédé pour l'amener et le maintenir à son point de fonctionnement optimal. Née du besoin d'un outil de visualisation des processus industriels, dans un contexte économique de productivité et de flexibilité, la supervision a bénéficié d'une avancée technologique exceptionnelle.

À ses débuts, elle se composait d'un grand tableau mural représentant la vision des opérateurs du processus industriel. Rapidement, avec l'essor informatique, les voyants ont été remplacés par des écrans et des claviers. Le but restait le même : contrôler et commander un processus industriel.

Maintenant, la supervision est un maillon de l'information totale et intégrée de l'entreprise. Les nouvelles tendances dans ce domaine font état d'une future intégration de la gestion de production dans le contrôle-commande, d'un regroupement des données de l'atelier avec celles des bureaux, de manière directe et saine. Ainsi, chaque personne de l'entreprise, quel que soit son niveau, peut bénéficier d'un accès direct et en temps réel à toutes les données nécessaires à son travail. (WWW.siemens.com/wincc)

III.2. La place de la supervision

La supervision industrielle est utilisée par de nombreux procédés, soit pour la surveillance d'équipements ou de locaux, on parlera alors de GTC (gestion technique centralisée), soit comme SNCC (systèmes numériques de contrôle-commande), principalement pour des procédés de type continu, ou encore SCADA (Supervisory Control and Data Acquisition) ; car ces procédés regroupent l'ensemble des fonctionnalités du superviseur. Une installation industrielle automatisée s'organise autour de quelques modules principaux prenant en charge différentes parties essentielles de l'automatisation Dans les situations dynamiques, dont relèvent les situations de contrôle de processus, l'environnement change, de plus, indépendamment des actions du sujet. Ces actions peuvent simplement se combiner à des dynamiques externes (exemple : les ordres de barre se combinent au vent et au courant pour résulter en une trajectoire de navire). Elles peuvent aussi infléchir l'action d'automatismes (exemple : le changement d'une consigne d'épaisseur va conduire à transformer un produit sous l'effet des nombreuses opérations automatisées d'un laminoir).
Une installation industrielle automatisée s'organise autour de quelques modules principaux prenant en charge différentes parties essentielles de l'automatisation. (Jean-Marc Charte)

Le système du supervision doit remplir une fonction hybride de pilotage et de surveillance (dans les situations spéciales comme la reprise après incident, la maintenance, la préparation d'un démarrage, un arrêt...).

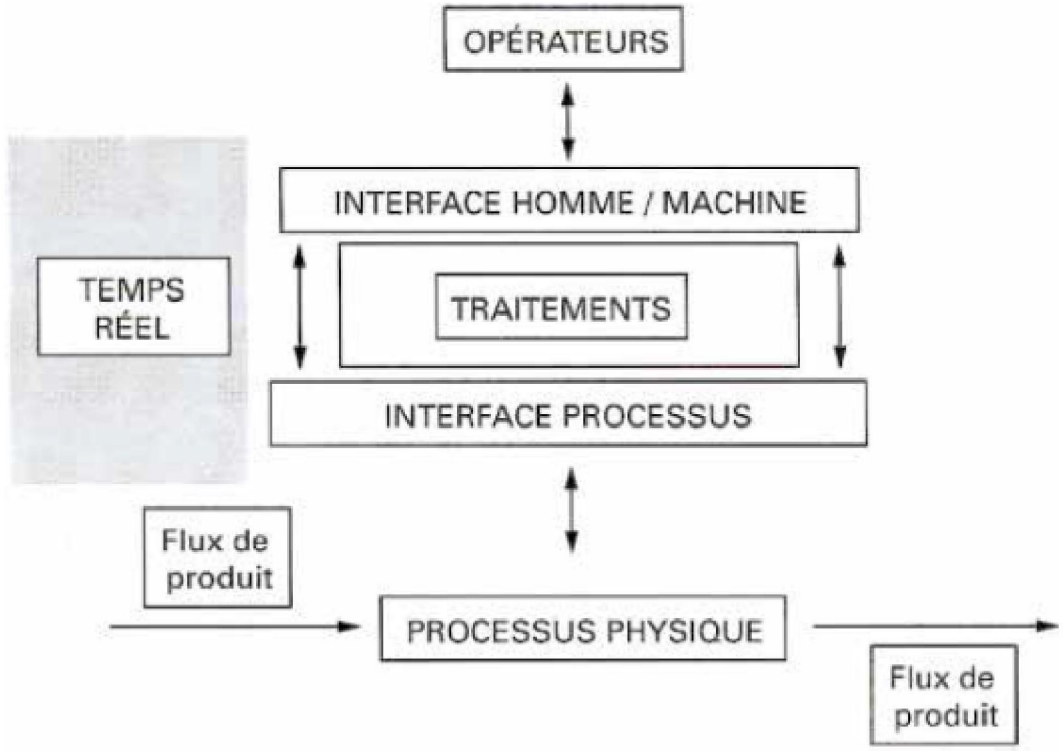


Figure III.1 : Organisation globale d'un système automatisé.

Un superviseur est souvent constitué :

- d'un module d'acquisition et de traitement des signaux physiques du procédé.
- d'un module de commande temps réel qui élabore les commandes en fonction des consignes, des signaux acquis et selon des modèles de commande prédéfinis
- d'un module de contrôle qui permet de surveiller la commande, l'évolution du procédé, de déclencher des procédures de sécurité (arrêts d'urgence) ou de prévenir l'opérateur d'une situation anormale.
- d'un module de visualisation-stockage, qui permet d'obtenir et de mettre à la disposition des opérateurs des éléments d'évaluation du procédé par ses valeurs instantanées et historiques.

III.3. Caractéristiques principales d'un système de supervision

En situation normale, le système de supervision présente, sur les synoptiques, une ou plusieurs vues de synthèse sur le système industriel, et une ou plusieurs vues spécialisées sur la phase de l'activité principale en cours et sur les éléments du système concerné.

Les modules de contrôle du système automatisé génèrent des alarmes selon une hiérarchie propre à chaque système. Un journal enregistre tous les événements significatifs survenus sur le système pendant que les écrans de contrôle de l'opérateur retransmettent les alarmes. Le degré d'élaboration de ces alarmes dépend beaucoup des systèmes et de l'effort de modélisation préalable à l'automatisation du système.

En dernier lieu, l'opérateur reste seul devant son système et, s'il dispose théoriquement de tous les éléments pour agir, en pratique il est facilement débordé par la quantité d'informations qui se présente à lui. Les éléments explicatifs présentés font souvent référence à des modèles qu'il connaît peu ou pas, et la surcharge mentale l'amène à prendre ses décisions sur des références qui lui ont personnelles et qui, en cas de non-adaptation à la situation réelle, peuvent engendrer des dangers.

La difficulté consiste à prendre en compte le temps et la dynamique propre du procédé dans les situations que l'opérateur doit gérer. Les événements sont en effet projetés sur la situation présente et l'effet de série n'est pas facile à prendre en compte par l'opérateur. Dans le contexte de la supervision globale, les données sont de natures extrêmement variées : imprécises (bruit), incomplètes (capteurs en défaut), hétérogènes, dépendant du contexte (régimes permanents, transitoires...) ; l'aide à l'opérateur nécessite d'assurer des tâches de diagnostic, d'interprétation et de planification d'actions.

Par ailleurs, la communication homme-machine doit être particulièrement étudiée pour rendre efficace l'interaction entre le système d'aide à la supervision et l'opérateur. Si le problème du rôle de l'opérateur n'est jamais négligé dans la conduite des procédés continus, où cet opérateur agit par des réglages nécessaires pour répondre à la variation des produits en entrée du système, il est souvent limité dans le domaine des systèmes à événements discrets et peu analysé dans les fonctions de supervision des systèmes complexes.

L'opérateur assure lui-même la fonction de supervision pour ce qui concerne l'interprétation des informations proposées. Par contre, les interfaces multimédias offrent des possibilités d'expression efficace des informations qui facilite la rapidité de prise en compte et limite les erreurs de lecture. (Jean-Marc Charte)

Nous pouvons repérer au moins quatre classes différentes dans les projets de supervision comme montré sur le tableau suivant:

Code	Champs d'application	Intégration	Commentaire
A	Actionneurs	La supervision est liée aux équipements	Visualisation de voyants, afficheurs.IHM
B	Système de contrôle	Mapping (représentation graphique) des informations	Système de collecte d'informations connectées sur les entrées-sorties du système de contrôle-commande
C	Systèmes de contrôle et de commande	La supervision est une extension des fonctions de contrôle du système	Partie intégrante du système, le module de supervision partage les informations des autres modules de commande et de contrôle. Les approches intégrant la sûreté de fonctionnement comme critère de contrôle et commande choisissent souvent ce type d'intégration.
D	Systèmes automatisés et systèmes de contrôle commande	La supervision est un module stratégique coopérant avec les différents systèmes de contrôle	La supervision se situe à un niveau supérieur dans la hiérarchie des systèmes d'information. Elle introduit des niveaux de redondance dans la collecte d'informations. Système complexe et comportant beaucoup de points, nécessite souvent un système d'AIDE

Tableau III.1 : Les classes des systèmes de supervision.

III.4. Les composants matériels de base d'une supervision industrielle

- **Le réseau de communication :** Le choix de réseau dépend fortement de la compatibilité des équipements à superviser le Modbus TCP/IP est le plus répondu, il permet à deux ou plusieurs équipements de communiquer entre eux. Sur un réseau Modbus TCP/IP, un équipement peut être une automate programmable, un HMI, un variateur de vitesse, un compteur, un régulateur …

Figure III.2 : module de connexion Modbus TCP/RTU.

- **Les cartes réseaux :** Les cartes réseaux concernent les automates, les relais de protection, lesordinateur.sur les ordinateurs, les carte réseaux classique RJ45 permettent souvent de pouvoir directement communiquer.par contre, certaines applications prouvent utiliser des cartes spécifiques du fait du protocole qui est utilise. Sur les automates certains fournisseurs proposent des ports natifs (à étudier au cas par cas la nécessité d'avoir une carte dédiée). Sur les régulateurs et les centrales de mesures, les ports de communication y sont souvent disponibles.

Figure III. 3 : Exemple de carte réseau industriel

✓ **Base de données :** La base de donnes du superviseur contient les informations concernant les divers automatismes, c'en est donc l'élément centrale, et il faut connaitre le nombre et le type de variable qu'elle peut memoriser.ces variable peuvent être:

- Tout ou Rien(TOR), représenté par un bit unique 0 ou1.
- Analogique, représenté par un nombre de bits prédéfini.
- Des chaines de caractères, également codées suivant un formatage (nombre de bits) prédéterminé.

✓ **Les postes de supervision et application de supervision :** Le poste de supervision peut être un ordinateur de type PC Windows avec l'application de supervision installée et configurée en mode Run Time. En générale, une supervision d'un superviseur permet de développer le programme Run Time de supervision. selon les superviseurs, le programme Run Time aura besoin d'une licence pour fonctionner.

