

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique



Ecole Supérieure des Sciences Appliquées d'Alger (ESSA-Alger)

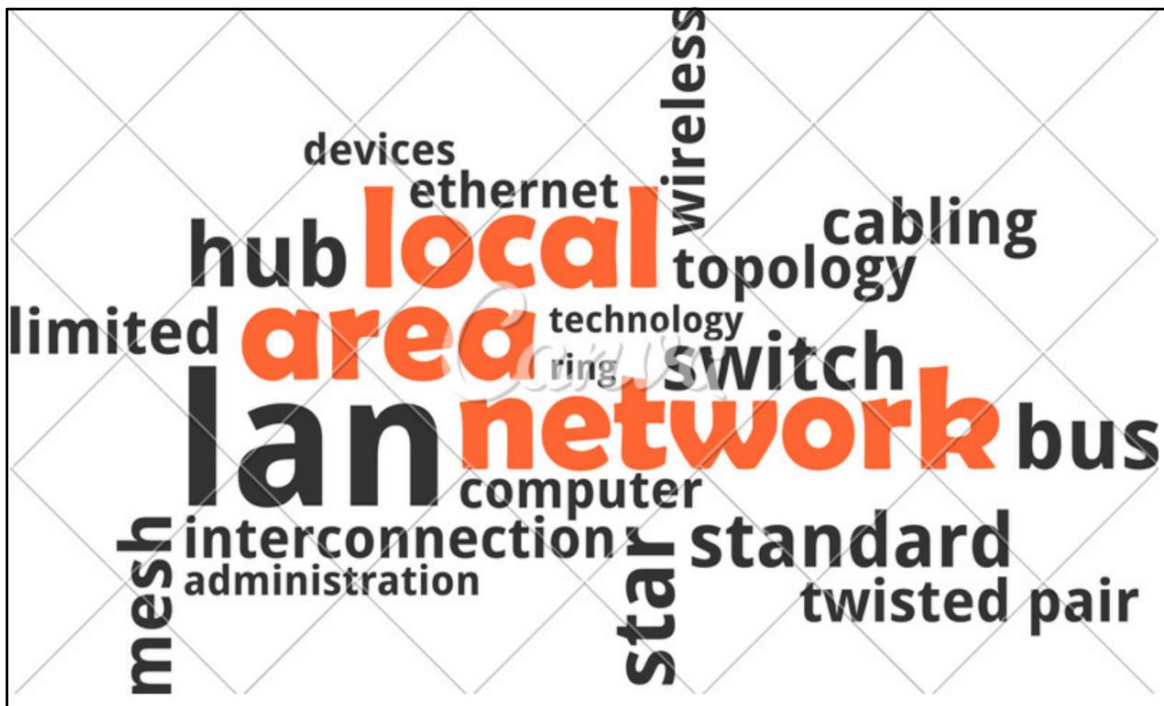
Département du second cycle

Filière: **Electrotechnique**

Spécialité: **Traction Electrique**

Polycopié du cours du module :

Réseaux industriels



En vue de soutenir l'habilitation à diriger des recherches

Réalisé par:

Dr. BENKRAOUA Souleyman

Maître de Conférences Classe B

Année universitaire: 2021-2022

Avant-propos

Cibles

Ce cours de « réseaux industriels » s'adresse essentiellement aux étudiants de l'ESSA-Alger du département second cycle pour l'option Traction Electrique, niveau 3^{ème} année S5. Il peut également être utile à toute personne appelée à l'étude d'Electrotechnique, Electronique, Génie Industriel, Génie Electrique, Automatismes, Régulation, Automatique, etc.

Charge horaire

Ce cours est dispensé à raison d'une heure et demi de Cours intégrés, d'une heure et demi de Travaux Dirigés et d'une heure et demi de Travaux Pratiques par semaine pendant quinze semaines soit, au total, soixante heures de Cours et de Travaux Dirigés et sept heures et demi de Travaux Pratiques avec un coefficient de l'unité égale à trois.

Objectifs généraux

L'évolution des automates programmables industriels a entraîné un changement des systèmes automatisés, qui continuent d'évoluer des architectures centralisées vers des architectures distribuées. Afin d'augmenter la production des usines de fabrication, doit répondre à l'expression du besoin d'assurer une communication entre l'automatisation de production ; et l'informatique de la gestion de l'entreprise.

L'objectif de ce cours consiste de donner à l'étudiant les notions de bases lui permettant de comprendre les différentes solutions et protocoles de communication utilisés dans les réseaux locaux en milieu industriel : du capteur/actionneur jusqu'au niveau entreprise.

Le présent cours comporte quatre chapitres organisés suivant une méthodologie mettant en valeur les objectifs fixés :

1. Le premier chapitre traite des notions de base sur la communication dans un environnement industriel ;
2. Au second chapitre sera présentée sur les techniques de transmission de données. Les notions de base pour l'échange des informations sur des distances importantes et les différentes solutions qui existent pour pouvoir communiquer ;
3. Le troisième chapitre sera consacré pour l'étude du modèle OSI des réseaux locaux industriels et le modèle TCP/IP. Ces études sont basées sur la restriction du modèle OSI à trois couches car la notion de temps est un point très important et le modèle TCP/IP ;
4. Le dernier chapitre est consacré à des études de cas, étude de quelques réseaux de terrain (bus WorldFIP, ASI, CAN, Modbus et Profibus).

Pré-requis

La communication entre les constituants des systèmes automatisés industriels (Ordinateurs, automates programmables, commandes numériques, capteurs/actionneurs..) est un grand problème technique de la conception des applications en informatique industrielle. Ce module s'appuie sur des connaissances de base en automatisme et l'informatique industrielle.

Les compétences visées par ce cours sont nécessaires à la compréhension de ce domaine. Les connaissances relatives aux:

- Besoins génériques en termes d'applications industrielles (à quoi sert la communication industrielle et quels sont les composants industriels qui sollicitent des services de communication) ;
- Sept couches du modèle OSI : les « composants matériels et logiciels » mis en œuvre pour la communication sont organisés et structurés en terme de leur réalisation et des services qu'ils proposent ;
- Techniques de transfert élémentaire de l'information (codage, mécanismes de transfert, modulation...);
- La sous couche MAC qui assure l'accès au support de transmission;
- Sous couche LLC (Logical Link Control) pour contrôler la CRC;
- Topologies de réseau (étoiles, maillés, bus, mixtes...);
- Notions de protocoles (trames, adressage, checksum, maître, esclave, bus....);
- Etudier des réseaux très répandus dans le monde industriel (MODBUS, PROFIBUS et autres ...) dont le coût unitaire est parfois très élevé pour servir lors de deux ou trois TP au cours du semestre.

Voilà autant de questions qui trouvent leurs réponses dans le développement de ce polycopié.

Table des matières

Chapitre 01 : Notion de base sur la communication dans un environnement industriel	1
1.1 Introduction	1
1.2 Qu'est-ce qu'un réseau local industriel (RLI).....	1
1.3 L'environnement industriel	1
1.4 Les différents niveaux d'abstraction dans un environnement industriel	2
1.5 Architecture d'un réseau industriel.....	3
1.6 Classement des réseaux en fonction de leur type.....	4
1.7 Caractéristiques du trafic	4
1.8 Les besoins et les contraintes de communication.....	6
1.9 Topologies des réseaux.....	8
1.10 Protocole	11
1.11 Description du modèle OSI : International Organization for Standardization.....	11
1.12 Concepts de base	14
1.13 Modèle OSI de trois couches et RLI.....	15
1.14 Conclusion.....	15
Chapitre 02 : Techniques de transmission de données	17
2.1 Introduction	17
2.2 La transmission en bande de base.....	18
2.3 L'amplification numérique des signaux.....	20
2.4 La modulation d'un signal porteur.....	21
2.5 Type de transmission.....	23
2.6 Mode de transmission.....	24
2.7 Conclusion.....	25
Chapitre 03 : Étude du modèle OSI des RLI et le modèle TCP/IP sur Ethernet	26
3.1 Introduction	26
3.2 Étude du modèle OSI à trois couches des RLI.....	26
3.2.1 Couche physique	26
3.2.2 La couche liaison de données	39
3.2.3 Couche Application	48
3.3 Étude du modèle TCP/IP	49
3.3.1 Ethernet	49
3.3.2 Modèle TCP/IP.....	49
3.3.3 Trame Ethernet V2	57

3.3.4 Trame Ethernet 802.3	57
3.3.5 Principe du modèle Client-Serveur en réseau	57
3.3.6 Les protocoles réseaux Ethernet (TCP/UDP/IP)	57
3.3.7 Principe de fonctionnement du TCP/IP sur Ethernet	57
3.3.8 Principaux services de la couche application	58
3.3.9 Conclusion.....	59
Chapitre 04 : Les réseaux de terrain.....	61
4.1 Introduction	61
4.2 Les réseaux de terrain et la boucle 4-20 mA.....	60
4.3 Critères de comparaison	63
4.4 Étude de cas.....	64
4.4.1 Le bus World FIP (Factory Instrumentation Protocol).....	64
4.4.2 Le bus AS-I (Actuators Sensors Interface)	67
4.4.3 Le bus CAN (Control Area Network).....	72
4.4.4 Le bus Modbus	82
4.4.5 PROFIBUS (PROcess FIeld BUS)	87
Conclusion générale et Références Bibliographiques	92
Références bibliographiques.....	93

Chapitre 01 : Notion de base sur la communication dans un environnement industriel

1.1 Introduction

Les réseaux locaux industriels ont été introduits progressivement dans les systèmes automatisés, à différentes étapes selon les domaines d'application. L'histoire des réseaux locaux industriels remonte à la fin des années 70, ils sont nés avec le développement de l'électronique et des appareils intelligents programmables. L'apparition des automates programmables a conduit les fournisseurs 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. Leur émergence répond à deux points très importants, le premier répond aux exigences croissantes de productivité dans le domaine industriel par l'automatisation de la communication entre les différents appareils industriels afin d'éliminer la perte du temps et les risques d'erreurs causées par l'intervention humaine, le second point, répond au besoin d'interconnexion des équipements pour résoudre chaque problème individuellement sans considérer l'intégrité de l'ensemble du système industriel.

Les informations peuvent être transmises sous forme analogique (évolution continue de la valeur), ou numérique (évolution discontinue de la valeur). Un automate programmable peut par exemple échanger avec une vanne des mots des bits dans le but de donner des consignes de vitesse de fermeture ou des modes d'arrêt et de marche. Ces deux types d'informations doivent être transmettre et partager dans l'industrie pour bien gérer la production, la logistique et le finance.

1.2 Qu'est-ce qu'un réseau local industriel (RLI)

Un RLI est un système de communication entre plusieurs appareils de types industriel (capteurs, actionneurs, automates..) dans une zone géographique limitée. Les réseaux locaux industriels, sont parfois appelés abusivement réseaux de terrain, s'inscrivent donc à différents niveaux au sein de la pyramide CIM (Computer Integrated Manufacturing). Il existe plus de 2000 bus de terrains différents, mais, les technologies les plus répandues sont : Modbus, Profibus-FMS/PA, Profibus-DP Interbus-S, ASI, WorldFIP, Lonworks et bus CAN.

1.3 L'environnement industriel

L'environnement industriel comprend tous les équipements participant à la chaîne industrielle Qu'il soit utilisé pour la fabrication, le contrôle ou la maintenance. Ces appareils peuvent être des stations de supervisions (SCADA, IHM), robots, capteurs, actionneurs, ...etc comme le montre la figure ci-dessous. Ainsi que les moyens dont ils ont besoin pour s'interconnecter, comme les câbles, Passerelles, routeurs, etc.

Aujourd'hui, dans un environnement industriel, la plupart des tâches se font d'une façon automatique ce qui donne un taux maximal de production, garantit une meilleure sécurité du personnel, et augmente la rentabilité de l'industrie en général.

L'automatisation des systèmes industriels permet concrétiser des objectifs très importants :

- Commercialisation rapide des nouveaux produits ;
- Réagir à court terme ;
- Réduire le temps de mise sur marché ;
- Produire de manière efficace et économique ;
- Exploiter de façon optimale les capacités des machines ;
- ...etc.

Pour atteindre de tels objectifs parfaitement, il faut que toutes les machines d'une installation soient complètement automatisées et fonctionnent en parfaite interaction, ce qui peut être atteint par :

- Utilisation des API (Automates programmables Industriels) qui permettent d'automatiser le système ;
- Utilisation des robots pour automatiser les tâches « intelligentes » telles que la soudure, le montage, assemblage, ... etc ;
- L'utilisation des RLIs pour garantir l'interopérabilité des équipements automatisés.

1.4 Les différents niveaux d'abstraction dans un environnement industriel

Pour mettre en œuvre un grand nombre de fonctions qui sont largement interdépendantes, les architectures actuelles se structurent en quatre niveaux distincts (de 0 à 3) et interconnectés par des réseaux. Les quatre niveaux d'abstraction de hiérarchie correspondent au niveau de décision, un niveau supérieur décide ce qu'un niveau inférieur exécute. Plus la hiérarchie s'élève, plus le niveau de décision est élevé, plus la visibilité est globale et plus la période standard s'allonge voir (figure 1.5).

1.4.1 Niveau 03 (entreprise)

Corresponds au sommet de la pyramide, on s'intéresse à toute une partie de l'usine. Ce niveau interconnecte les ateliers et permet l'utilisation des logiciels ERP (Enterprise resource Planning) en liaison avec les données de production. On trouve à ce niveau des services de gestion tel que ; la gestion des produits et des stocks, la gestion des approvisionnements, la gestion des clients, des commandes et de la facturation.

1.4.2 Niveau 02 (usine)

À ce niveau on retrouve des automates programmables maîtres et des ordinateurs qui gèrent les tâches de la production telle que:

- ✓ GPAO : Gestion de Production Assistée par Ordinateur ;
- ✓ CFAO : Contrôle de Fabrication Assisté par Ordinateur ;
- ✓ CAO : Conception Assisté par Ordinateur.

Ces postes permettent de visualiser l'état du procédé (la localisation des produits en stocks, les mouvements physiques et la gestion des lots, permettent aussi de contrôler et de commander les actionneurs.

1.4.3 Niveau 01 (Atelier)

Contient plusieurs îlots de fabrication, avec des modules d'entrées/sorties déportées, de vision, de supervision, des automates programmables...etc. La communication descendante vise à véhiculer les signaux pour les capteurs et les actionneurs.

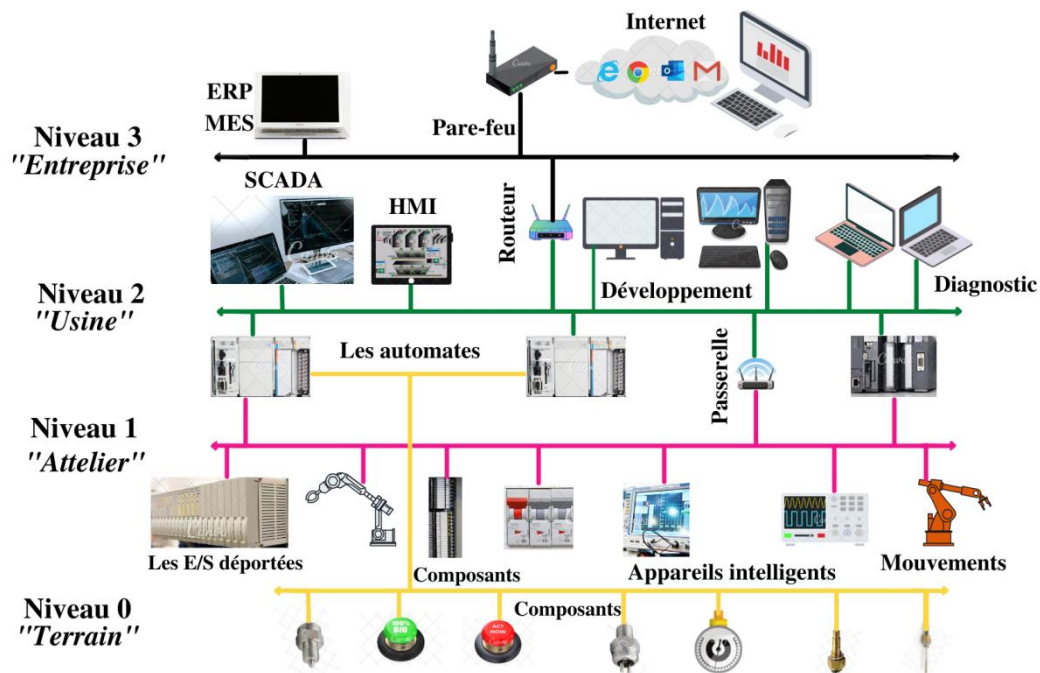


Figure 1.1 : Les différents niveaux d'abstraction dans un environnement industriel.

1.4.4 Niveau 0 (terrain)

C'est le niveau le plus bas de la pyramide, qui contient des actionneurs/capteurs. Les capteurs sont des instruments de mesure qui peuvent donner à des machines intelligentes (telles que les PC ou les API) des informations telle que la température, la pression, la tension, ...etc. Les actionneurs peuvent être activés par des appareils intelligents (Automates programmables) telles que les moteurs, les vannes, les capteurs, les alarmes,...etc.

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. Il existe donc trois types de réseaux :

1.5 Architecture d'un réseau local industriel

1.5.1 Les réseaux de terrain

Les réseaux de terrain comprennent et connectent un grand nombre de nœuds, tels que des capteurs, des actionneurs, des automates, des régulateurs, et plus généralement tout appareil prenant en charge des applications nécessitant l'accès à des appareils de terrain. Ils peuvent même être connectés via plusieurs réseaux locaux.

1.5.2 Les réseaux d'atelier ou de cellule

Les réseaux d'atelier comprennent et connectent, un nombre moins important tel que les dispositifs de commande de robots, de machines-outils, de contrôle de la qualité (lasers). Ces réseaux existent principalement dans l'industrie manufacturière.

1.5.3 Les réseaux d'usine

Le réseau d'usine comporte quelques stations, ils interconnectent des ateliers, des cellules avec des services de gestion et de conception

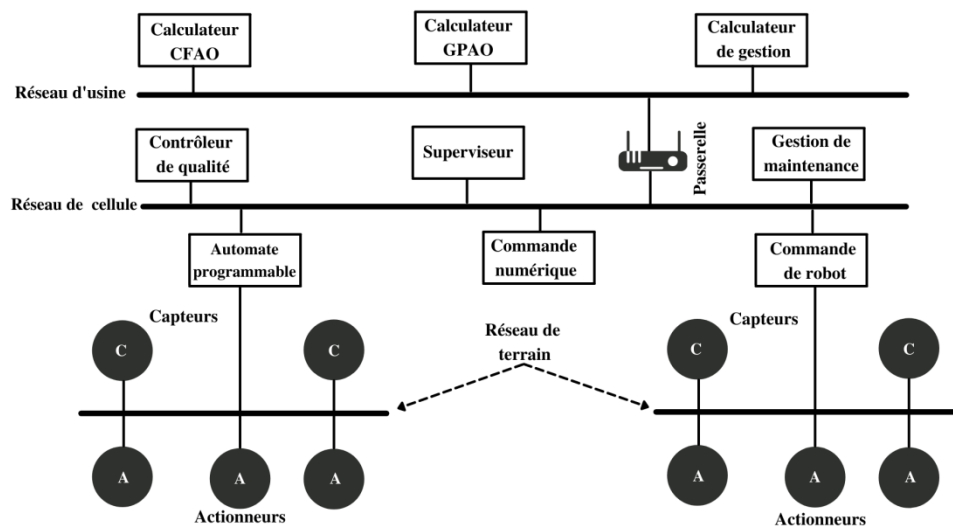


Figure 1.2 : Architecture globale d'un réseau local industriel RLI.

1.6 Classement des réseaux en fonction de leur type

1.6.1 Réseaux homogènes

Fourni par le fabricant de l'équipement d'automatisation. Par exemple, le cas des automates télémechaniques, seuls leurs capteurs et leurs actionneurs peuvent être intégrés pour automatiser un procédé.

1.6.2 Réseaux hétérogène

Les réseaux hétérogènes sont des réseaux multi fournisseurs, on peut trouver plusieurs types d'automates programmables (schneider, siemens, Omron..), plusieurs types d'entrées sorties et plusieurs protocoles de communications (Profibus, Ethernet, Modbus,...). Actuellement, la majorité des réseaux sont des réseaux hétérogènes

1.7 Caractéristiques du trafic

Dans un réseau local de bureau, les messages ont la même priorité, contrairement aux données échangées dans un réseau industriel, ils varient selon deux points essentiels :

- La priorité en termes d'urgence de transmission ;
- La taille de messages.

1.7.1 Nature des messages échangés

Les réseaux industriels traitent les informations généralement en temps réel, où les contraintes de temps sont très importantes, et de multiples événements doivent être traités en temps réel, et leur retard peut provoquer des dommages catastrophiques. À cet effet, les informations échangées peuvent être :

1.7.1.1 Messages urgents

Généralement ce type de message peut être trouvé au niveau du terrain, par exemple, transmission d'un message d'alarme (dépassement du seuil autorisé), ou un ordre de fermer ou d'ouvrir une vanne, etc.

1.7.1.2 Messages non urgents

On trouve ce type de message par exemple le chargement d'un programme exécutable sur un automate programmable ou le transfert d'un rapport.

1.7.1.3 Taille des messages

La taille des messages peut être :

- **Courts** : tel que la valeur d'une mesure envoyée par un transmetteur, ou un ordre de démarrage pour une machine, l'information peut être de type (binaire, Word, double Word, réelle) ;
- **Longs** : tel qu'un programme ou un fichier.

1.7.2 Qualités requises

1.7.2.1 Fiabilité

La majorité des équipements industriels représentent des sources sérieuses de perturbation des communications dans l'environnement industriel, donc les messages acheminés nécessitent un très haut degré de fiabilité pour une transmission sans erreur, sans perte et sans retard, et cela au niveau physique ou au niveau des protocoles de communication.

Par exemple, on a un automate programmable qui commande une machine, et on veut déplacer cette machine au-delà de 80m, donc il faut constater qu'on a ici un trajet ou l'information aussi doit se déplacer, donc ce trajet doit être sans pollution magnétique et pas de source de perturbation, sans poussière et aussi il faut éviter la communication série.

1.7.2.2 Performance

Même dans des conditions dégradées, c'est-à-dire lorsque certains composants tombent en panne, la continuité de fonctionnement doit être garantie. Vous devez avoir un bon Tolérant aux pannes et capable de reprendre certaines activités après les anomalies.

Par exemple, si une voiture a un problème du capteur de l'air, donc, le régime de la voiture dégrade et on ne peut pas aller au-delà de 100 km/h mais on peut circuler.

1.7.3 Services spécifiques

Un RLI peut être caractérisé par plusieurs phénomènes de communications spécifiques, envisager et apporter des solutions pour assurer le fonctionnement normal du réseau

- **Diffusion** : La diffusion peut être simultanée, ce qui signifie que plusieurs émetteurs doivent envoyer à plusieurs récepteurs en même temps.

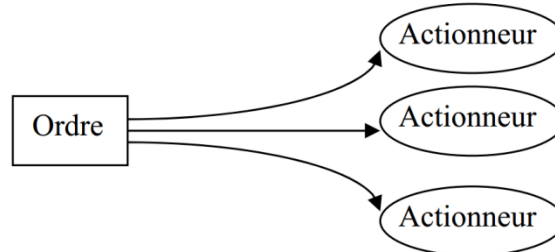


Figure 1.3 : La diffusion dans un réseau local industriel.

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

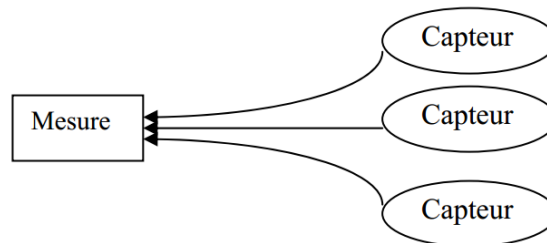


Figure 1.4 : La concentration dans un réseau local industriel.

- **Périodicité** : plusieurs traitements peuvent être périodiques tel que le prélèvement périodique des mesures de quelques capteurs (mesures cycliques).

1.8 Les besoins et les contraintes de communication

Avant de faire une analyse sur les technologies des réseaux de communication, il est nécessaire de résumer les principales exigences pour fournir des réponses pertinentes à ces niveaux. Parmi les caractéristiques citées dans le tableau ci-dessous, nous pouvons retenir les deux principaux axes de besoins :

- Le nombre d'informations à transmettre ;
- Le temps de réponse nécessaire.

Niveau	Besoin	Volume d'information à transmettre	Temps de réponse	Distance	Topologie réseau	Nombre d'adresses	Médium
Niveau 03	Echange de données. Sécurité informatique. Standards entre progiciels.	Fichiers Mbits	1 mn	Monde	Bus, étoile	Non limitée	Electrique, optique, radio
Niveau 02	Synchronisation des API d'un même îlot d'automatisme échanges d'information en mode client/serveur avec les outils de conduite (HMI, supervision). Performances Temps réel.	Données Kbits	50 à 500 ms	à 40 Km	Bus, étoile	10 à 100	Electrique, optique, radio
Niveau 01	Architecture distribuée. Intégration fonctionnelle et transparence des échanges. Topologie et coût de connexion.	Données Kbits	5 à 100 ms cycle de l'API)	0 m à 1 Km	Bus, étoile	10 à 100	Electrique, optique, radio
Niveau 0	Simplification du câblage distribution des alimentations des capteurs et actionneurs. Optimiser les coûts de câblage.	Données bits	1 ms	à 100 m	Sans contrainte	10 à 50	Electrique radio

Tableau 1.1 : Besoins et contraintes de communication.