III.5. Interface homme-machine (IHM)

Avec la complexité de processus industriels a automatisé le dialogue entre les operateurs de production et de maintenance s'avère plus que nécessaire et les contraintes d'enregistrements et de command de procédés apparaissent. Un système IHM constitue l'interface entre l'homme (operateur) et le processus (machine/installation). le contrôle proprement dit du processus est assure par le système d'automatisation. Un système IHM est charge des tache suivantes:

✓ **Animation graphique des objets :** Le processus est représenté sur le pupitre opérateur. Lorsqu'un état du processus évolue par exemple l'affichage du pupitre opérateur est mis à jour. Cette figure ci –dessous présente un exemple d'une vue de supervision sur une station de production de l'air froid et chaud :

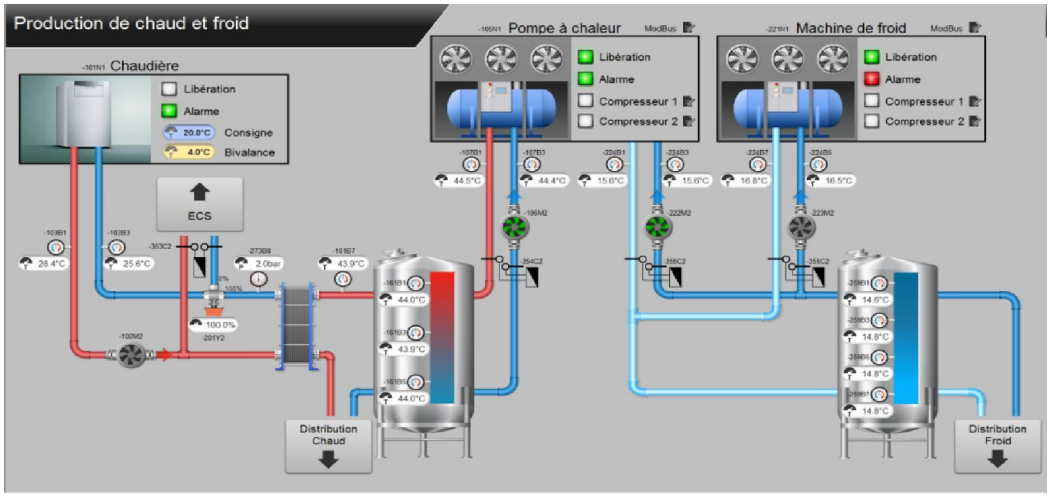


Figure III.4 : Vue générale de la production d'air froid et chaud.

On peut voir sur cette vue :

- Une palette de boutons vers le bas pour l'accès aux déférents autres vues.
- Les objets graphiques des boutons de commande.

L'animation graphique des objets est à la base de toute application de supervision. Les objets sont de 2 grands types :

- Les symboles de la bibliothèque de base (symboles disponibles à l'installation du superviseur).
- Les symboles créés par l'utilisateur.

En général, pour les symboles de la bibliothèque, les animations sont déjà programmées et il suffit juste d'associer la variable d'équipement qui pilote le symbole.

Considérons par exemple un voyant de la bibliothèque de base d'un superviseur.

Le voyant peut prendre 2 états représentés par une couleur :

- Couleur rouge pour l'état 1.
- Couleur verte pour l'état 0.

La configuration de ce symbole sur l'écran consiste à définir la variation booléenne pour qu'en cours d'exécution, les différents états soient mis à jour en fonction de l'état de la variable. Les symboles créés par l'utilisateur peuvent être animés de plusieurs manières. Les animations peuvent être sur couleur, sur remplissage de couleur, de changement de symbole etc. Par exemple un barre-graphe qui permet de visualiser l'état d'une grandeur analogique.

- ✓ Commande du processus

L'opérateur peut commander le processus via l'interface utilisateur graphique. Il peut par exemple démarrer un moteur.

- ✓ Vue des alarmes

Lorsque surviennent des états critiques dans le processus, une alarme est

Immédiatement déclenchée, par exemple lorsque la valeur limite est franchie.

- ✓ Archivage de valeurs processus et d'alarmes

Les alarmes et valeurs processus peuvent être archivées par le système IHM. Nous pouvons ainsi documenter la marche du processus et accéder ultérieurement aux données de la production écoulée.

- ✓ Documentation de valeurs processus et d'alarmes

Les alarmes et valeurs processus peuvent être éditées par le système IHM sous forme de journal.

- ✓ Gestion des paramètres de processus et de machine

Les paramètres du processus et des machines peuvent être enregistrés au sein du système IHM dans des recettes. Ces paramètres sont alors transférables en une seule opération sur l'automate pour démarrer la production d'une variante du produit.

✓ **Les boutons de commande** : Les boutons de commande permettent de passer des ordres (écriture des variables dans les mémoires des équipements industriels) ou de donner à l'application des fonctions de navigation (ouverture des vues spécifique par exemple, passage d'une vue à une autre). Les boutons peuvent être de plusieurs formes comme le montre la figure suivante :

Figure III.5 : Différentes formes de boutons dans une application de supervision.

✓ **Les faceplates** : Il est d'usage dans les applications de supervision de définir pour des éléments de commande standards des faceplates. Le faceplates est un groupe d'objets permettant d'afficher des informations d'état d'un équipement et des informations de commande. Pour un régulateur par exemple, le faceplates peut afficher :

- La valeur de la consigne.
- La valeur de la sortie du régulateur.
- La valeur de la mesure.
- Les modes de marche du régulateur.

Figure III.6: Exemple d'un faceplate d'un régulateur.

- ✓ **Les alarmes :** les alarmes sont des messages transmis par le superviseur en phase exploitation permettant d'attirer l'attention des opérateurs sur les modifications d'actions de variable de mesure, etc.
- ✓ **La mise en ouvre d'une application de supervision :**

- Configuration de la communication avec les équipements à superviser.
- Création de la table d'échange encore appelée tables des variables.
- Création des blocs-types ou faceplate qui sont utilisé dans l'application.
- Création des vue de supervision.
- Configuration des droits des utilisateurs.
- Paramétrage des alarmes.
- Paramétrage des courbes de tendance.
- Teste et débogage.

Conclusion

La prolifération d'informations et la nécessité d'être en permanence capable de décider, voire d'anticiper, exige une supervision pertinente. Celle-ci doit se faire autour du schéma général de l'activité de l'opérateur. La flexibilité globale s'applique aussi aux systèmes d'information, qui devront être facilement modifiables, pour s'adapter au mieux aux situations nouvelles.

Introduction

Actuellement, réduire les coûts de maintenance est de plus en plus important dans l'industrie. C'est la raison pour laquelle les machines non seulement rendent service sur le lieu, mais aussi à distance. Ce type d'opération qui semble à première vue caractéristique d'une démarche gagnant-gagnant, pose aux deux partenaires des questions cruciales en termes de sécurité informatique.

IV.1. Définition

La télémaintenance est une technologie de prise de contrôle à distance d'un serveur ou d'autre équipements informatique à l'aide l'un logiciel afin d'apporter une assistance technique à son utilisateur, à diagnostiquer une panne logicielle ou matérielle. Il utilise le plus souvent le protocole TCP/IP. Le technicien opérant en télémaintenance peut intervenir sur le serveur distant sans y être physiquement présent. Cette technique peut aussi être utilisée sur un réseau local.

IV.2. Les avantages de la télémaintenance

La télémaintenance consiste à accéder à un équipement distant, généralement au travers d'Internet, pour pouvoir y réaliser des manipulations d'ordre technique (reprogrammation totale d'un automate, modification de paramètres…).

Les principaux avantages de la télémaintenance sont :

- Les coûts : réduction des coûts de maintenance liés au transport d'un technicien chez le client distant mais également ses frais de service.
- La réactivité : pouvoir agir à l'autre bout de la planète en temps réel, sans se déplacer.
- La satisfaction du client d'avoir été dépanné « en temps réel ».

IV.3. Les risques d'une télémaintenance non sécurisée

La télémaintenance nécessite de faire la réparation au travers d'une connexion à distance (internet) pour accéder au réseau interne de l'entreprise. Cela implique donc des risques de sécurité pour l'entreprise demandant la réparation.

- **Risque lié à l'intrusion d'un pirate**

Via une connexion à distance, la télémaintenance ouvre une « porte » dans le

réseau interne de l'entreprise. Si le processus n'est pas sécurisé, il est possible qu'un pirate informatique profite de cette ouverture pour accéder au réseau de l'entreprise et donc aux informations et aux données.

Il existe également un risque lors de l'échange de données entre le terminal de l'entreprise et celui du responsable informatique. Si le transfert n'est pas sécurisé, un pirate peut surveiller le trafic et intercepter des données confidentielles et donc accéder ensuite aux documents de l'entreprise.

Il est par ailleurs judicieux d'activer et d'enregistrer les journaux d'évènements au niveau du routeur d'accès afin de garder le contrôle sur les tentatives d'accès extérieures.

- **Risque lié au « Bureau à distance »**

Pour prendre le contrôle à distance d'un terminal, il est possible d'utiliser l'outil « Bureau à distance » de Windows. Cependant, cet outil est très vulnérable et ne complique pas la tâche à un pirate voulant s'introduire dans le réseau interne d'une entreprise.

La désactivation du « Bureau à distance » est conseillée afin de limiter les risques d'intrusion. Pour procéder à la prise de contrôle à distance, il est préférable d'opter pour un outil qui fonctionne uniquement après avoir été lancé par une personne de l'entreprise. La mise en route de l'outil peut également être protégée par un mot de passe.

- **Risque lié à une maintenance externalisée**

Dans le cas où la télémaintenance est effectuée par un prestataire extérieur, ce dernier a la possibilité de se connecter quand il le souhaite. Cette situation est source de problèmes pour l'entreprise, notamment lorsque le prestataire programme une mise à jour sans en avoir référé auparavant à l'entreprise.

Pour éviter cette perte de contrôle sur les interventions extérieures, il est important de bien déterminer le périmètre d'intervention ainsi que les objectifs à atteindre. Les règles liées à l'intervention seront consignées dans le contrat de maintenance. Parmi ces contraintes, on pourra retrouver :

- ✓ Pas d'opération de télémaintenance sans accord préalable de l'entreprise.
- ✓ L'entreprise doit être informée avant le processus des inconvénients (redémarrage,

indisponibilité, …) dus à l'intervention

- ✓ L'intervention sera consignée dans un compte-rendu détaillé.
- ✓ Les échanges entre le prestataire et l'entreprise seront cryptés afin de garantir la confidentialité des informations.

IV.4 : Solution de télémaintenance TeamViewer

Pouvoir assister, dépanner ou bien intervenir sur une machine sans se déplacer et dans un délai très rapide, c'est possible grâce à une solution de télémaintenance. Il existe plusieurs logiciels de télémaintenance (Teamviewer , Logmein Rescue, ShowMyPC, Crossloop , UltraVNC, Gotoassist, Spark-Angels.)[1] .

Selon l'avis d'utilisateurs (note de bas de page 1), TeamViewer reste une excellente solution[2].

On peut aussi utiliser la maintenance assistée par Vidéo VAM (Video-Assisted Maintenance) où un expert guide un technicien sur site à travers une vidéo pour l'aider à intervenir sur le procédé. https://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9maintenance

V.4.1 : Présentation de Team Viewer

TeamViewer est une application intuitive, rapide et sûre, destinée au contrôle à distance et aux réunions. En tant que solution tout en un, Team Viewer peut être utilisé pour les applications suivantes:

- ✓ Proposer à des clients, collègues et amis une assistance à distance immédiate.
- ✓ Administrer les serveurs et postes de travail Windows. Vous pouvez exécuter Team Viewer comme service système Windows. Cela permet d'accéder à un ordinateur avant même de connecter à Windows.
- ✓ Connecter à d'autres plateformes comme Linux.
- ✓ Connecter depuis des périphériques mobiles Android à des ordinateurs Windows ou Linux.

[1] Voir ces références : https://www.generation-nt.com/assistaer-article-50005-7.html https://www.tech2tech.fr/assistance-a-distance-quel-logiciel-utiliser/

[2] **Spark-Angels & Crossloop** permettent de trouver facilement des clients pour des dépannages à distance en proposant votre savoir-fairence-a-distance-telemaintenance-prise-controle-logmein-pcvisit-ntr-support-ultravnc-pchelpware-teamview

- ✓ Partager le bureau pour les réunions, les présentations ou le travail en équipe.
- ✓ Connecter à un ordinateur à domicile.
- ✓ Connecter à l'ordinateur au travail de n' importe où dans le monde

IV.4.2: Comment TeamViewer fonctionne ?

Si on considère une connexion Team Viewer comme un appel téléphonique, l'ID (Identifiant) Team Viewer est le numéro de téléphone auquel tous les clients Team Viewer peuvent être joints séparément. Les ordinateurs et appareils mobiles qui exécutent Team Viewer sont identifiés par un ID global unique. L'ID est automatiquement généré au premier démarrage de l'application, sur la base des caractéristiques matérielles et ne change pas par la suite. Toutes les connexions Team Viewer sont hautement cryptées et ainsi protégées de tout accès par des tiers.

IV.5 : Description de la fenêtre principale de TeamViewer

La fenêtre principale de Team Viewer se divise en deux onglets: Contrôle à distance et Réunion

Figure IV.1 : La fenêtre principale de TeamViewer.

IV.5.1 : L'onglet de contrôle à distance

L'onglet Contrôle à distance se divise dans les deux zones suivantes:

a. Autoriser le contrôle à distance

Dans cette zone, on trouve l'identifiant Team Viewer et le mot de passe temporaire. Si vous Partagez cette information avec le partenaire, il ou elle pourra se connecter à votre ordinateur. En cliquant sur le symbole  dans le champ Mot de passe, fait apparaître un menu contextuel pour modifier le mot de passe aléatoire ou pour le copier dans le presse-papier (fonction Copier & coller de Windows). En plus, on peut définir un mot de passe personnel.

b. Contrôler un ordinateur distant

Pour contrôler un ordinateur à distance, il faut entrer son ID dans la liste déroulante ID du partenaire. Par ailleurs différents modes de connexion sont disponibles:

- **Contrôle à distance:** Contrôler l'ordinateur du partenaire ou travailler ensemble sur un seul ordinateur.
- **Transfert de fichiers:** Transférer des fichiers depuis ou vers l'ordinateur du partenaire.
- **VPN:** Création d'un réseau virtuel privé avec le partenaire.

IV.5.2 : La barre de menu de la fenêtre principale de TeamViewer

La barre de menu se trouve sur le bord supérieur de la fenêtre principale de Team Viewer et contient les rubriques de menu Connexion, Suppléments et Aide.

a. Connexion

Le menu Connexion propose les options suivantes:

- Pour inviter quelqu'un à une session Team Viewer, cliquez sur Inviter un partenaire**.**
- Pour configurer le démarrage automatique de Team Viewer avec Windows (service système), cliquez sur Installation accès non surveillé**.**
- Pour ouvrir la Team Viewer Management Console, cliquez sur Ouvrir la Management Console.
- Pour quitter Team Viewer, cliquez sur Quitter Team Viewer.

b. Suppléments

Le menu Suppléments contient les options suivantes:

- Pour lire ou convertir les vidéos des sessions Team Viewer enregistrées cliquer sur ***Lire ou convertir la session enregistrée.***
- Pour recommander Team Viewer à d'autres personnes, cliquez sur Parlez-en à un ami.
- Pour accéder aux fichiers journaux créés par Team Viewer (en particulier si l'équipe de support de Team Viewer en a besoin pour des questions d'analyse), cliquez sur Ouvrir les fichiers journaux.
- Pour activer la clé de licence sur cet ordinateur, cliquez sur Activer une licence

c. Aide

Le menu ***Aide*** contient les options suivantes:

- pour l'aide, cliquer sur ***Assistance TeamViewer (Web)***.
- Pour ouvrir le site Web Team Viewer, cliquer sur ***Site Web Team Viewer***.
- Pour donner votre avis sur Team Viewer, cliquez sur ***Donnez votre avis***.
- Pour vérifier que vous avez la dernière version de TeamViewer, cliquer sur ***Vérifier les mises à jour***.
- Pour obtenir des informations sur Team Viewer et la licence, cliquer sur ***À propos de***.

IV.6 : Etablir une connexion TeamViewer

Pour se connecter à un partenaire pour une session de contrôle à distance, suivez les étapes ci-dessous:

1. Démarrez Team Viewer sur l'ordinateur
2. Cliquez sur l'onglet ***Contrôle à distance***.
3. Demandez au partenaire de démarrer la version complète de TeamViewer.
4. Demandez au partenaire son ID Team Viewer et son mot de passe.
5. Entrer l'ID du partenaire dans la liste déroulante ***ID du partenaire***.
6. Cliquez sur la case d'option ***Contrôle à distance***.
7. Cliquez sur le bouton ***Connexion à un partenaire***.
   - La boîte de dialogue **Authentification Team Viewer** s'ouvre.
8. Entrez le mot de passe de l'ordinateur distant.
9. Cliquez sur ***Connexion***.
10. Connexion établie avec l'ordinateur du partenaire.

IV.7 : Le mode de connexion VPN

Le mode de connexion ***VPN*** permet de créer un réseau virtuel privé (VPN) entre deux ordinateurs Team Viewer. Deux ordinateurs connectés via VPN agissent dans un réseau commun. Cela permet d'accéder aux ressources de l'ordinateur du partenaire et vice versa.

IV.7.1 : Exemples d'utilisation de TeamViewer VPN

- Imprimer des documents sur une imprimante activée connectée à l'ordinateur distant.
- Exécuter des applications localement sur l'ordinateur qui accède à une base de données distante en établissant une connexion VPN au serveur de cette base par exemple pour la télémaintenance.
- Donner à des partenaires externes un accès à des périphériques par exemple disques durs ou clés USB connectés à l'ordinateur distant

IV.7.2 : Option de la boite de dialogue VPN

Une fois une connexion établie à l'ordinateur distant via VPN, la boîte de dialogue ***VPN-Team Viewer*** s'ouvre.

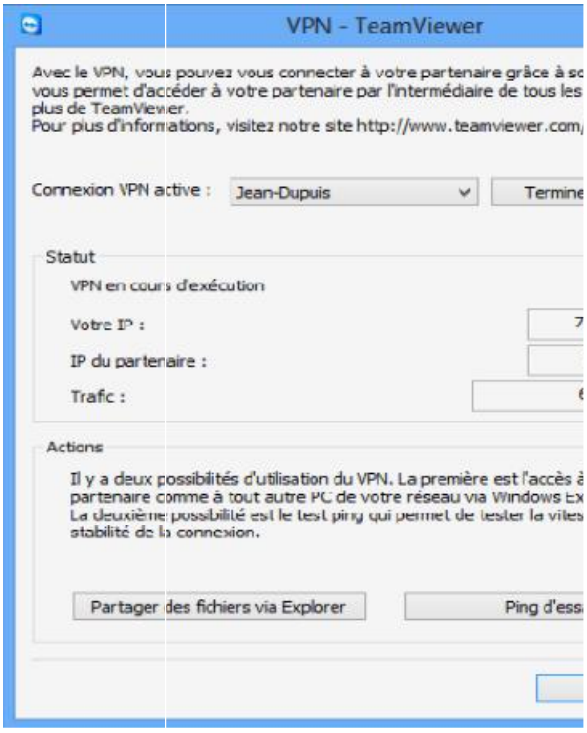


Figure IV.2 : La boite de dialogue VPN.

La fenêtre VPN de Team Viewer présente les options suivantes:

▪ En cas de connexions VPN multiples simultanées, on peut sélectionner la connexion requise dans la liste déroulante ***Connexion VPN active***. Les détails et actions disponibles pour cette connexion sont affichés dans la boîte de dialogue.

▪ La zone ***Etat*** montre les adresses IP VPN assignées des deux ordinateurs. Une fois assignée, l'adresse IP VPN reste la même. La quantité de données transmises est également affichée.

▪ Le bouton ***Partager des fichiers via Explorer*** permet d'ouvrir Windows Explorer donnant ainsi accès au système de fichiers distants. Si des dossiers sont partagés sur l'ordinateur distant via le réseau local, on peut y accéder et supprimer, copier ou déplacer les fichiers selon les besoins.

▪ Le bouton ***Ping d'essai*** envoie un signal PING à l'ordinateur distant. Cela permet de vérifier si une connexion a été établie avec succès.

Application 1 : Connexion de deux automates Maître- Esclave via Profibus DP.

IV.1.1. Partie 01: Configuration Matériel

Dans cette application nous allons connecter deux automates S7 300 de la même référence 314C-2 DP, afin de récupérer les sorties de l'automate programmable en mode "Maître", et comme entrée de l'automate programmable en mode "Esclave".

Avant d'entamer les connexions nous devons effectuer la configuration du matériel sur le logiciel Step 7. Les figures suivantes montrent les étapes à suivre :

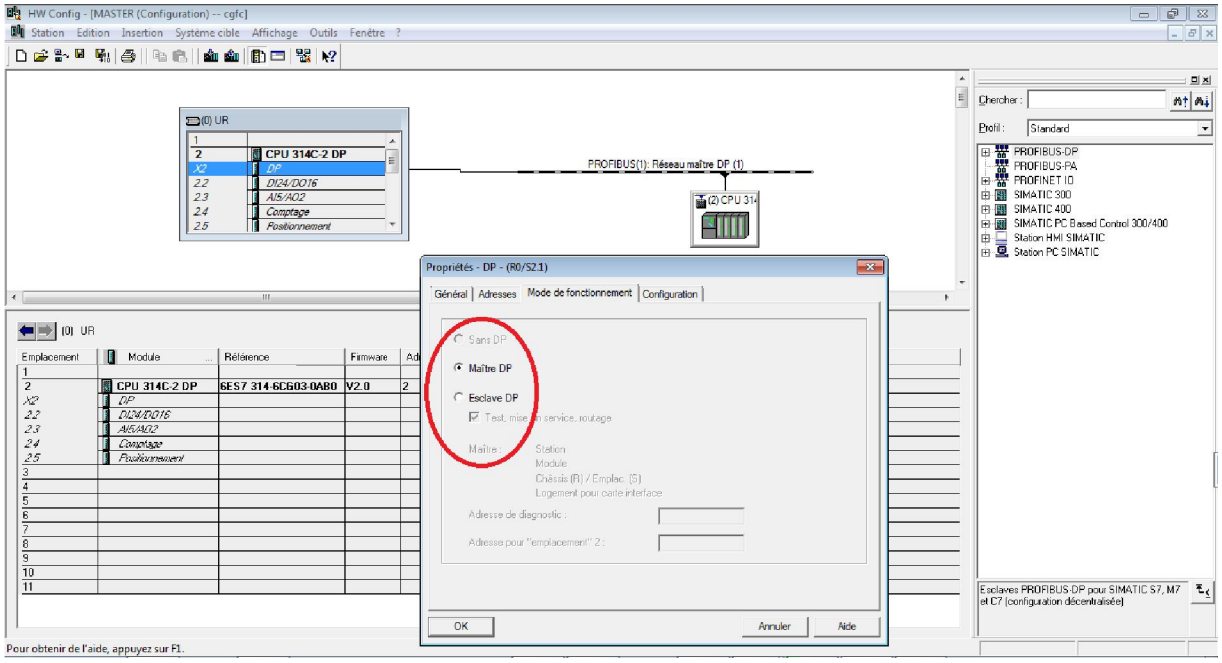


Figure IV.3: Configuration du réseau Maître.