En effet, quand on se place au niveau 0, le problème qui se pose s'est de communiquer l'état de ces derniers ou de les commander. Dans ce cas un octet suffit comme donnée utile. Par contre, au niveau 01, il peut s'agir d'application de MES (Manufacturing Executing System) pour la production avec des fichiers lourds de recettes.

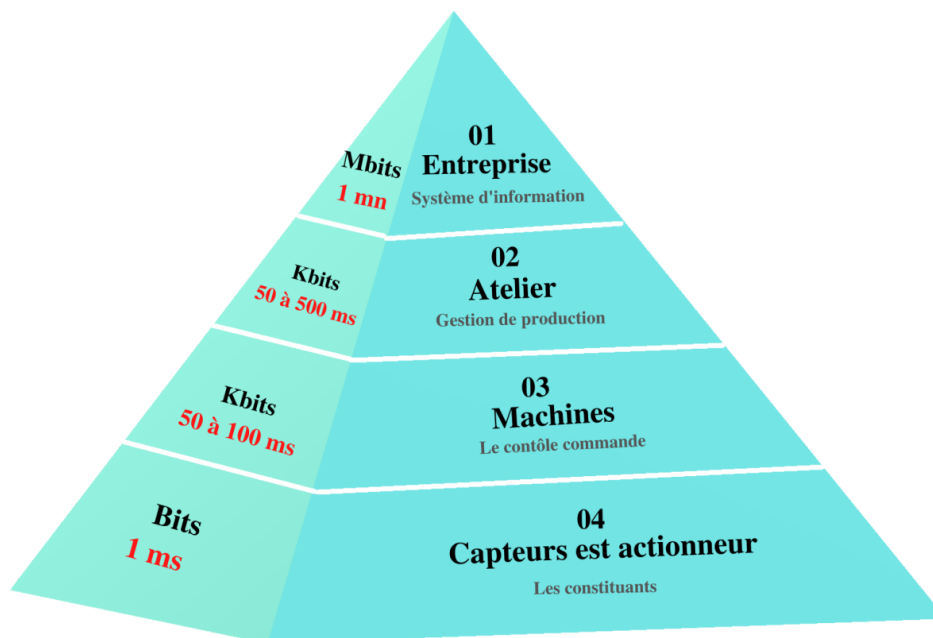


Figure 1.5 : Capacité et débit d'information à transmettre.

Ces caractéristiques nous permettent de localiser les principaux réseaux commercialisés (figure 1.6)

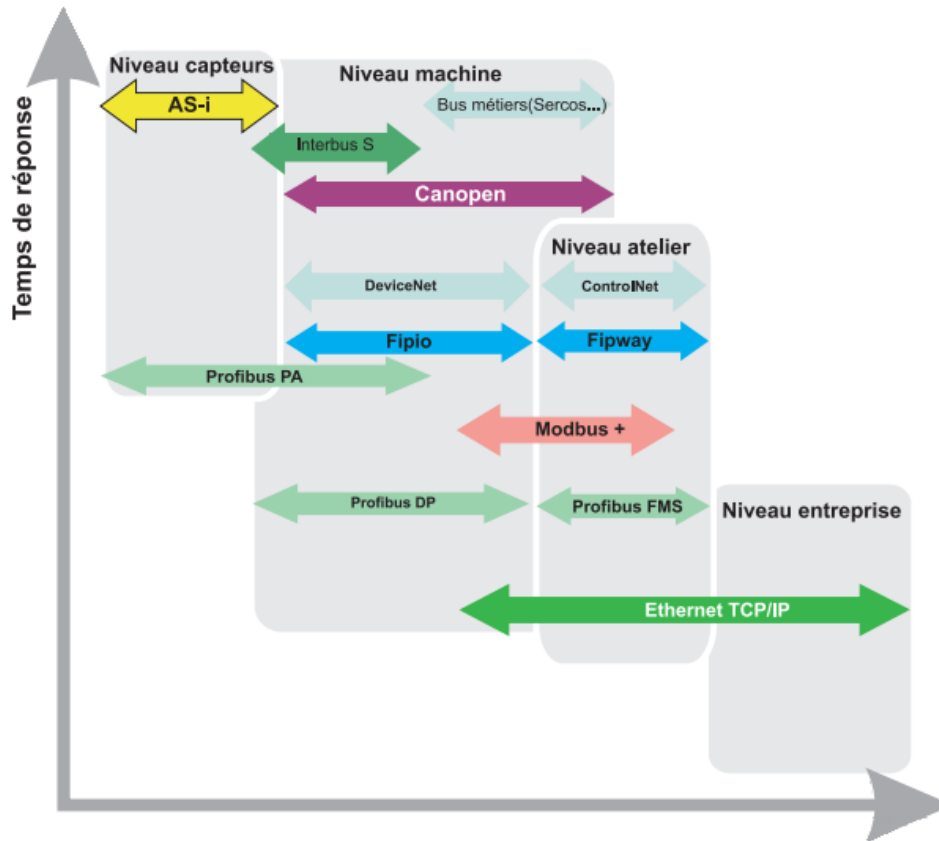


Figure 1.6 : Principaux réseaux industriels [23].

1.9 Topologies des réseaux

Une topologie désigne la structure de réseau et la manière dont les équipements sont organisés. En effet, il existe deux types de topologies :

- **Topologie logique** : dans la topologie logique on considère le parcours de l'information entre les différents éléments de réseau ;
- **Topologie physique** : Un réseau industriel est constitué d'automates programmables, des IHM, des PC, des équipements d'E/S, connectés entre eux grâce à des lignes de communication, telles que des câbles électriques, des fibres optiques, des liaisons radio et des éléments d'interface, tels que des cartes réseaux, des Switch, des passerelles, routeurs,... etc.

Il existe plusieurs topologies possibles, donc, les principales topologies sont :

- En étoile ;
- En bus ;
- En anneau ;
- Maillées.

1.9.1 Topologie en étoile

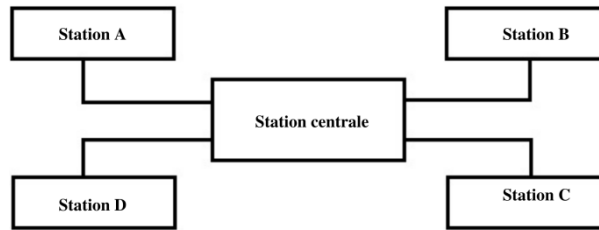


Figure 1.7 : Topologie des réseaux en étoile

Cette typologie est la plus utilisée au niveau de l'entreprise et de l'atelier. Elle est celle du réseau Ethernet. Son avantage qu'elle est très flexible en matière de gestion et de dépannage. La défaillance d'un nœud ou une liaison est coupée ne perturbe pas le fonctionnement global du réseau, aussi il n'y a pas de risque de collision de données. Les stations finales sont connectées ensemble à travers un élément central qui peut être (répéteur, commutateur). Le principal inconvénient de cette topologie, c'est que si la station centrale central ne fonctionne plus, plus rien ne fonctionne.

1.9.2 Topologies en bus

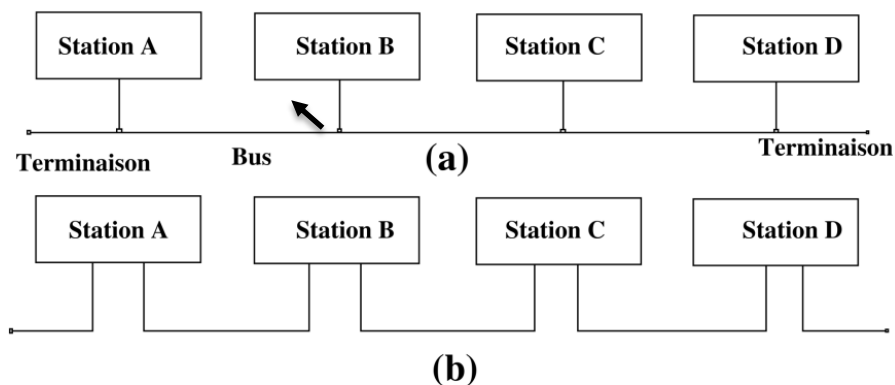


Figure 1.8 : Topologie des réseaux en bus

Cette topologie est plus simple, elle a les caractéristiques d'un bus (une ligne droite). Tous les éléments sont connectés entre eux par un seul câble, le réseau débute et termine par des terminateurs pour maintenir les données dans le câble. Cette topologie est facile à mettre en œuvre, la défaillance d'un nœud ou d'un élément ne n'interférera avec les fonctions des autres organes. Cette typologie est réalisée en reliant les équipements les uns avec les autres soit via un câble principal (figure 1.8a) ou par chaînage via un boîtier de raccordement (figure 1.8b).

1.9.3 Topologie en anneaux

La topologie de type bus possédait un problème de collision de données. Deux stations ne doivent pas échanger des données en même temps. Ce principe est repris dans le réseau en anneau. Sauf que, le système de Token ring une méthode anticollision différente. Le principe est assez simple : une station reliée au réseau possède un jeton virtuel, ce dernier est une autorisation de communication. Une fois que la station a transmis ce qu'elle voulait, elle passe le jeton à la station suivante, et ainsi de suite. Si une station n'a rien à envoyer, elle passe le jeton à la station suivante.

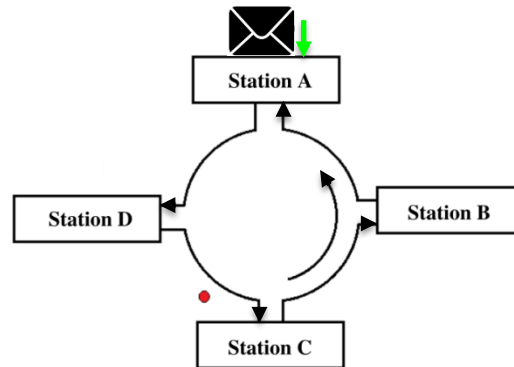


Figure 1.9 : Topologie des réseaux en anneaux.

Pour ajouter une station au réseau, il faut couper le câble. À ce moment, le réseau ne fonctionne plus. Par conséquent, afin d'éviter une panne du réseau en cas de destruction du câble, une autre boucle de secours est ajoutée à la topologie double anneaux.

1.9.4 Topologies en réseau maillées

Cette topologie est assez peu utilisée dans l'industrie et présente l'inconvénient d'un nombre important de connexions. La formule utilisée pour connaître le nombre de câbles est $N(N-1)/2$, avec N le nombre stations. Donc rien qu'avec 6 ordinateurs par exemple, ça nous donnera $4(4-1)/2$, soit 6 câbles.

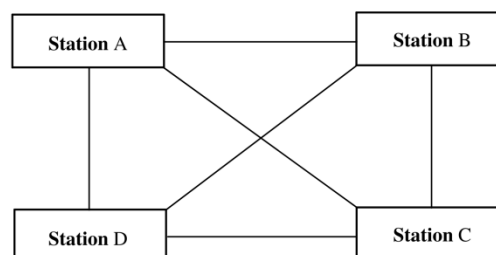


Figure 1.10 : Topologie des réseaux maillée.

En plus, chaque câble doit être connecté à deux cartes réseau, par exemple un réseau de quatre stations, ça ferait trois cartes réseau par station.

1.10 Protocole

Un protocole de communication est la spécification de plusieurs règles pour des types spécifiques de communication. Initialement, on nommait protocole, ce qui était utilisé pour communiquer sur la même couche d'abstraction entre deux appareils différents. Grâce à l'expansion du langage, le mot est parfois utilisé aujourd'hui pour spécifier les règles de communication entre deux couches sur le même appareil

1.11 Description du modèle OSI : Open System Interconnection Model

En 1977 l'Organisation Internationale de Normalisation ISO (International Organization for Standardization) a créé pour des besoins de compatibilités entre les différentes machines tout un ensemble de lois de compatibilités baptisé modèle OSI . Celui-ci est appelé modèle de référence OSI parce qu'il traite de la connexion entre les systèmes ouverts, c'est à dire des systèmes pouvant s'interfacer avec d'autres systèmes

Dans ce modèle, les protocoles du réseau sont divisés en 7 parties, appelées couches OSI, et sont numérotées de 1 à 7. Les couches du modèle OSI suit les principes suivants :

- chaque couche supporte un protocole indépendamment des autres couches ;
- chaque couche fournit des services à la couche immédiatement supérieure ;
- chaque couche a besoin des services de la couche inférieure ;
- la couche 1 décrit le médium (support de communication).

Le modèle est applicable à tous les types de réseaux. Nous passons brièvement en revue le rôle de chaque couche. Tous les détails peuvent être trouvés dans de nombreux ouvrages. Les sept couches initiales du modèle sont rappelées par la (figure 1.11). Les couches 1, 2, 3 et 4 se préoccupent du transport d'informations et masquent aux couches supérieures les problèmes liés à la communication d'informations entre des équipements distants.