Une fois que la référence de l'automate programmable est insérée, nous allons sélectionner le mode de fonctionnement "Maître"

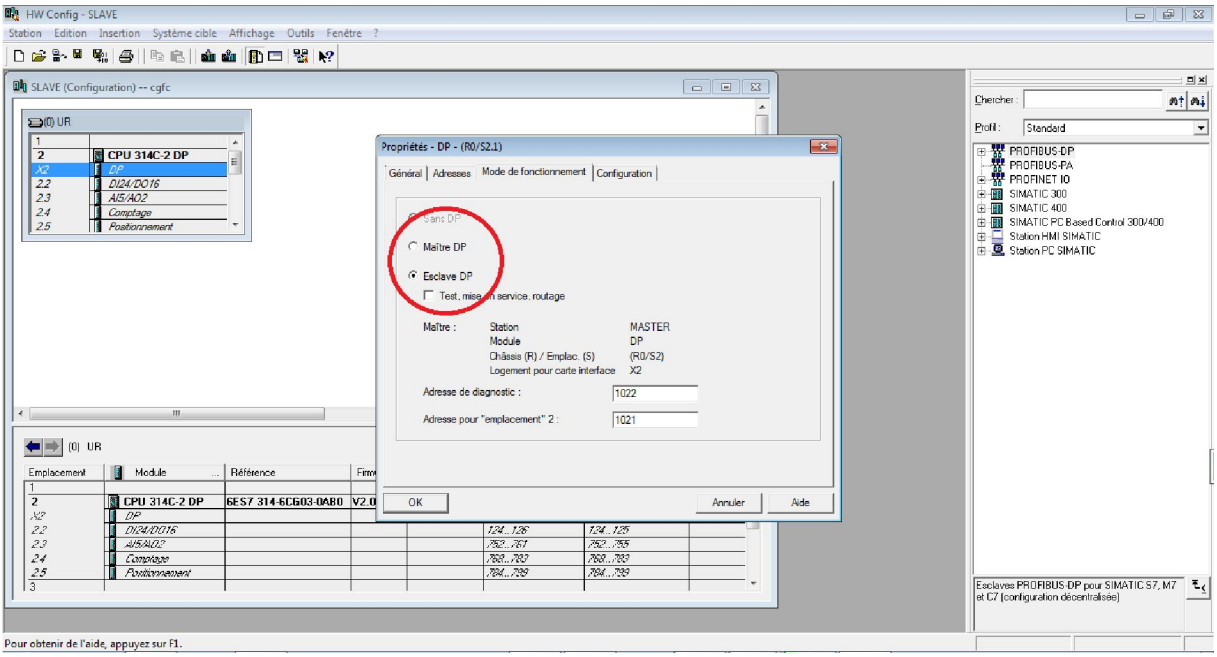


Figure IV.4 : Configuration du réseau Esclave.

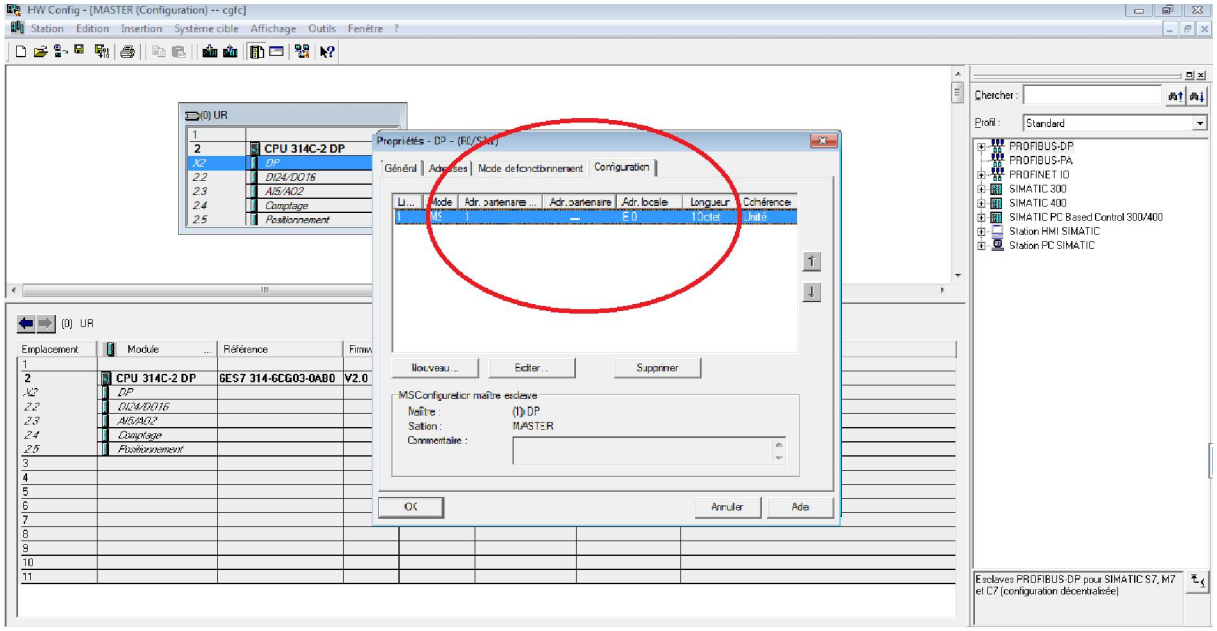


Figure IV.5: Configuration de l'Esclave.

Nous remarquons que nous disposons d'aucune adresse partenaire. Pour établir une connexion nous devons insérer une adresse du partenaire puis les coupler.

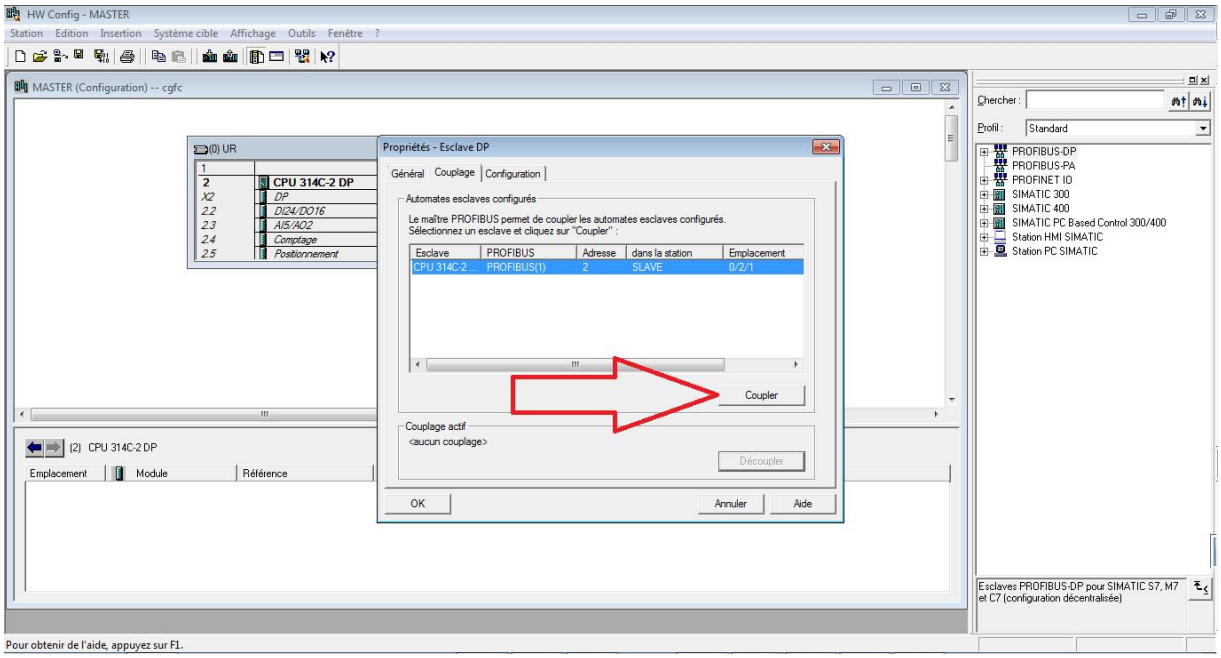


Figure IV.6: Couplage de deux stations.

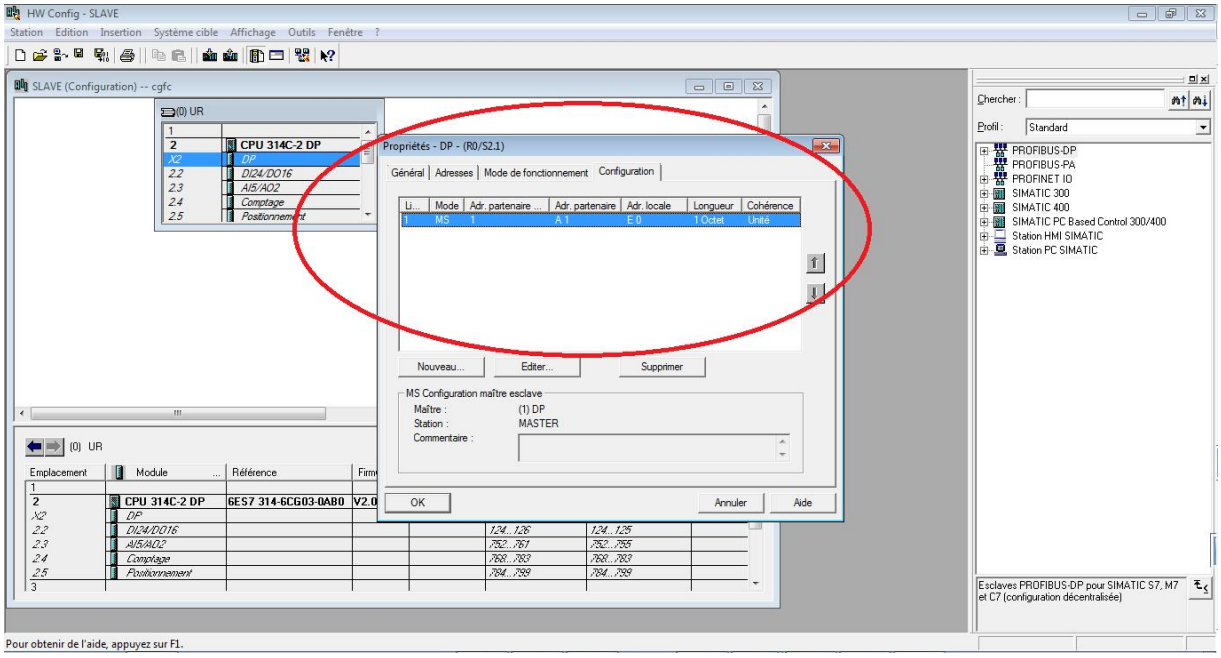


Figure IV.7: Récupération des sorties du maître comme entrées de l'esclave après couplage.

Nous pouvons vérifier la connexion sur Netpro :

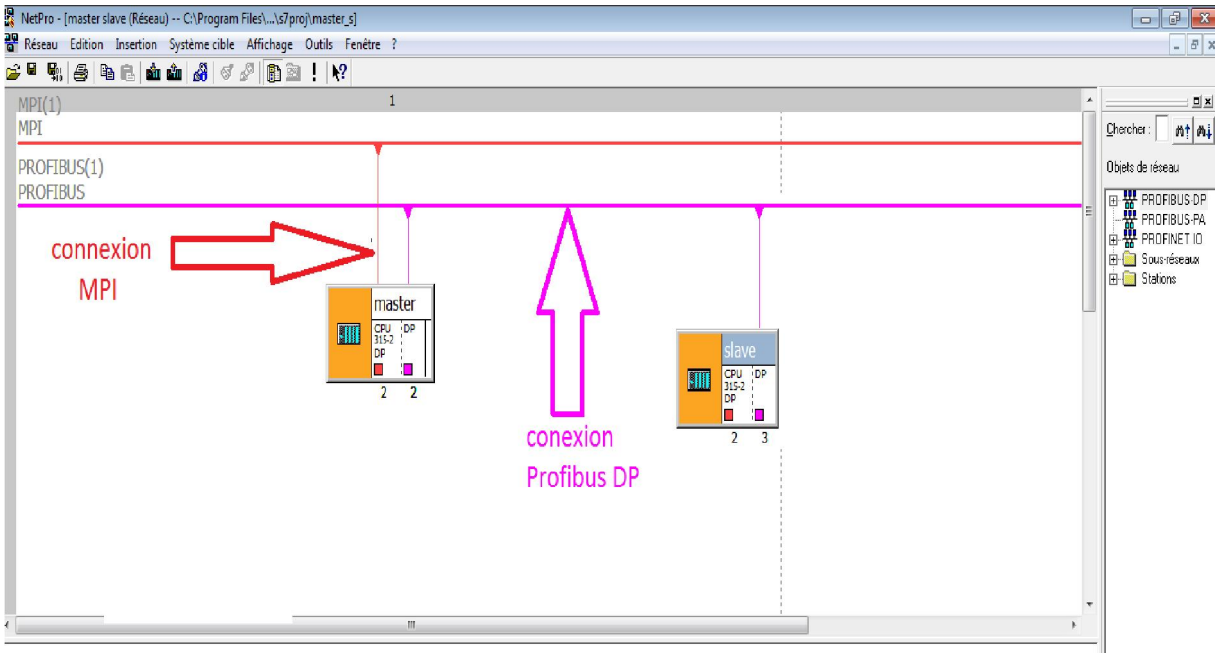


Figure IV.8 : Etablissement de la connexion sur NetPro.

IV.1.2. Partie 02 : Programmation

L'opération transfert (MOVE) permet le transfert des données. Copier que des octets, des mots ou des doubles mots.

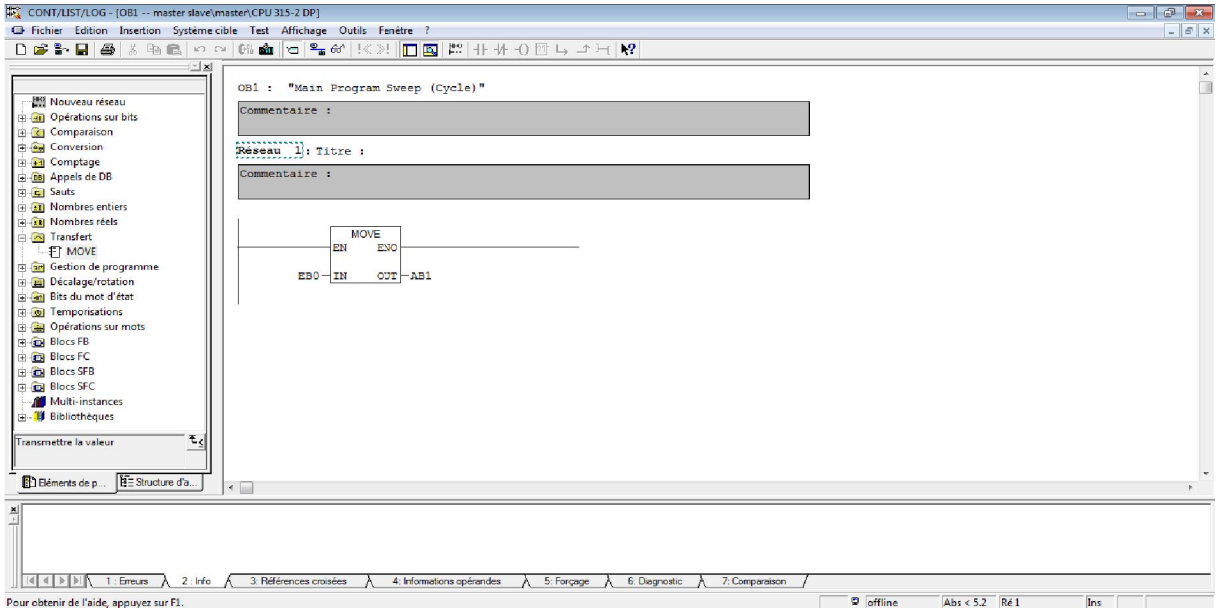


Figure IV.9: Insertion de l'opérateur MOVE dans la station Maître.

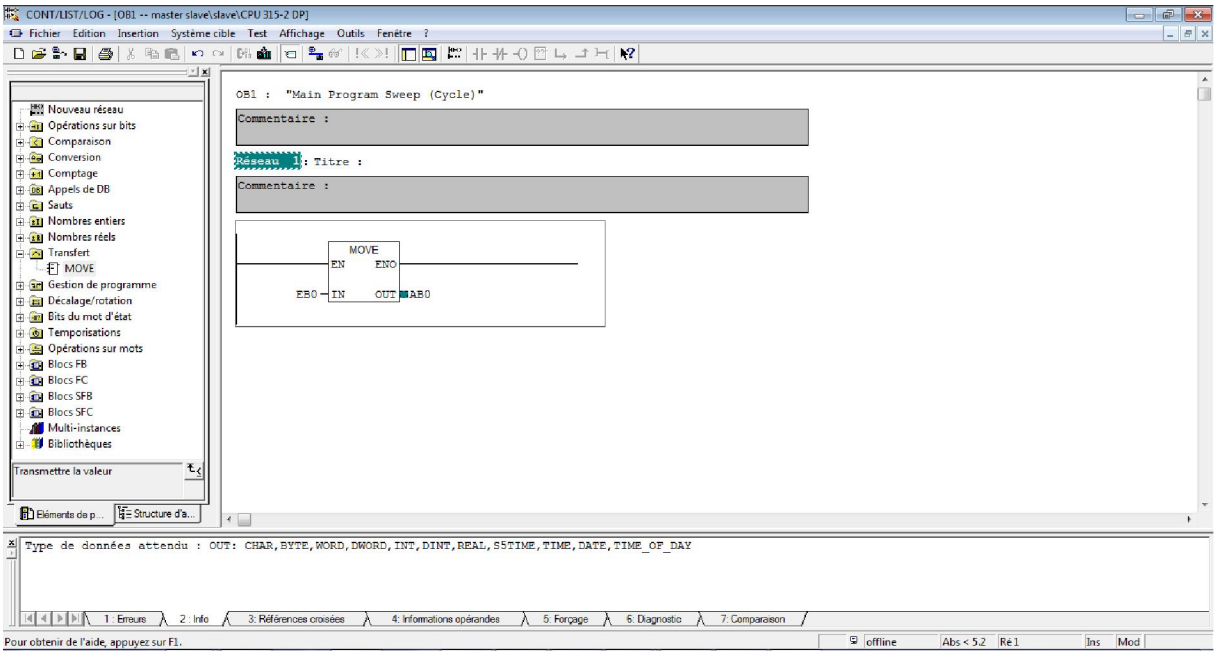


Figure IV.10 : Insertion de l'opérateur MOVE dans la station Esclave.

Après avoir réussit la programmation nous allons passer au câblage des deux stations:

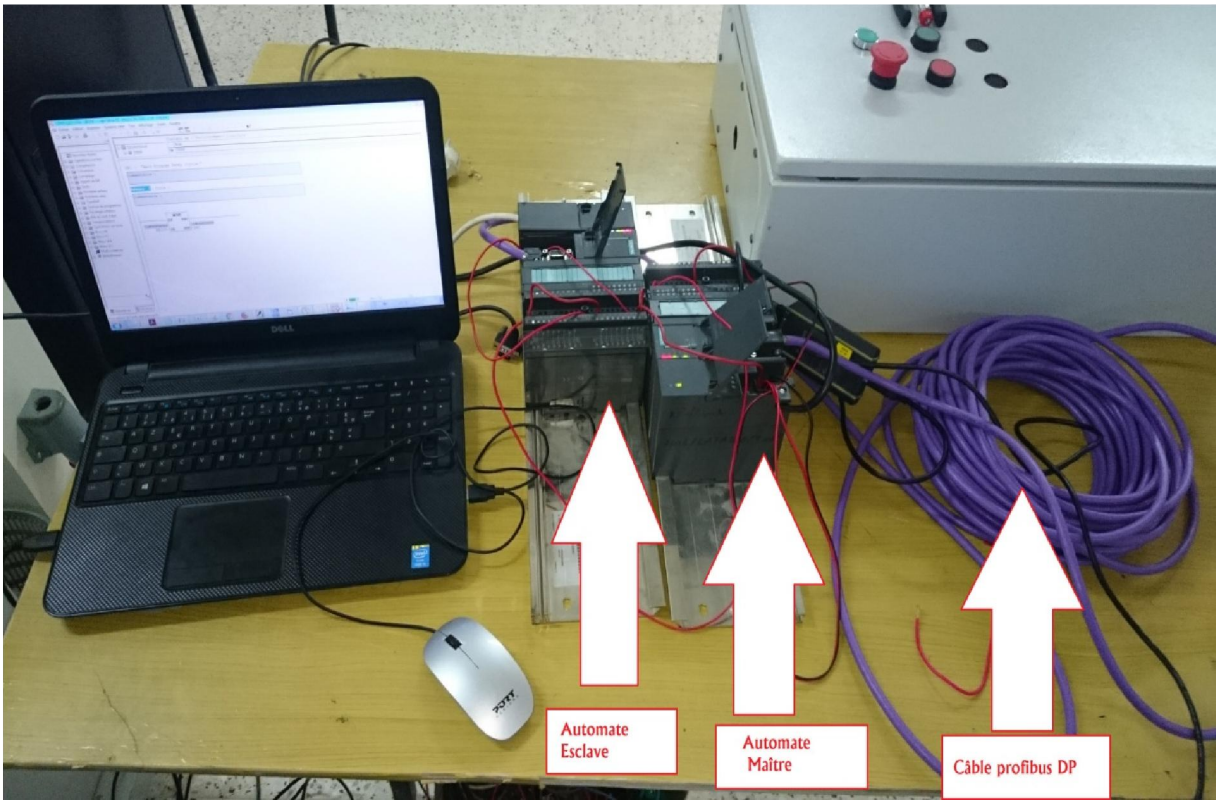


Figure IV.11: Plateforme d'essai réalisée au laboratoire LATAGE

L'excitation d'une entrée du maître nous permet de récupérer une sortie de l'esclave comme montré sur la figure suivante :

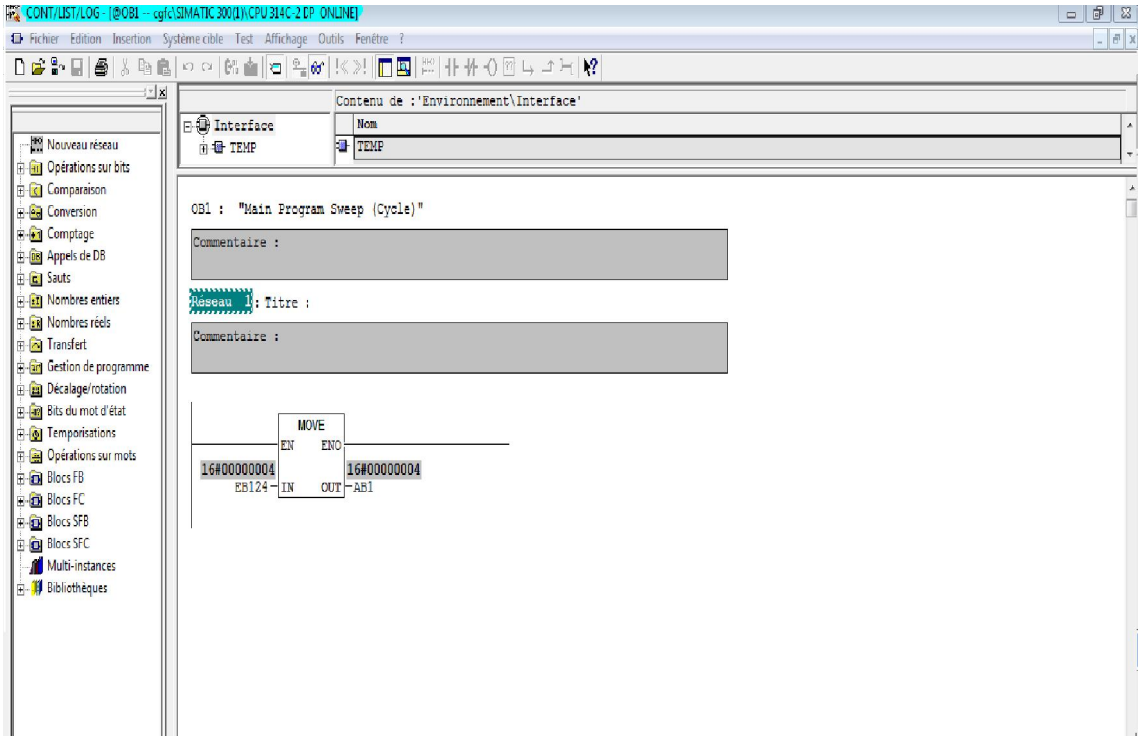


Figure: IV.12: Affichage du transfert de données.