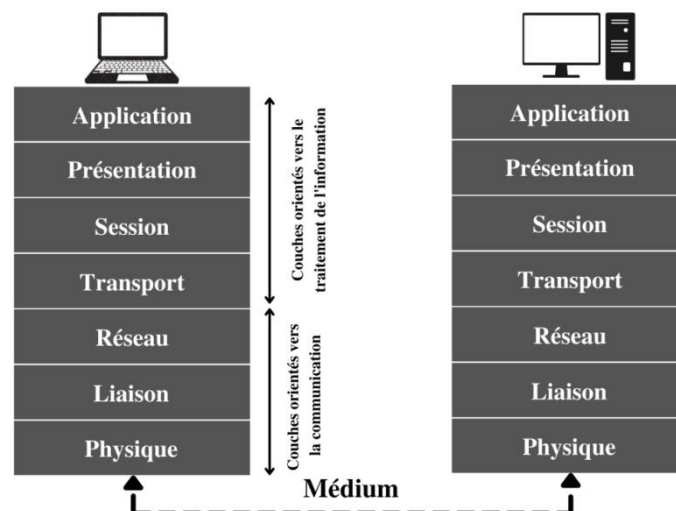


Figure 1.11 : Représentation du modèle à sept couches OSI.

Les couches 5, 6 et 7 fournissent des services d'accès à la communication pour différents types d'applications. A noter que les sept couches définies ne sont en générale pas toutes utilisées.

Quand deux personnes veulent communiquer elles doivent suivre un protocole précis. Il se décompose logiquement en sous-ensembles qui répondent chacun à un type de préoccupation ces sous-ensembles sont adjacents deux à deux et constituent chacun une couche du protocole global

Dans le processus de communication, l'utilisateur d'un réseau utilise les services de la couche 7 via un programme. Cette couche met en forme et enrichit l'information qu'elle reçoit du programme tout en respectant son protocole. Ensuite, l'information est envoyée à la couche inférieure lors d'une demande de service. À chaque couche, l'information subit des mises en forme et des ajouts selon le protocole utilisé. Enfin, elle est envoyée sur le support de transmission et reçue par un autre nœud du réseau. Elle traverse toutes les couches de ce nœud dans l'autre sens pour finir au programme du correspondant, dépouillée des différents ajouts liés aux protocoles.

Qu'on souhaite envoyer une lettre d'embauche, autour de l'information à transmettre, on doit définir un ensemble de paramètres qui permettent d'acheminer des données, de nous, vers un responsable. Procédons par étapes comme le montre la figure ci-dessous.

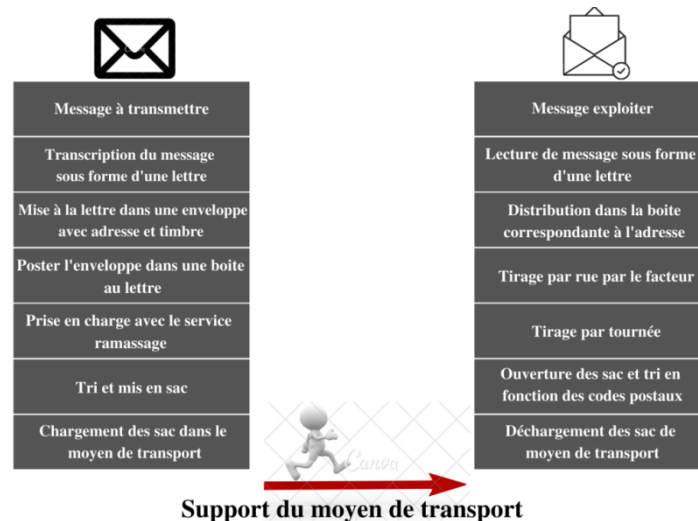


Figure 1.12 : Modèle d'architecture à 7 couches pour l'interconnexion des systèmes ouverts.

Un ensemble d'éléments représentent peu d'information, mais ils permettent au courrier d'atteindre sa cible. On a donc déposé des couches successives d'information. D'où l'idée d'une définition de ces ajouts sous forme de couches

1.11.1 Couche physique (couche 01)

La couche physique représente le plus bas niveau du modèle OSI, elle définit les règles électriques et mécaniques d'un réseau. On définit ainsi le type de connexion (full duplex, half

duplex ou simplex), le type de liaison (série ou parallèle), le média (câble coaxial, paire torsadée, fibre optique,.. etc).

1.11.2 Couche liaison de données (couche 02)

Le problème à résoudre au niveau de la couche de liaison c'est l'identification de deux machines sur le même support physique, elle gère les processus de connexion et de déconnexion, elle détecte les erreurs, gère l'adressage et définit le formalisme de la trame pour l'adapter au support physique.

Il existe deux sous-couches très importantes la sous-couche MAC (Médium Access Control) qui permet de gérer l'accès au médium (gestion du droit d'émission), gérer les conflits ou les éviter et la sous-couche LLC (Logic Link Control) qui s'occupe du service avec les couches supérieures.

1.11.3 Couche réseau (couche 03)

La couche réseau permet de réaliser le routage, elle s'occupe de l'acheminement de paquets (datagrammes) de données entre deux machines qui ne sont pas sur le même support physique.

1.11.4 Couche transport (couche 04)

C'est la frontière entre le monde de la transmission et celui de l'application. La couche de transport a pour but de contrôler le flux des données dans un réseau. Elle gère le contrôle des erreurs de transmission, segmentation des messages et la fiabilité de la liaison.

1.11.5 Couche session (couche 05)

La couche Session, s'occupe de l'établissement, de la gestion et coordination des communications. Cette couche offre la possibilité d'organiser les échanges en unités indépendantes. Elle offre aussi une structure de contrôle pour la communication entre applications. Elle établit, maintient et clôt les sessions s entre les applications. L'un des points forts de cette couche est la sécurité.

1.11.6 Couche présentation (couche 06)

La couche présentation s'occupe de la mise en forme des textes et des conventions d'affichage. Elle permet entre autre de fournir une représentation des données tels que, le codage et le décodage de l'information, le cryptage, la compression et le formatage des données. Le rôle de cette couche est en fait de rendre compatibles des machines hétérogènes (par exemple, dialogue entre un MAC et un PC).

En effet, il existe de multiples manières de coder les informations en informatique suivant le matériel et les logiciels utilisés, par exemple :

- Il existe plusieurs codes pour coder les caractères (ASCII, BCIDC, etc.) ;
- Les nombres peuvent être codés sur un nombre d'octets différents ;

- La compression des fichiers,...etc.

1.11.7 Couche application (couche 07)

La couche application est la couche supérieure du réseau, elle a pour but de donner des services aux utilisateurs d'un réseau. Cette couche contient l'application informatique qui peut communiquer avec un ordinateur distant. Il existe deux types d'applications :

- les applications en mode connectées (où la connexion doit être maintenue) ;
- les applications en mode non connectées (où la connexion est intermittente, comme par exemple internet ou le courrier électronique).

1.12 Concepts de base

1.12.1 PDU (*Protocol Data Unit*)

Comme le montre la (figure 1.13). Le PDU est l'unité de mesure¹ des informations échangées dans un réseau informatique. Appliqué au système de couches du modèle OSI, le PDU de :

- La couche physique est le bit ;
- La couche liaison est la trame ;
- La couche réseau est le paquet;
- La couche transport est le segment pour le protocole TCP, et le datagramme pour le protocole UDP.

1.12.2 Paquets

Un paquet inclut un en-tête, comprenant les informations nécessaires pour acheminer et reconstituer le message, et encapsule une partie des données.

1.12.3 Trames

Une trame représente la plus petite unité compréhensible par un réseau, c'est à dire le minimum de bits pour que le message puisse être transmis.

1.12.4 Encapsulation et décapsulation des données

Lors d'une transmission, les données parcourent chacune des couches au niveau de la station émettrice (encapsulation). À chaque couche, une information est ajoutée au paquet de données, il s'agit d'un entête, cet ensemble d'informations garantit la transmission. Au niveau de la station réceptrice (décapsulation), lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi à la réception, le message est dans son état originel. À chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches voir figure ci-dessous.

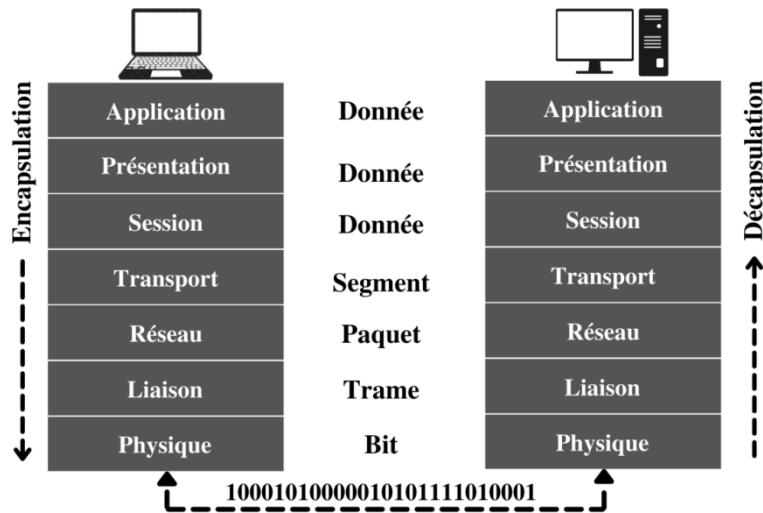


Figure 1.13 : Encapsulation et décapsulation des données.

1.13 Modèle OSI de trois couches et RLI

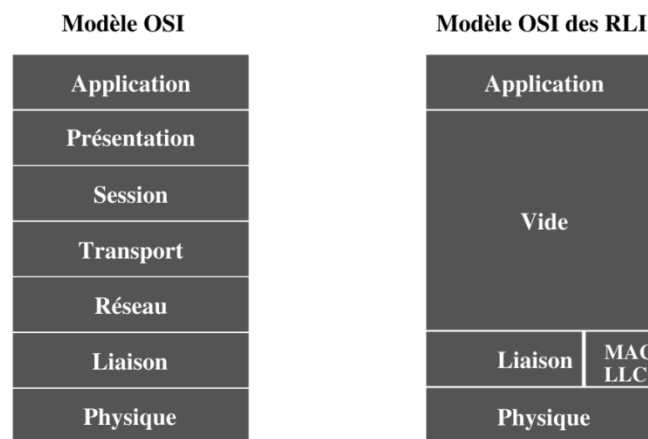


Figure 1.14 : Modèle OSI à trois couches pour RLI.

Comme le montre la figure ci-dessus, les RLI ne sont pas construits sur le modèle OSI à sept couches (contrairement aux réseaux informatiques). Ce modèle a montré dès ses premières applications une lourdeur pénible et des temps de réponse assez longs dans les réseaux locaux industriels, des versions réduites sont apparues pour pallier ces problèmes, ces versions essaient de ne garder des couches OSI que l'essentiel, elle ne comporte que les couches (1,2 et 7), il en résulte un modèle à trois couches son implémentation rapide et efficace. Les couches 4 à 6 sont regroupées avec la couche 7 et ce qui appartenait à la couche 3 est regroupé avec la couche 2, car il n'y a pas d'interconnexion avec un autre réseau.

1.14 Conclusion

Dans une première partie de ce chapitre nous nous sommes intéressés à la communication dans un environnement industriel. Nous avons vu qu'est-ce qu'un réseau local industriel, et

ses différents niveaux au sein de la pyramide CIM qui décrit l'automatisation complète des processus de fabrication, une segmentation « verticale » en niveaux des réseaux d'automatismes proposent différents niveaux de communication correspondant à une forme quantitative de données à véhiculer. Ainsi, au niveau le plus bas (capteurs et actionneurs), les messages sont courts mais les temps de réaction sont plus rapides. Au niveau le plus haut, les messages sont longs mais les temps de réaction sont non critiques. Entre ces deux niveaux, on trouvera le niveau qui correspond au pilotage des machines et le niveau qui correspond à la supervision du système (SCADA). Un aperçu sur les différents types de réseaux et leur classement en fonction de leur type. Nous avons vu aussi les différentes principales topologies des réseaux.

Dans une deuxième partie de ce chapitre, et en termes de protocole, nous avons vu les règles pour un type de communication particulier, ou bien entre deux couches sur un même équipement. Le modèle OSI à sept couches est applicable à toutes les catégories de réseaux, cependant, ce modèle a montré dès ses premières applications une lourdeur pénible et des temps de réponse assez longs dans les RLI. Des versions réduites sont apparues qui sont très rapides et très efficaces afin d'atténuer ces problèmes. Ces versions ne comportent que les couches (1,2 et 7) car ils ne sont pas interconnectés avec un autre réseau.

Chapitre 02 : Techniques de transmission de données

Transmission de données



2.1 Introduction

La nécessité d'échange des données entre différents systèmes, il doit exister une ligne de transmission, appelée canal de transmission ou médium. Le support de l'information de tout système informatique ou automatique est le signal numérique qui s'apparente au signal binaire si la transmission sur un seul fil de donnée. Le signal numérique, de part sa nature, n'est pas adapté à la transmission sur un support qui est, généralement fil de cuivre. Le signal numérique, en se propageant sur le support physique qui est sensible aux parasites, va subir des déformations, qui vont si elles sont très importantes, empêcher la détection correcte du signal à la réception. Le bit envoyé ne correspond pas au bit reçu. La communication avec un signal numérique ne peut être ni vite ni loin.