Conclusion

Le Profibus bus permet de connecter l'ensemble de la périphérie à un contrôleur central (Maître). Les avantages sont les gains de câblage, souplesse, flexibilité dans les architectures sans oublier l'exploration de l'intelligence embarquée dans les équipements de terrain (variateur de vitesse, contrôleur de moteur ...etc.).

Application 02 : Tapis à deux sens

IV.2.1: Domaine d'utilisation de WINCC flexible

Le WINCC est logiciel qui permet la supervision des programmes et la commande des installations industrielles d'une manière facile et accessible tous. Cette commande s'effectue à travers un écran de contrôle qui sera conçu à partir du programme Step 7 qui été utilisé pour la programmation des machines. (WinCC, Avril 2009)

IV.2.2: Création station de supervision à partir de Step 7

Dans notre cas nous allons créer une station de supervision à partir du logiciel STEP 7. Avant il est demandé de configurer le matériel (pupitre, automate) et établir une connexion entre les deux équipements. Nous avons choisie la liaison Profibus DP car c'est la plus utilisée dans l'industrie en raison de sa simplicité. Les figures suivantes montrent les procédures à suivre pour la réalisation :

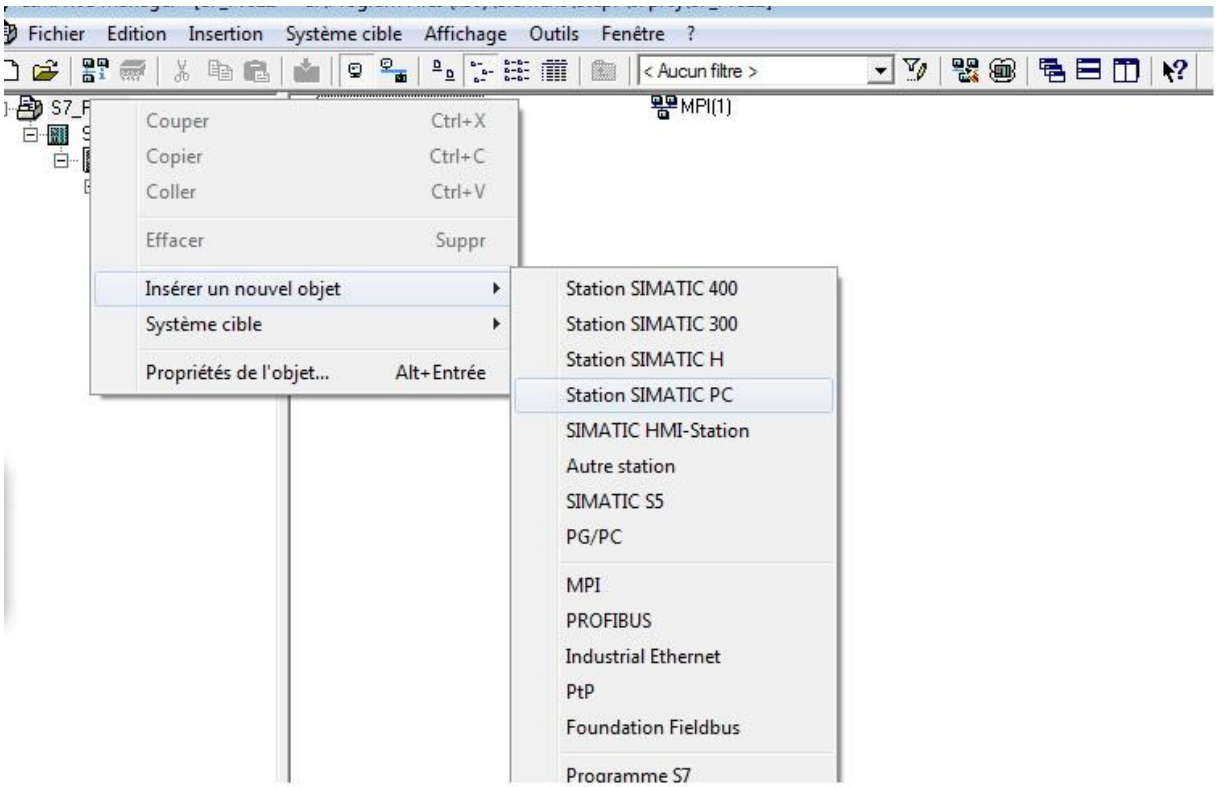


Figure IV.13 : Insertion de la station de supervision dans STEP 7.

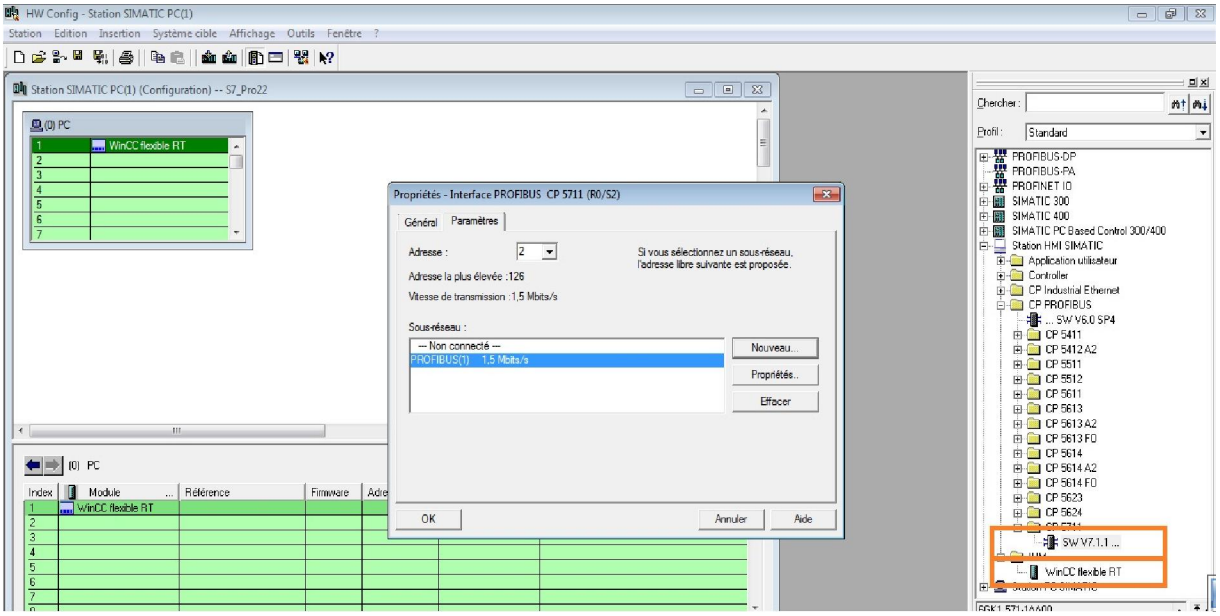


Figure IV.14: Introduire la connexion via Profibus DP.

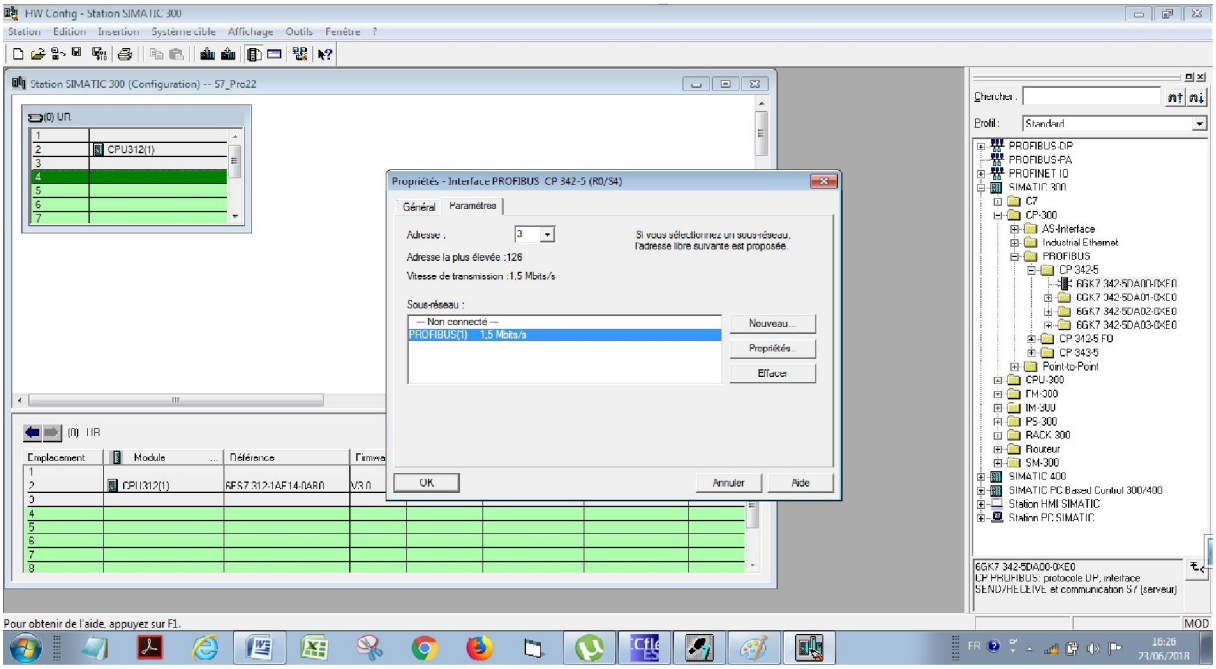


Figure IV.15: Configuration de la connexion automate et station de supervision.

NB:

Il est important de sélectionner le même réseau Profibus DP afin d'assurer l'interconnexion entre les deux stations.

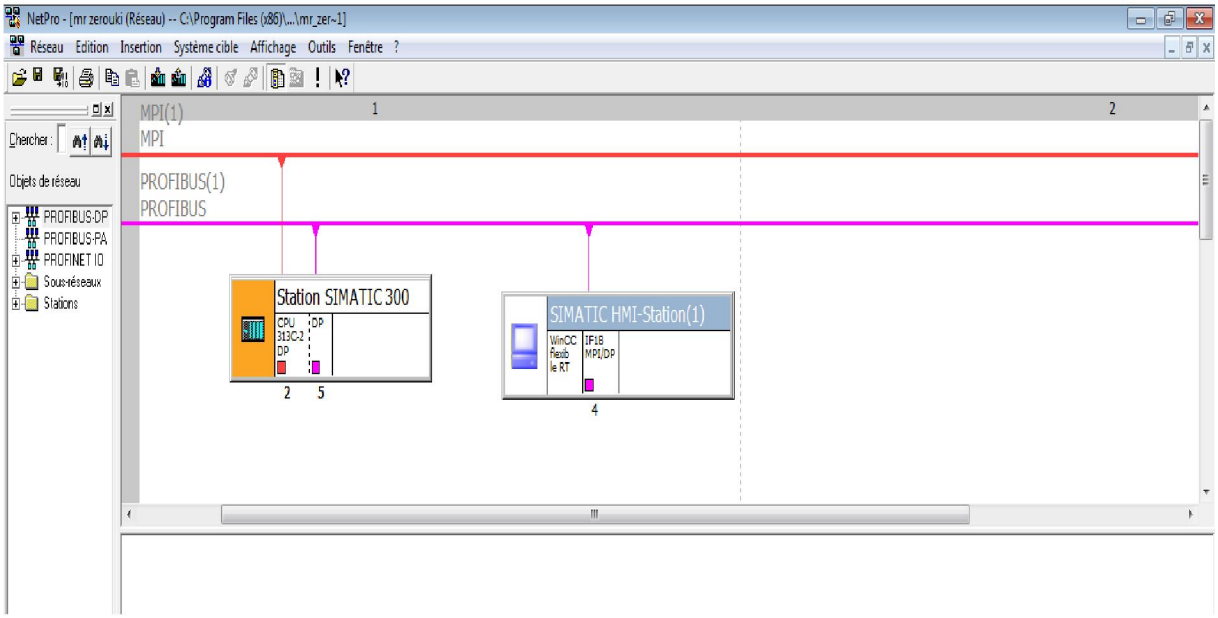


Figure IV.16: Connexion de des stations sur Netpro.