Pour pouvoir échanger des informations sur des distances importantes, il faudra une adaptation sur les caractéristiques du signal en fonction :

- Des contraintes du médium ;
- De la vitesse de transmission ou débit ;
- De la résistance ou l'immunité aux perturbations ;
- De la distance entre deux stations ou machines communicantes.

Plusieurs solutions existent pour pouvoir communiquer plus vite et à distance plus loin :

- La transmission en bande de base ;
- L'amplification numérique ;
- La modulation d'un signal porteur.

2.2 La transmission en bande de base

La transmission est dite en bande de base lorsque le signal ne subit pas de transposition en fréquence. Le signal présente souvent un aspect rectangulaire, car la fonction de modulation simple utilisée est rectangulaire. Le principe de la transmission en bande de base consiste à modifier le spectre du signal, sans le décaler dans un autre domaine de fréquence, en jouant sur des paramètres d'amplitude ou en associant différents signaux.

La figure ci-dessous résume le principe de la transmission des données en bande de base.

L'inconvénient de bande de base est qu'on peut transmettre les données seulement sur courtes distances avec des débits faibles à moyens, atténuation des signaux, bande passante limitée vers les hautes fréquences, et le problème quand on a une suite de 1 ou de 0.

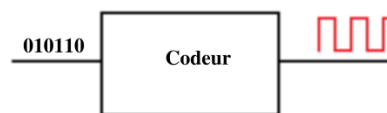


Figure 2.1 : Codeur bande de base.

Le choix d'un code dépend du spectre de ce code, la bande passante disponible du bruit et interférence du canal, du contrôle de la performance, de la tenue en horloge et la fiabilité de la mise en œuvre.

Les principaux codes utilisés sont : NRZ, Miller et Manchester.

2.2.1 Code NRZ : *No Return to Zero* (unipolaire)

Le signal binaire des données est simplement transposé en tension afin d'éviter les valeurs nulles, ce qui annule la composante continue. Ce code présente l'inconvénient de ne pas offrir de repère de synchronisation d'où le risque d'une mauvaise interprétation du signal en réception.

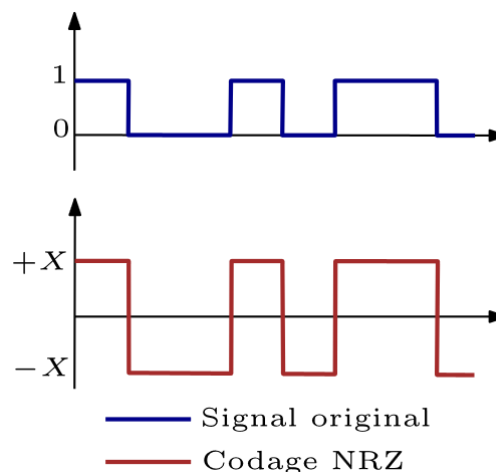


Figure 2.2 : Codage Non-Retour à Zéro.

2.2.2 Code Manchester : *biphase*

Une opération « OU exclusif » est réalisée entre les données binaires à transmettre et le signal d'horloge de transition ce qui amène une transition systématique au milieu de chaque bit du signal binaire à transmettre. L'avantage de cette transition a pour but d'offrir une synchronisation en réception du signal transmis des données pour chaque bit. Ce code est le codage numérique retenu pour la communication Ethernet

La transition se traduit par les règles suivantes :

- Bit de donnée à 0 un front montant ;
- Bit de donnée à 1 un front descendant.

L'allure de ce signal est représentée ci-dessous :

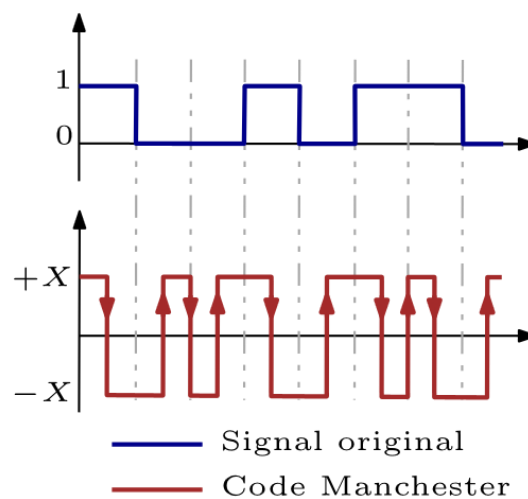


Figure 2.3 : Code Manchester (**biphase**).

2.2.3 Code Miller : *Delay Mode*

Le code de Miller a été obtenu à partir du codage Manchester dans lequel on supprime une transition sur deux. En d'autres termes, les règles d'encodages prennent la forme suivante :

- Si le bit de donnée est égale 1, alors nous insérons une transition au milieu de l'intervalle significatif ;
- Si le bit de donnée vaut 0, alors il n'y a pas de transition au milieu de l'intervalle significatif, mais si le bit suivant est égale 0, alors on place une transition à la fin de l'intervalle significatif.

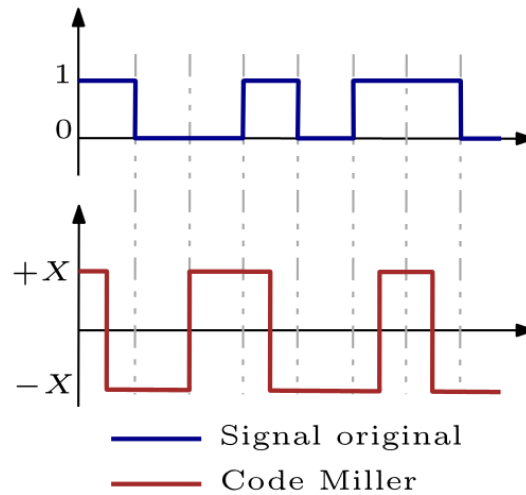


Figure 2.4 : Code Miller.

Par exemple, on remarque que le codage Manchester permet de transmettre environ 85% de la puissance de signal sur la bande passante correspondant à la longueur du premier lobe. Il suffit alors d'utiliser le médium dont la bande passante correspond à cette longueur de bande.

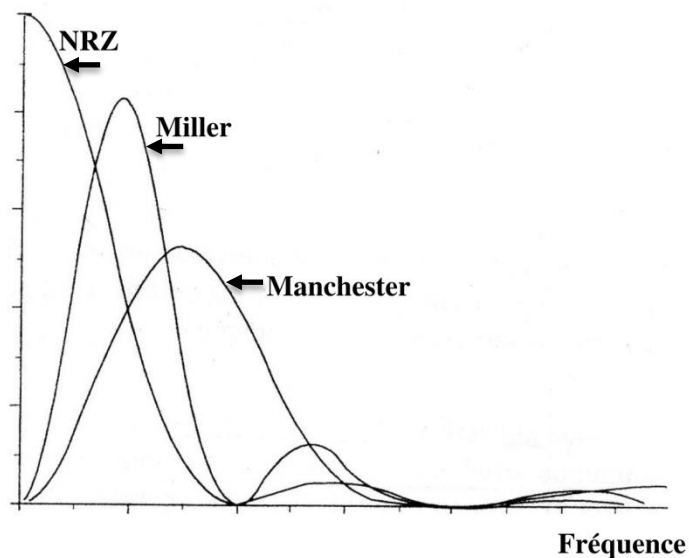


Figure 2.5 : L'allure du spectre pour les trois codages (NRZ, Manchester et Miller).

2.3 L'amplification numérique des signaux

Lorsque la longueur du médium dépasse quelques centaines de mètres, le signal peut se dégrader et se déformer de façon significative. Le taux d'erreur de transmission deviendra alors très élevé. Il est donc nécessaire de régénérer le signal. C'est le rôle de l'amplificateur numérique appelé répéteur dans une architecture de type Ethernet, le répéteur répète ou amplifie les signaux numériques.

2.4 La modulation d'un signal porteur

Lorsqu'on souhaite transmettre des signaux numériques sur des distances de plus de quelques kilomètres, il convient de régler le signal à transmettre.

En effet, si la ligne de transmission est trop longue, même avec des vitesses de transmission faibles, les signaux sont rapidement déformés.

Puisque le signal numérique n'est plus adapté, il faut donc utiliser un signal sinusoïdal dont la forme est plus adaptée. Une ou plusieurs caractéristiques d'un signal sinusoïdal qui sera appelé signal porteur ou bien porteuse.

Le signal sinusoïdal est caractérisé par :

- Son amplitude qui mesure l'importance des variations ;
- Sa fréquence qui quantifie la rapidité de ces variations ;
- Sa phase qui détermine le décalage du signal dans le temps.

La modulation d'un signal c'est effectuer des modifications sur ces caractéristiques, faire varier un ou plusieurs de ces paramètres le définissant en fonction des données à transmettre. Suivant le cas on parlera alors de :

- Modulation d'amplitude : $s(t) = A(t). \sin(ft + \varphi)$(2.1)
- Modulation de fréquence : $s(t) = A. \sin(f(t) + \varphi)$(2.2)
- Modulation de phase : $s(t) = A. \sin(ft + \varphi(t))$(2.3)

Avec $A(t)$ l'amplitude de la porteuse ; $f(t)$ la fréquence de la porteuse en hertz et $\varphi(t)$ la phase de la porteuse.

2.4.1 Modulation d'amplitude

Les deux états 0 ou 1 du signal à transmettre sont représentés par des amplitudes :

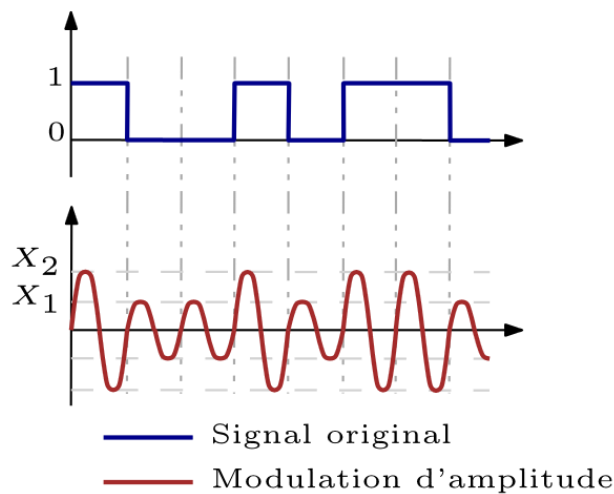


Figure 2.6 : Codage par modulation d'amplitude.

- Si le bit de donnée est égale 0 alors amplitude sera divisé en deux $\frac{A}{2}$;
- Si le bit de donnée est égale 1 alors amplitude du signal égale A.

2.4.2 Modulation de fréquence

Les deux états 0 ou 1 du signal à transmettre sont représentés par des fréquences (f et $2f$).

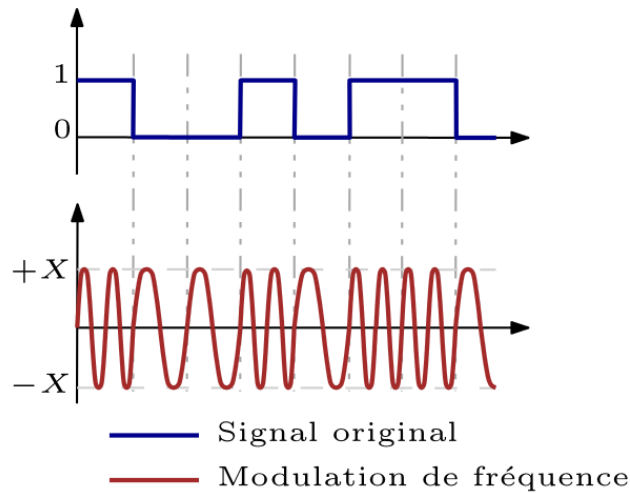


Figure 2.7 : Codage par modulation de fréquence.

- Si le bit de donnée est égale 0 alors fréquence du signal égale $2f$.
- Si le bit de donnée est égale 1 alors fréquence du signal égale f .

2.4.3 Modulation de phase

Les deux états 0 ou 1 du signal à transmettre sont représentés par des angles de phase (0° et 180°).

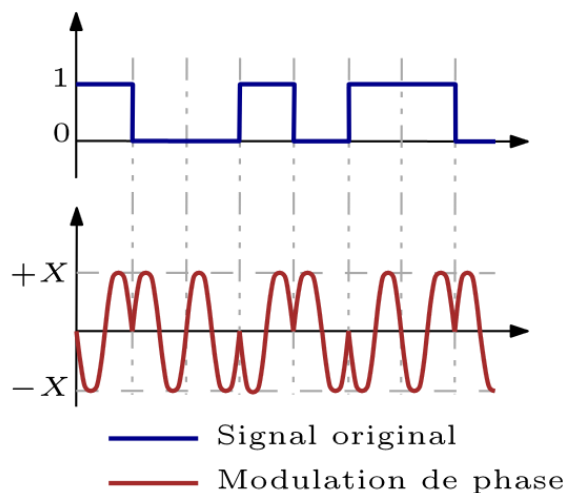


Figure 2.8 : Codage par modulation de phase.