Une fois que la configuration du matériel est faite, nous allons ouvrir l'application WINCC à partir de STEP 7 et l'intégration du programme Ladder se fait automatiquement (sans passer par la procédure d'intégration). Puis activer la liaison comme le montre la figure suivante :

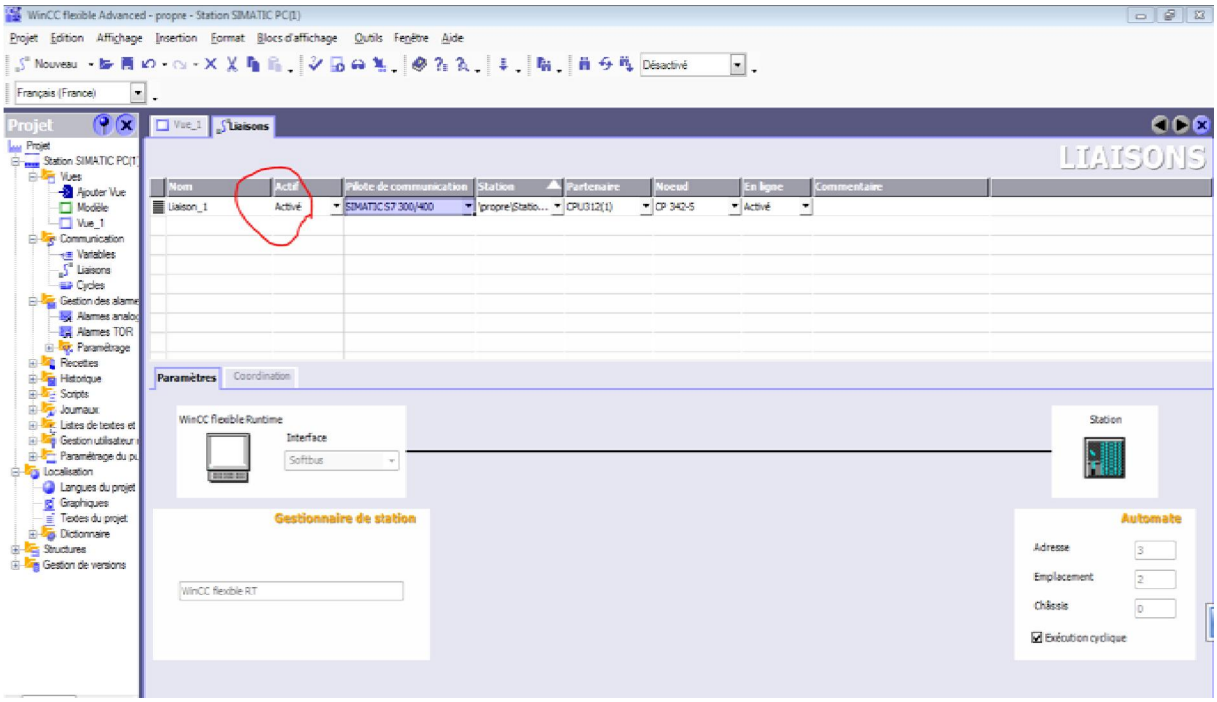


Figure IV.17: Activation de la liaison automate station de supervision.

IV.2.3. Création de la vue sur la station PC

La création des vues se fait en insérant les éléments de notre programme (moteur, bouton poussoir, alarmes...) et en leurs affiliant des adresses correspondantes comme le montre la figure suivante :

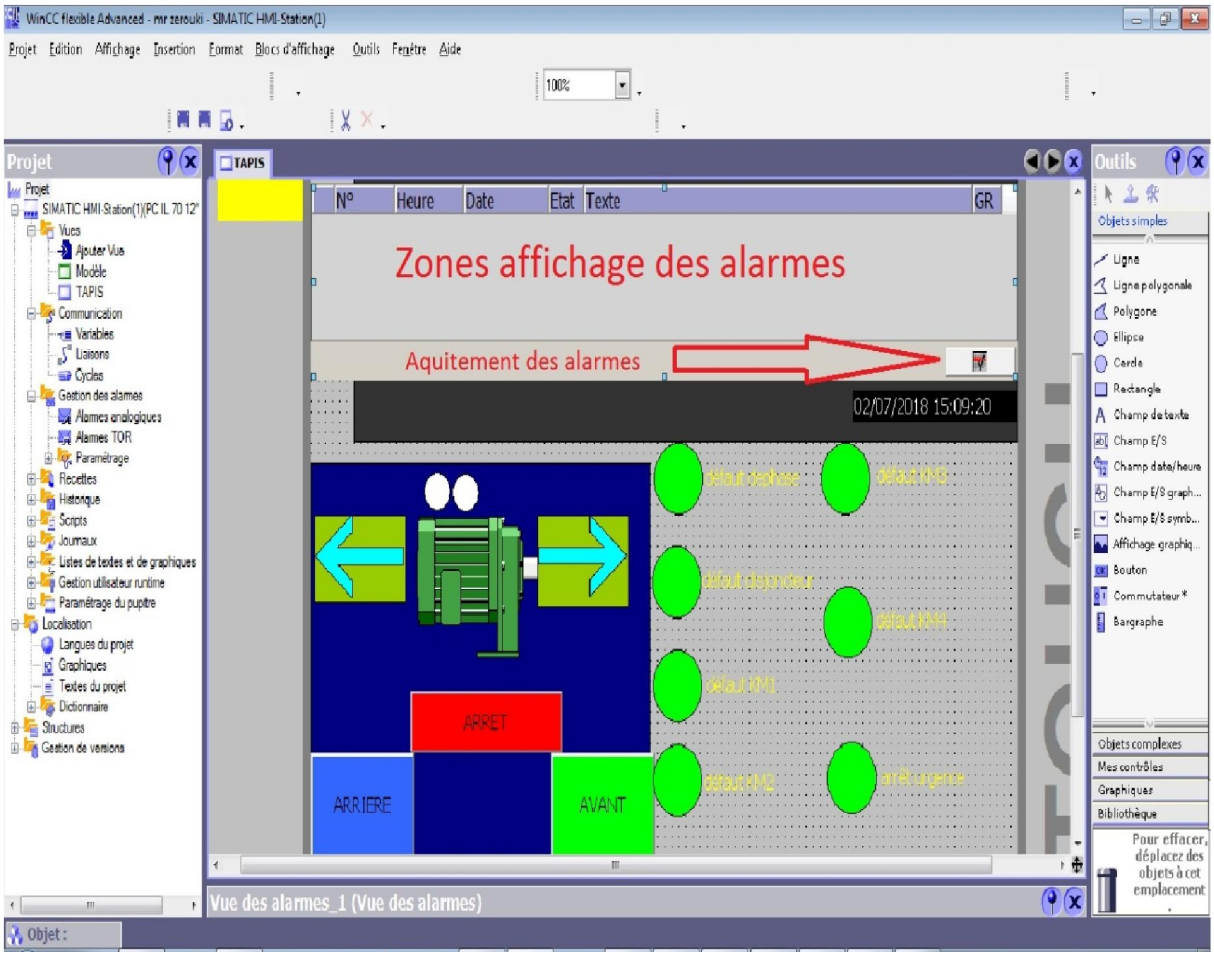
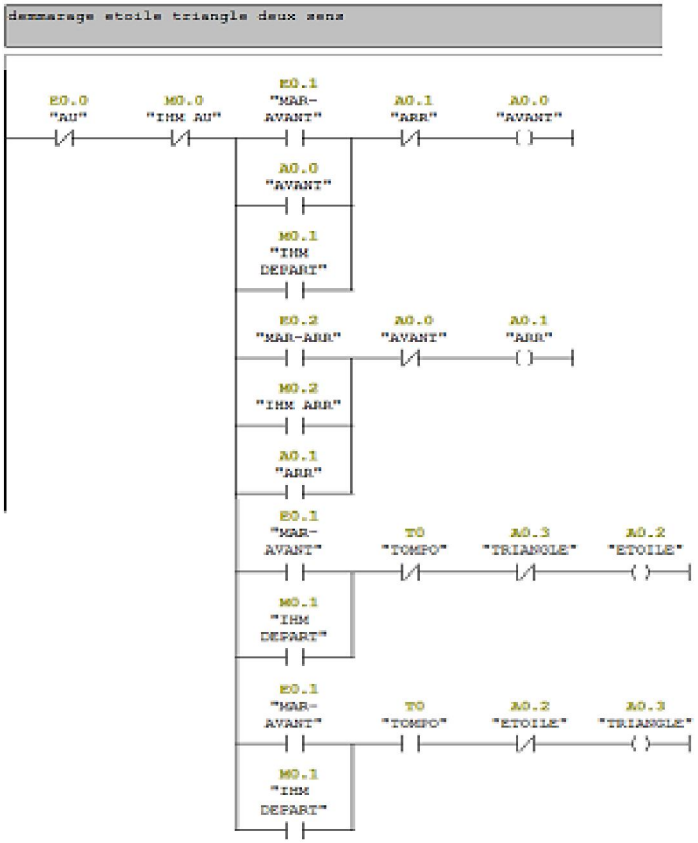


Figure IV.18 : Vue principale du moteur Tapis.

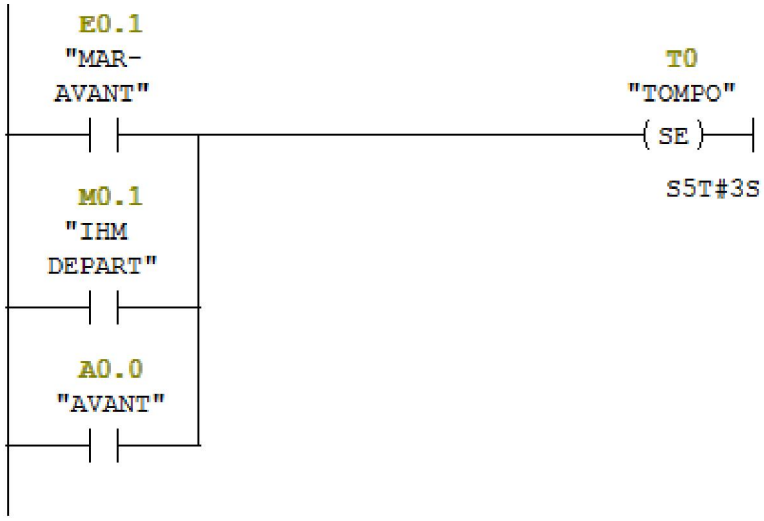
IV.2.4. Programme de l'application sur Step7 :

La programmation des différentes actions du cycle de fonctionnement est effectuée en langage Ladder ou CONT



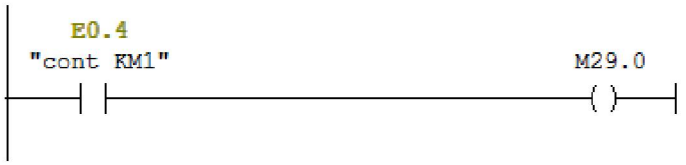
Dans ce programme nous avons inséré des mnémoniques en parallèle aux entrées/sorties de la CPU afin d'avoir le contrôle du moteur à partir de la station de supervision.

Programme de la temporisation:



c) Programme des alarmes et retour d'informations

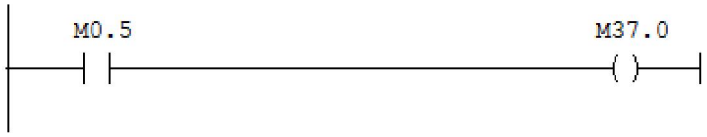
défaut contacte de ligne



défaut disjoncteur

défaut contacte 2

défaut km4



IV.2.5. La table de mnémoniques

Il s'agit d'une table qui permet d'affecter des noms a des adresses de données globales, accessible a partir de tous les blocs, ils peuvent être en particulier des mémentos(M),des entrées (E),des sortie (A),des temporisateurs ou des éléments de bloc de données (DB) .

La fenêtre des mnémoniques s'affiche comme suite:

Editeur de mnémoniques - [Programme S7(3) (Mnémoniques) -- mr zerouki\Station SIMATIC 300\CPU 314C-2 DP]

Table Edition Insertion Affichage Outils Fenêtre ?

Tous les mnémoniques

	Etat	Mnémonique	Opérande	Type de d	Commentaire
1		Alarme arrêt	MW 25	WORD	
2		ARR	A 0.1	BOOL	
3		AU	E 0.0	BOOL	
4		AVANT	A 0.0	BOOL	
5		cont disj	E 0.3	BOOL	
6		cont KM1	E 0.4	BOOL	
7		cont km2	E 0.5	BOOL	
8		cont phase	E 0.7	BOOL	
9		contac km3	E 0.6	BOOL	
1		défaut km 2	MW 30	WORD	
1		défaut disjoncteur	MW 26	WORD	
1		défaut km 3	MW 32	WORD	
1		défaut km1	MW 28	WORD	
1		défaut km4	MW 34	WORD	
1		défaut phase	MW 36	WORD	
1		ETOILE	A 0.2	BOOL	
1		IHM ARR	M 0.2	BOOL	
1		IHM AU	M 0.0	BOOL	
1		IHM DEPART	M 0.1	BOOL	
2		MAR-ARR	E 0.2	BOOL	
2		MAR-AVANT	E 0.1	BOOL	
2		TOMPO	T 0	TIMER	
2		TRIANGLE	A 0.3	BOOL	

Figure IV. 19 : La table de mnémoniques.

IV.2.6. Elaboration de la supervision

La supervision du permet de commander et de contrôler l'état de marche de moteur (démarrage, marche avant, marche arrière, arrêt et les alarmes) comme le montre la figure suivante:

IV.2.7. La simulation de programme PLCSIM avec WinCC.

ce logiciel permet de simuler le programme s7, la simulation étant réalisée complètement au sein du logiciel step7,il n'est pas nécessaire qu'une liaison pc/automate soit établie, cette interface simple permet de visualiser et forcer les différents paramètres présents dans le programme. On peut observer en parallèle le programme **WinCC et PLCSIM.**

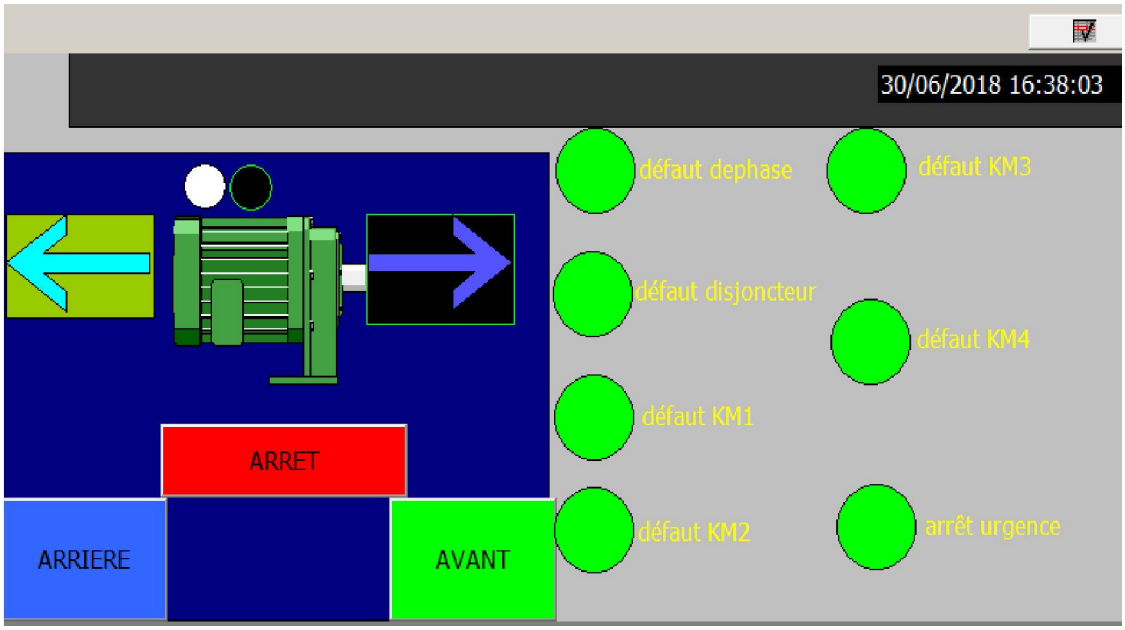


Figure IV. 20 : Observation du moteur en marche.

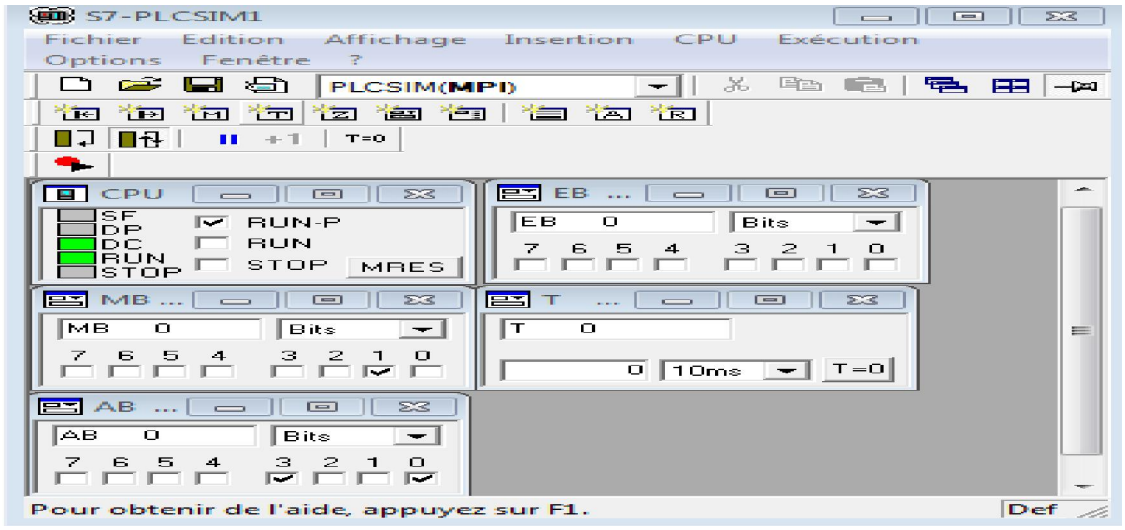


Figure IV. 21 : Fenêtre de PLCSIM.

Remarque

Après le chargement et l'activation du simulateur et le système runtime,on peut observer les autres états de fonctionnement (arrêt, arrière et les alarmes).

Conclusion

La supervision de chaque équipement des installations nous permet de récupérer plus d'informations sur l'état de fonctionnement de chaque composant, ces dernières offrent aux techniciens un moyen simple de détecter des défaillances sans solliciter l'ingénieur, l'intervention de celui-ci se fait uniquement si le problème est lié à la programmation.

Conclusion générale

Nous concluons qu'avec les nouveaux protocoles de communication et l'intégration de l'utile informatique dans l'industrie, les transferts de données se fait en paquet voir des gigabits et en un temps records. Ce dernier permet surveiller et superviser les processus de production en un temps réel.

À la venue d'Internet et l'adoption du TCP/IP l'accès à l'informatique de production des entreprises peuvent se faire sans la présence physique des personnes, donc on parlera de télémaintenance. Faire de la télémaintenance exige des compétences en réseau et informatique industrielle; connaître les notions d'adresse IP, de masque de sous-réseau.

Comme internet est public le risque d'être piraté par une tiers personne est un facteur que Team Viewer ne prends pas à légère. Il conviendra donc de passer par des services avec tunnel VPN pour sécuriser chaque connexion et empêcher toute personne non identifié d'accéder à votre équipement.

A. DJEFFAL, « Cours Réseaux locaux industriels » 2010-2011, Université de Mohamed Khider, Biskra.

D. REYNAL, J-G RORTHAIS, S-S.TAN, « Présentation sur les VPN », Université de Marie la Valée, 2004.

https://www.generation-nt.com/assistaer-article-50005-7.html

https://www.tech2tech.fr/assistance-a-distance-quel-logiciel-utiliser/

J-f. HECOLD, G. OLIVIER, P.ANAYA, « Informatique Industrielle et Réseaux » Juin 2015, France.

J-M. CHARTE, « Supervision : outil de mesure », Technique de l'ingénieur n° R 7630.

J-P. DALZON, « Ne laissez pas votre système de contrôle ouvert au piratage » 2009 côte d'azur, France.

L.FRANÇOIS, « Cours d'introduction à TCP/IP », Version 25 février 2009, France.

O, BELKACEM, **«** les bus et les réseaux de terrain en automatisme industriels», 2002.

Schneider électrique et Télémécanique, « Les Réseaux de communication Industriels » Mai 2007, Cedex, France.

WinCC, SIMATIC, « Supervision de Process avec Plant Intelligence », Brochure, 2009, France.

WWW.norminfo.afnor.org

WWW.siemens.com/wincc

WWW.supinfo.com

WWW.TeamViewer.com

Résumé

De nos jours il est impossible de réaliser une installation de production sans le contrôle par l'outil informatique. Cette opportunité que l'informatique offre aux entreprises le privilège de télé-maintenir leurs installations : Au lieu de faire venir sur place une personne aux compétences rares et de payer des frais de déplacement (trajet aller et retour, hébergement), il est plus économique de la laisser sur son lieu habituel de travail et de l'autoriser, grâce aux réseaux existants et aux logiciels de prise de contrôle à distance, à effectuer les mêmes opérations qu'elle serait amenée à réaliser si elle se trouvait sur le site de l'entreprise. Notre travail comprends quatre chapitres, au premier nous avons définit les types de communications en informatique industrielles ainsi les leurs protocoles. Au second chapitre nous avons expliqué les nouvelles architectures des réseaux locaux industriels et le rôle de l'utile l'informatique à stigmatiser les communications. Le troisième chapitre parle de la supervisons et la capacité de visualiser les processus industriels en temps réel sur les écrans de supervision. Pour terminer, au quatrième chapitre nous avons présenté le Logiciel qui nous permet l'accès à distance TeamViewer suivis de deux applications. Application 01 : est une communication Via Profibus DP entre deux automate l'un est configuré comme Maître et l'autre en Esclave. Application 02 : Visualisation d'un moteur asynchrone qui démarre en étoile/ triangle à deux sens entrainant un tapis roulant, A l'aide de TeamViewer nous avons pu accéder au programme à distance et effectuer quelques opérations de programation.

Mot clé : Step7, WinCC Advensed , Station PC , TeamViewer, Profibus DP, TCP/IP.