- Si le bit de donnée est égale 0 alors le signal est en phase avec la porteuse.
- Si le bit de donnée est égale 1 alors le signal est en opposition de phase avec la porteuse.

2.5 Type de transmission

La transmission des bits peut s'effectuer en série ou en parallèle. Quel que soit le mode de transmission, l'émission est toujours cadencée par une horloge dont la vitesse donne le débit de la ligne exprimé en bauds.

Les bauds caractérisent le nombre de tops d'horloge générés en une seconde. Par exemple, un débit de 80 bauds autorise 80 émissions de bits par seconde. Si à chaque top d'horloge un signal représentant 0 ou 1 est émis, alors, dans ce cas le débit en bits est équivalent au débit en baud.

2.5.1 Transmission sérielle

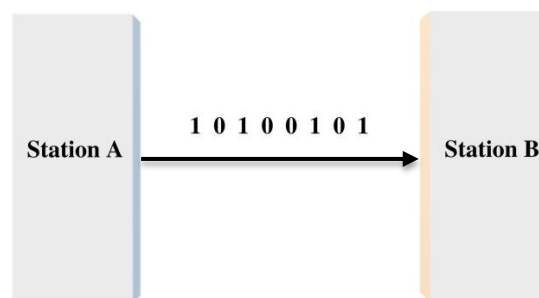


Figure 2.9 : Transmission série.

C'est la liaison série qui est la plus utilisée, elle nécessite en générale trois fils : émission, réception et la masse. Les bits d'un octet sont transmis les uns à la suite des autres de manière synchrone ou asynchrone.

Exemples : les protocoles de communication série RS-232, Rs-422, ...etc

2.5.2 Transmission parallèle

Les bits d'un octet sont transmis simultanément. Cette transmission est utilisée pour les courtes distances, chaque canal peut dégrader et déformer ses voisins et la qualité de l'information se dégrade rapidement. Elle n'est pas utilisée dans les RLI, est surtout utilisée à l'intérieur des réseaux informatiques via un BUS. La longueur de bus 20 m max, 15 stations connectables et 2m max entre deux stations.

Exemple : Les imprimantes peuvent se connecter en « liaison parallèle », via le connecteur CENTRONICS).

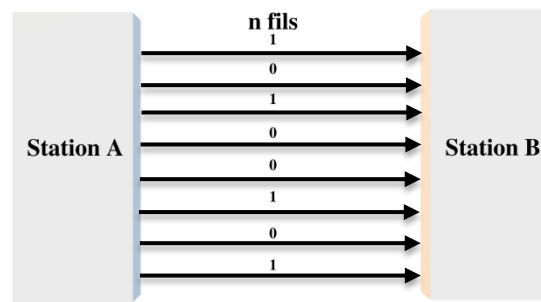


Figure 2.10 : Transmission parallèle de données.

2.6 Mode de transmission

Il existe 3 types de modes de transmission qui sont donnés ci-dessous: le mode simplex, le mode half duplex et le mode full duplex.

2.6.1 Mode simplex

Un mode simplex se caractérise par une transmission unidirectionnelle. Une station A émet vers une station B (TV/parabole).

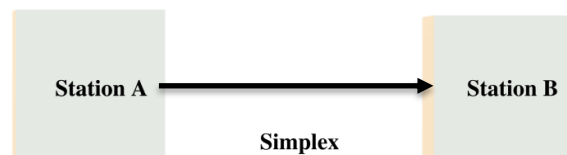


Figure 2.11 : Mode simplex.

2.6.2 Mode semi-duplex (*half duplex*)

Ce mode est bidirectionnel. La station A et la station B peuvent émettre. Toutes fois, ces deux stations ne peuvent pas émettre simultanément. Pendant qu'une station émet, l'autre reçoit.

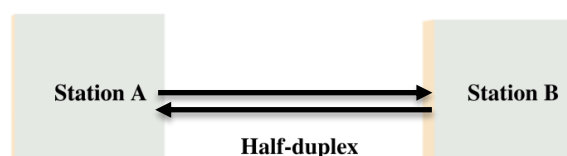


Figure 2.12 : Mode Half-duplex.

2.6.3 Mode duplex (*full duplex*)

Ce mode est bidirectionnel permettant l'émission et la réception simultanée des deux stations A et B.

**Figure 2.13** : Mode Full-duplex.

2.7 Conclusion

Les supports de communication ne sont pas parfaits, car les informations sont très sensibles aux parasites, affaiblissement, déphasage, bruits. L'échanger des informations sur des distances importantes, convient d'adapter des techniques de transmission aux caractéristiques du support de communication. Au vu de ce qui précède, il existe deux grandes techniques de transmission qui sont la modulation d'un signal porteur et la transmission en bande de bas. Ces deux techniques de transmission ne suffisent pas à assurer que les communications se déroulent sans aucune erreur.

Les codes de transmission (NRZ, Manchester, Miller, etc.), chacun possédant certaines des caractéristiques voulues, mais pas toutes, l'inconvénient est qu'on peut transmettre les données seulement sur courtes distances avec des débits faibles à moyens, atténuation des signaux. Pour une transmission sur des distances au-delà du kilomètre, il convient une adaptation du signal à transmettre par un signal porteur, La modulation d'un signal c'est effectuer des modifications sur ses caractéristiques, on parlera alors de modulation de l'amplitude, de fréquence et de phase.

Au cours de ce chapitre, nous avons vu aussi les deux méthodes de transfert de données, à savoir la transmission série et la transmission parallèle. Elles ont leurs avantages et leurs inconvénients. La transmission parallèle est utilisée pour une distance plus courte, fournit une plus grande vitesse. Tandis que, la transmission série est fiable pour le transfert de données à plus longue distance, pas trop d'erreurs et bruit dans la transmission et les données passent seulement par un seul fil.

À la fin de ce chapitre, la transmission de données sur un canal de communication entre deux stations peut s'effectuer de différentes manières. Simultanément dans les deux sens (full-duplex), alternativement dans un sens ou l'autre (half-duplex), ou uniquement dans un sens (simplex).

Chapitre 03 : Étude du modèle OSI des RLI et le modèle TCP/IP sur Ethernet.

3.1 Introduction

Les réseaux locaux industriels ne sont pas construits sur le modèle OSI théorique à 7 couches (contrairement aux réseaux informatiques). Les constructeurs s'y réfèrent et adaptent leurs nouveaux produits en tenant compte du modèle. Un RLI est basé sur la restriction du modèle OSI à 3 couches, la notion de temps est un point très important. Dans une première partie de ce chapitre, nous allons étudier les trois couches des RLI qui sont : la couche physique, qui est indispensable à la communication, la couche liaison de données définit les trames à transmettre et la gestion d'accès au médium, aussi pour détecter les erreurs de transmission et la couche application reste évidemment nécessaire. Les deux couches réseaux et transport ont été définies pour gérer les problèmes des paquets qui transitent par des stations intermédiaires : elles sont inutiles pour les RLI car toutes les stations sont interconnectées. La couche session permet l'échange d'une grande quantité d'informations, ce qui n'est pas le cas pour les RLI. La couche présentation peut être figée et non dynamique ce qui la rend transparente.

Dans une deuxième partie de ce chapitre, nous allons étudier le modèle TCP/IP. Comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI. TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

On peut utiliser le modèle OSI pour situer la fonction technique d'un dispositif d'interconnexion de réseaux. Ainsi, le répéteur se situe au niveau de la couche physique, de même pour le hub ; le pont, donc le *Switch* se situe au niveau de la couche de liaison de données et le routeur se situe au niveau de la couche réseau.

3.2 Étude du modèle OSI à trois couches des RLI

3.2.1 Couche physique

La couche physique gère la transmission des bits de façon brute : et fiable (être sûr qu'un bit à 0 ou à 1 reçu était bien un bit à 0 ou à 1 émit). La couche est régie par des normes et standards qui définissent les types de connecteurs (mécaniques) de signaux émis (mécanique et électrique), les caractéristiques (mécaniques et électriques) des supports de type câbles, fibres optiques..., les mécanismes de transmission synchronisation, sens des échanges, détection d'erreurs de bas niveau...).

3.2.1.1 Les principaux supports utilisés (*Médium*)

Le médium est la liaison physique entre les stations, il existe une grande variété de média. Toutefois il faut en convenir, c'est essentiellement par des liaisons filaires que s'établit la communication. Actuellement, il existe deux types de liaison filaire, les paires torsadées, et les fibres optiques.

Généralement, on utilise une paire torsadée pour réaliser des réseaux de petite taille. En effet, il est souvent plus simple d'accepter un certain taux d'erreur que d'utiliser des médiums à coût élevé.

Les supports de transmission influent sur :

- La vitesse de transmission ;
- La distance ;
- Facilité d'installation (problèmes de raccordement) ;
- Le coût ;
- L'immunité électromagnétique.

Le tableau ci-dessous montre les avantages et les inconvénients des différents supports utilisés.

Support	Avantage	Inconvénient
Cuivre	<ul style="list-style-type: none"> - Faible coût - Large bande - Peu d'atténuation 	sensible aux (IEM Interférences Electromagnétique)
Fibre optique	<ul style="list-style-type: none"> - Peu sensible 	Coût élevé
Sans fil	<ul style="list-style-type: none"> - Mobilité, flexibilité 	Très sensible aux IEM

Tableau 3.1 : Caractéristiques des différents types de supports de transmission

Dans un réseau local, les câbles métalliques sont principalement utilisés pour le câblage. Il existe deux types de câbles métalliques dans le domaine des réseaux : la paire torsadée et le câble coaxial.

3.2.1.1.1 La paire torsadée.

Ce médium est le plus simple à mettre en œuvre, et le moins cher. Certains types de paires torsadées peuvent également être envisagés. Il y a quatre types de câbles. UTP (Unshielded Twisted Pair) est une première version non blindée. Dans un environnement perturbé, son utilisation est bien évidemment à bannir. Deux types de blindages sont possibles, le premier, STP (Shielded Twisted Pair) consiste à insérer une tresse métallique. Le deuxième, FTP (Foiled Twisted Pair), est doté d'une mince feuille d'aluminium ou feuillard. La combinaison des deux, SFTP, présente des avantages dans les environnements perturbés. Les principales catégories de câbles torsadés sont : Paires torsadées UTP La paire torsadée non blindée n'est couvert d'aucun blindage protecteur.

3.2.1.1.1.1 Paire torsadée UTP

La paire torsadée non blindée n'est entourée d'aucun blindage protecteur.

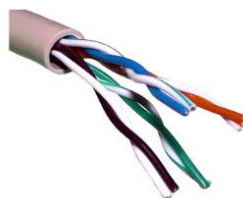


Figure 3.1 : Câble paire torsadée non blindée UTP.**3.2.1.1.1 .2 Paire torsadée FTP**

L'ensemble des paires torsadées contiennent un blindage commun global assuré par une feuille d'aluminium. L'écran se trouve entre la gaine extérieure et les 4 paires torsadées

**Figure 3.2** : Câble blindé avec une mince feuille d'aluminium ou feuillard **FTP**.**3.2.1.1.1 .3 Paire torsadée SFTP**

Câble contient un double écran (feuille métallique et la tresse) commun à l'ensemble des paires.

**Figure 3.3** : Câble reprenant les propriétés **STP** et **FTP****3.2.1.1.1 .4 Paire torsadée SSTP**

Chacune de ces paires sont blindées par un blindage en aluminium, de plus, la gaine extérieure est blindée par une tresse en cuivre étamé.

Exemple : pour mesurer la température ou la pression à longue distance, on utilise les câbles SSTP ou SFTP, car la tension induit par les thermocouples (c'est dans un intervalle en mv)

**Figure 3.4** : Câble double blindé **SSTP**

- **U** (« unshielded ») : non blindé
- **F** (« foil shielding ») : blindage par feuillard
- **S** (« braided shielding ») : blindage par tresse

Les deux câbles SFTP et SSTP, sont utilisés pour les longues distances et la mesure de température ou bien la pression. La tension induit par les thermocouples c'est dans un intervalle de mv, donc une petite perturbation peut erroné l'information.

Les câbles utilisés en industries sont renforcés en fonction du cas d'utilisation et les conditions à la quelles sont exposés tel que les pressions basses et élevées, les produits chimiques, les chocs, ... etc.

3.2.1.1.2 Le câble coaxial



Figure 3.5 : Connecteur BNC à monter sur le câble.

Il se compose d'un conducteur en cuivre (âme), entouré d'un écran mis à la terre (tresse). Entre les deux, une couche isolante de matériau plastique (diélectrique). Le câble a d'excellentes propriétés électriques et se prête aux transmissions à grande vitesse. (Par exemple en Allemagne, les sociétés proposent l'internet à travers ce type de câble, car, l'information est très rapide avec un débit très grand).

Les transmissions dans l'environnement industriel sont souvent soumises à des interférences extrêmes. Par conséquent, le choix des composants utilisés, notamment le choix des supports de transmission est primordial. Dans un milieu perturbé, le câble coaxial épais peut être envisagé.

La connexion d'une liaison coaxiale à un équipement réseau se fait à l'aide de prises du type BNC (*British Naval Connector*).

3.2.1.1.2.1 Le câble coaxial fin

Correspond à un câble relativement souple et dont la gaine en PVC est noire. Il est caractérisé par un diamètre de 6 mm et une vitesse de 10 Mbits/s. Il est souvent utilisé dans les téléviseurs.

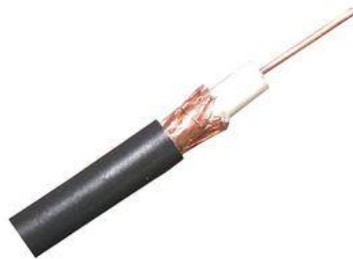


Figure 3.6 : Câble coaxial fin.

3.2.1.1.2 Le câble coaxial épais



Figure 3.7 : Câble coaxial épais.

Il se caractérise par un diamètre de 12 mm, un fil rigide, un débit de 10Mbits/s et essentiellement utilisé pour la transmission des données de plus longue distance grâce à l'épaisseur du fil en cuivre qui a une bonne immunité contre les perturbations. La figure ci-dessus présente un câble coaxial épais a une résistance de 50Ω.

3.2.1.1.3 La fibre optique

La fibre optique est un support de transmission d'informations entre les équipements réseaux en utilisant des signaux lumineux. Les informations échangées entre les équipements se font à l'aide de signaux électriques. Ces signaux électriques sont convertis en signaux lumineux avant d'être transmis sur un câble optique. Le câble optique fait circuler les informations dans un conducteur central en verre ou en plastique. L'ensemble est enveloppé dans une gaine plastique. Lorsque les signaux lumineux atteignent l'équipement cible, ces signaux lumineux sont à nouveau convertis en signaux électriques pour être exploitables. L'installation de la fibre optique est difficile et délicate à cause du conducteur central qui peut être cassé, d'où le coût relativement élevé pour ce type de médium.

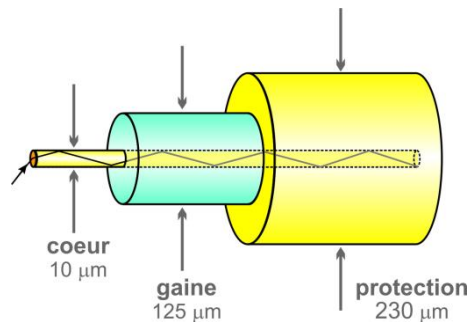


Figure 3.8 : Câble fibre optique.

Les réseaux par fibre optique sont utilisés :

- Quand les champs électromagnétiques perturbent les réseaux conventionnels ;
- lorsque de hauts débits sont nécessaires, car peut atteindre une vitesse de plus de 2 Gbits/s ;
- lorsqu'une éventuelle étincelle causée par une connexion électrique doit être évitée ;
- lorsque les transmissions sont sûres ou des données doivent être transportées sur une grande distance.

Il faut savoir que chaque solution à ces coûts, donc, le choix augmente en faisant la fibre optique.

3.2.1.2 Performance des différents médiums

Support	Débit	Distance	Remarques
Paires métallique torsadées blindée	100-500Kbits/s	1 Km	Pose facile Raccords aisés Immunité moyenne
Coaxial Bande de base	1-100 Mbits/s	2.5 Km	Raccords faciles Bonne immunité
Coaxial large Bande	300 Kbits/s	10-50 Km	Raccords faciles Bonne immunité
Fibres optiques	1Gbits/s	> 10 Km	Prix le plus élevé Immunité parfaite Grande bande passante Atténuation faible

Tableau 3.2 : Comparaison des différents médiums.

3.2.1.3 Normes et standards en transmission de données

Pour transmettre des informations numériques entre deux équipements, nécessite l'utilisation de règles communes : type de liaison, vitesse de transmission, format des données transmises, détection d'erreurs,...etc.

La transmission série est une des transmissions dites asynchrones (RS-232, RS-422, RS-485) car il n'y a pas de signal d'horloge dans le câble ; cela implique que l'émetteur et le récepteur :

- Soient configurés au même débit ;
- La configuration de la liaison soit identique sur les deux équipements informatiques utilisés (nombre de bits de chaque donnée identique, nombre de bits de stop identique ;
- utilisation d'un même type de bit de parité (qui est un des moyens utilisés pour vérifier l'intégrité des données transmises à la réception) sur les deux équipements.

Les ingénieurs et les techniciens interviennent en utilisant de simples commandes en lignes. C'est pourquoi la traditionnelle prise SUB-D mâle à 9 contacts se trouve toujours en façade des équipements réseaux professionnels.

3.2.1.3.1 La norme EIA RS-232

L'EIA (*Electronic Industrial Association*) a créé le standard RS-232 en 1962 dans le but de normaliser l'interface entre les équipements. Le RS-232 assure les transmissions de types, half-duplex, full-duplex et simplex. La liaison point à point assurée par un connecteur SUB-D avec 9 broches (voir figure ci-dessous). La distance assurée est inférieure à 15 mètres avec un débit inférieur à 20 Kbits/s.

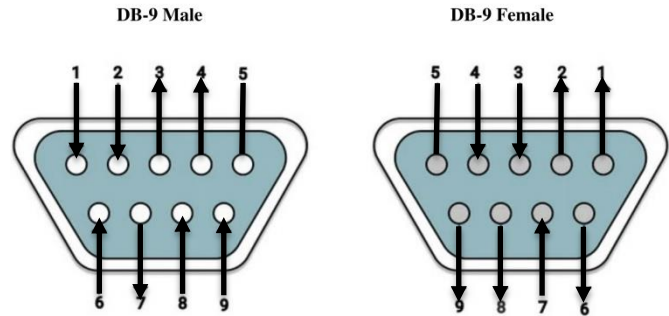


Figure 3.9 : Connecteurs standard DB9.

Le tableau suivant présente le brochage du connecteur DB-9.

1	CD	Carrier Detect	Détection de porteuse (pour les modems)
2	RXD	Receive Data	Réception de données
3	TXD	Transmit Data	Transmission de données
4	DTR	Data Terminal Ready	Terminal prêt
5	GND	Signal Ground	Masse logique
6	DSR	Data Set Ready	Données prêtes
7	RTS	Request To Send	Demande d'émission
8	CTS	Clear To Send	Prêt à émettre
9	RI	Ring Indicator	Indicateur de sonnerie (pour les modems)

Tableau 3.3 : Brochage du connecteur DB-9

Très souvent, 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 RX, TX et GND. La liaison à mettre en œuvre dans la figure ci-dessous est une liaison dite *croisée*.

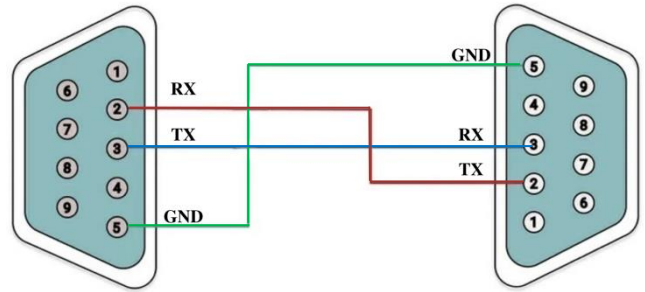


Figure 3.10 : Liaison à trois fils (croisée).

3.2.1.3.2 La norme EIA RS-422

Décrit une interface de communication fonctionnant sur des lignes différentielles capables de connecter un dispositif émetteur à un maximum de 10 récepteurs. Le débit pouvant atteindre plusieurs Mbit/s, selon la longueur du bus (de 100 kbit/s sur ligne de 1219 m à 10 Mbit/s sur ligne de 12 m). Le support physique défini pour RS-422 est constitué de deux paires torsadées. L'utilisation de deux paires permet la transmission et la réception de données entre le maître et l'esclave au même temps. La possibilité de transmission et de réception simultanées caractérise le RS-422 en full-duplex.

3.2.1.3.3 La norme EIA RS-485

Décrit une interface de communication fonctionnant sur des lignes différentielles capables de communiquer avec 32 récepteurs. Généralement, un appareil émetteur-récepteur correspond à une « unité de charge », ce qui rend possible de communiquer avec 32 appareils au maximum. Le débit peut atteindre plusieurs Mbit/s, selon la longueur du bus (de 100 kbit/s sur ligne de 1200 m à 35 Mbit/s sur ligne de 10 m). Le support physique le plus largement utilisé est une paire torsadée. Grâce à cette paire de fils unique, chaque appareil transmet et reçoit des données. Chaque appareil déclenche son émetteur uniquement au moment où il doit émettre, le laissant inactif le reste du temps pour permettre aux autres appareils de transmettre des données. À un moment donné, un seul dispositif peut transmettre, ce qui caractérise ce réseau en half-duplex. Un réseau RS-485 peut également utiliser 2 paires torsadées fonctionnant en mode full-duplex, entièrement compatibles avec RS422.

De nombreux constructeurs des automates programmables industriels ont adopté l'interface RS-485 pour la mise en œuvre de leur bus d'automates tels que : Modbus, Jbus, Profibus,etc.

3.2.1.4 Transmission synchrone et asynchrone

À cause de problèmes d'interférences électromagnétiques entre les conducteurs posés par la liaison du type parallèle, c'est la liaison sériée qui est la plus utilisée. Toutefois, puisqu'un seul fil transporte l'information, il existe un problème de synchronisation entre l'émetteur et le récepteur, car les bits sont envoyés successivement. On distingue donc deux types de transmission permettant de remédier à ce problème :

3.2.1.4.1 Transmission asynchrone

Pour une transmission asynchrone, chaque donnée est émise de façon irrégulière dans le temps, donc, la transmission se fait sans signal d'horloge commune entre l'émetteur et le 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 des données est la procédure dite « *Start-Stop* » qui correspond au chronogramme suivant :

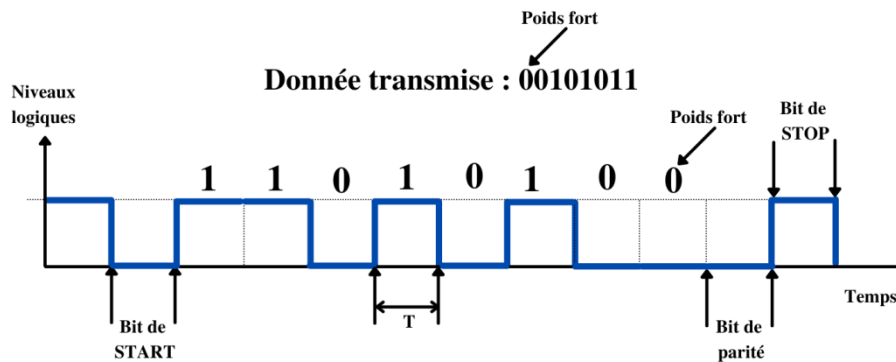


Figure 3.11 : Chronogramme d'une transmission asynchrone des données « *Bit de START-bit de STOP et bit de Parité* ».

Chaque donnée transmise est précédée d'une information indiquant le début de la transmission de données et terminée par l'envoi d'une information de fin de transmission appelée bit STOP.

La donnée à transmise peut être représentée sur 5 à 8 bits. Parfois un bit supplémentaire est ajouté après la donnée : c'est le bit de « *parité* ».

3.2.1.5 Le contrôle d'erreurs

Les signaux électriques peuvent subir des interférences (distorsion, bruit), notamment lors de la transmission des données sur une longue distance. Ainsi, le contrôle de la validité des données est nécessaire pour certaines applications. C'est pourquoi il existe des mécanismes permettant de garantir un certain niveau d'intégrité des données. La protection contre les erreurs peut se faire de deux façons : soit en fiabilisant le support de transmission, soit en mettant en place des mécanismes logiques de détection et de correction des erreurs.

Plusieurs mécanismes sont utilisés tels que :

- Le codage de la parité.
- Le contrôle de redondance cyclique CRC (*Cyclic Redundancy Check*)).

3.2.1.5.1 Codage de la parité

Le bit de parité est généré par l'interface de communication pour détecter les erreurs de transmission. On parle alors de parité « *paire* » et de parité « *impaire* ». Pour former un octet avec le bit de parité) dont la valeur (0 ou 1) est telle que le nombre total de bits à 1 soit pair, il consiste à ajouter un 1 si le nombre de bits du mot de code est impair, 0 dans le cas contraire.

Exemple :

Dans la (figure 3.12a), le nombre de bits de données à 1 est pair, le bit de parité est donc positionné à 0. Par contre, dans la (figure 3.12b) les bits de données étant en nombre impair, donc, le bit de parité est à 1

À la réception, l'interface calcule la parité et compare le résultat au bit de parité transmis. Imaginons la transmission de bit de poids faible de l'octet précédent soit victime d'une perturbation (fig 3.12d): Le bit de parité ne correspond alors plus à la parité de l'octet : une erreur est détectée.

La (figure 3.12c) montre si deux bits de même niveau sont altérés dans la transmission, l'erreur ne sera pas alors détectée.

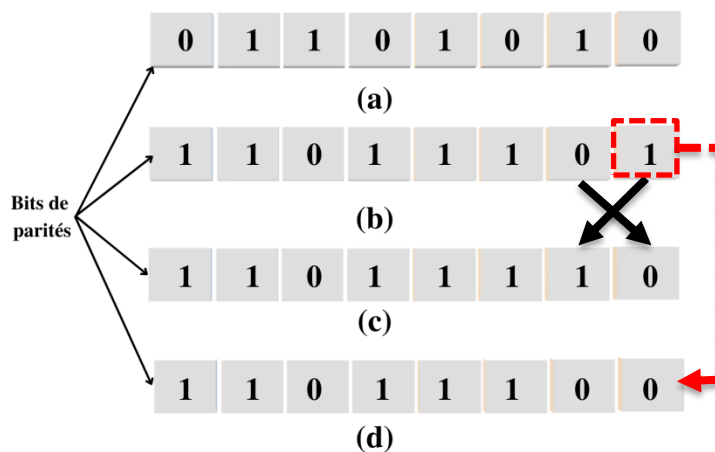


Figure 3.12 : calcul de parité.

La méthode de contrôle de parité ne détectant que les erreurs en nombre impair, ce contrôle ne permet donc de détecter que 50% des erreurs. Cette méthode de détection d'erreurs possède l'inconvénient de ne pas permettre de corriger les erreurs détectées, le seul moyen est de refaire la retransmission de l'octet erroné).

3.2.1.5.2 Le contrôle de redondance cyclique CRC

Le contrôle de redondance cyclique est un moyen de contrôle d'intégrité de données puissantes et faciles à mettre en œuvre. Il représente la principale méthode de détection d'erreurs utilisée pour la transmission des données. Pour faire cela, l'expéditeur de la donnée calcule une valeur "Checksum CRC" qui est fonction du contenu du message, puis l'ajoute à la fin du message. Le destinataire effectue le même calcul et vérifie si la «Checksum» est la même que la valeur de l'expéditeur. La création du code CRC implique l'utilisation d'un code: générateur polynomial noté G(x).

La séquence binaire (0111011101) peut être représentée sous la forme polynomiale suivante :

$$0 * X^9 + 1 * X^8 + 1 * X^7 + 1 * X^6 + 0 * X^5 + 1 * X^4 + 1 * X^3 + 1 * X^2 + 0 * X^1 + 1 * X^0 \dots\dots(3.1)$$

Soit :

$$X^8 + X^7 + X^6 + X^4 + X^3 + X^2 + X^0 \dots\dots\dots(3.2)$$

Ou encore :

$$X^8 + X^7 + X^6 + X^4 + X^3 + X^2 + 1 \dots\dots\dots(3.3)$$

Ce polynomial est le diviseur, les données (informations) sont dividende et le reste de la division et le résultat.

Le CRC et la somme de contrôle sont tous deux excellents pour découvrir les erreurs aléatoires de transmission, mais offrent peu de protection contre une attaque intentionnelle sur les données.

Exemple

On veut émettre le message 1011101001, on utilise pour cela un contrôle CRC avec le polynôme: $G(x) = X^4 + X^1 + X^0$.

Solution

$G(x) = 10011$

On rajoute 4 bits nuls au dividende (**10111010010000**) car le polynôme est de puissance 4.

Le CRC est égal au reste de la division de message M par G : **0110**, donc le message à transmettre est : **10111010010110** (figure 3.13a).

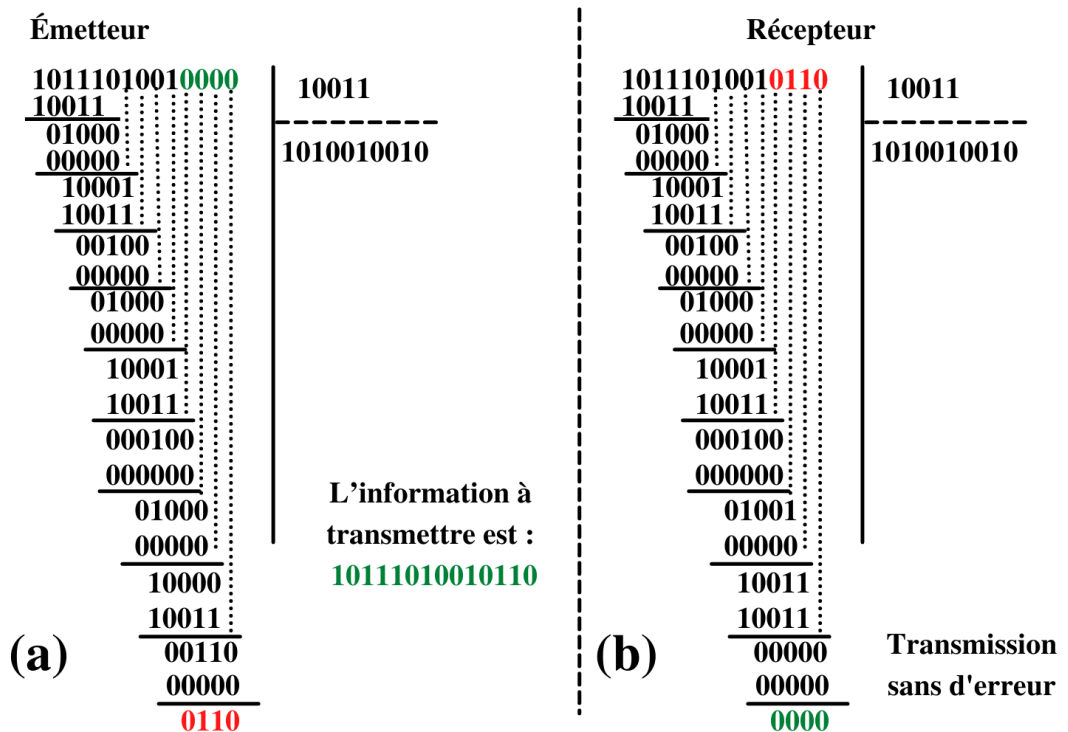


Figure 3.13 : (a) calcul de la valeur CRC (b) Vérification de validité de message en réception.

A la réception, on refait la même opération et le résultat est nul alors l'information est correcte (figure 3.13b).

On remarque que le taux de détection avec un contrôle CRC est quasi-parfait, il y a très peu de chance qu'il ne découvre pas l'erreur.

3.2.1.6 Transmission synchrone

Une transmission est dite synchrone lorsque l'émetteur et récepteur sont cadencés à la même horloge. Le récepteur reçoit de façon continue les données selon le débit de l'émetteur. C'est pour cela il est indispensable qu'émetteur et récepteur soient cadencés à la même vitesse. Pour s'assurer qu'il n'y a pas d'erreurs lors de la transmission, on doit insérer des informations supplémentaires.

L'inconvénient majeur cette transmission est qu'il peut exister des différences entre les horloges de l'émetteur et du récepteur. C'est pour cela chaque envoi consomme une période assez longue pour que le récepteur la distingue. Ainsi, la vitesse de transmission ne peut pas être élevée pour ce type de transmission.

3.2.1.7 Dispositifs d'interconnexion de réseaux

Pour construire un réseau, il faut non seulement les équipements aux câbles, mais, très souvent, il est indispensable de connecter des réseaux entre eux. Différents types d'équipements sont à la disposition de l'administrateur pour mettre en œuvre ces interconnexions.

3.2.1.7.1 Le répéteur

Est un dispositif qui intervient au niveau de la couche physique : sa fonction est de répéter le signal pour étendre la distance de câblage. Le répéteur peut aussi constituer une interface entre deux supports physiques de types différents (RS485 vers fibre optique). Le *hub* également est un répéteur multiport, le trafic provenant d'un hôte est diffusé sur les autres ports. Tout en répétant les signaux réseaux.

3.2.1.7.2 Le Pont

Permet de filtrer le trafic sur un réseau local et établir une connectivité avec d'autres segments du réseau pour le trafic qui y est destiné. Le pont fait le suivi des adresses MAC se trouvant de chacun de ses côtés et prend des décisions en fonction de cette liste d'adresses. Le *switch* et fait partie de cette catégorie, il prend des décisions en fonctions des adresses MAC et améliore les performances du réseau.

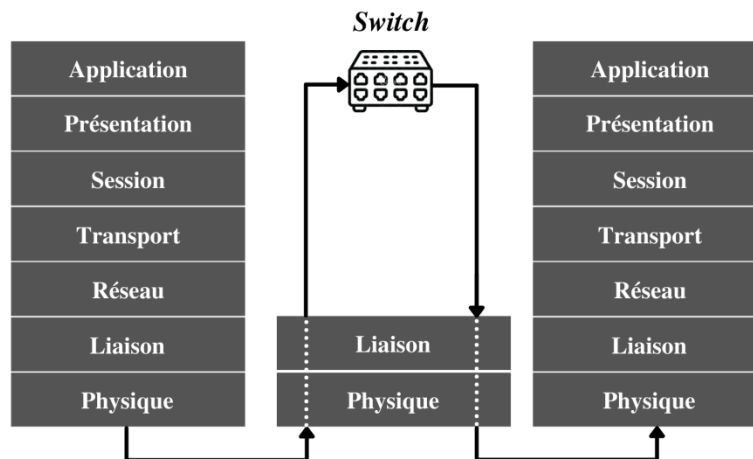


Figure 3.14 : Connexion de deux appareils à un réseau Ethernet à travers l'équipement « Switch ».

3.2.1.7.3 Le routeur

Achemine les données entre les différents réseaux qu'il interconnecte (réseaux de même nature), il connaît les routes à emprunter pour joindre tel ou tel hôte ou du moins l'adresse du prochain routeur susceptible de la connaître. Parce que, il maintient une table de routage qui décrit les routes disponibles.

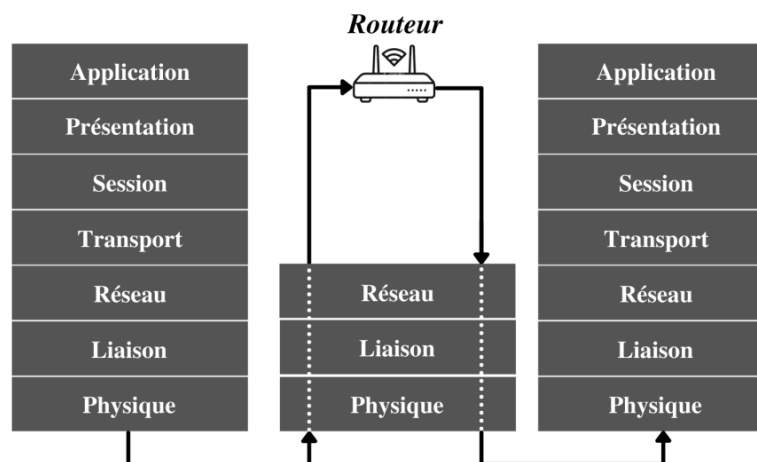


Figure 3.15 : Connexion de deux réseaux de même nature à travers l'équipement « Routeur ».

La passerelle (Gateway) permet de relier deux réseaux de nature différente (Exemple : passerelle Modbus) Il y a deux situations d'acheminement d'un paquet, le destinataire appartient au même réseau local ou bien il appartient à un autre réseau, donc, une passerelle doit toujours être un routeur, mais un routeur ne doit pas nécessairement être une passerelle.

Dans les RLI, deux équipements sont très important, le switch voir (figure 3.14) et le Routeur (figure 3.15).

3.2.2 La couche liaison de données

Si tout le monde parle en même temps, on ne va pas comprendre et le message ne sera pas transmis, donc, c'est la même chose si deux nœuds tentent de transmettre sur un bus, le message ne sera pas transmis à cause du problème de collision. La couche de liaison des données du modèle de communication OSI est très importante dans les réseaux locaux industriels. En effet, c'est la couche de liaison qui définit les trames à transmettre et la gestion d'accès au médium. Elle comprend deux sous couches :

- La sous couche MAC (Media Access Control) ou bien, accès à la voie ;
- La sous couche LLC (Logical Link Control).



Figure 3.16 : Décomposition en sous couche de la couche de liaison de données.

3.2.2.1 La sous-couche MAC

La sous couche MAC assure l'accès au support de transmission. En effet, la plupart des transmissions étant de nature électrique, un problème se pose lorsque deux nœuds veulent émettre sur le médium. Il existe plusieurs méthodes pour assurer que deux nœuds ou plus ne transmettront jamais de trames simultanément sur le réseau. Les techniques MAC peuvent être partagées en trois groupes, selon les règles auxquelles doivent se conformer les nœuds pour accéder au support de transmission : méthodes par consultation, méthodes par compétition et méthodes par multiplexage.

Le choix d'une technique d'accès au médium dépend de plusieurs critères, notamment : la topologie du réseau, le type de support physique, le déterminisme d'accès, la possibilité de privilégier certains nœuds et la tolérance aux fautes.

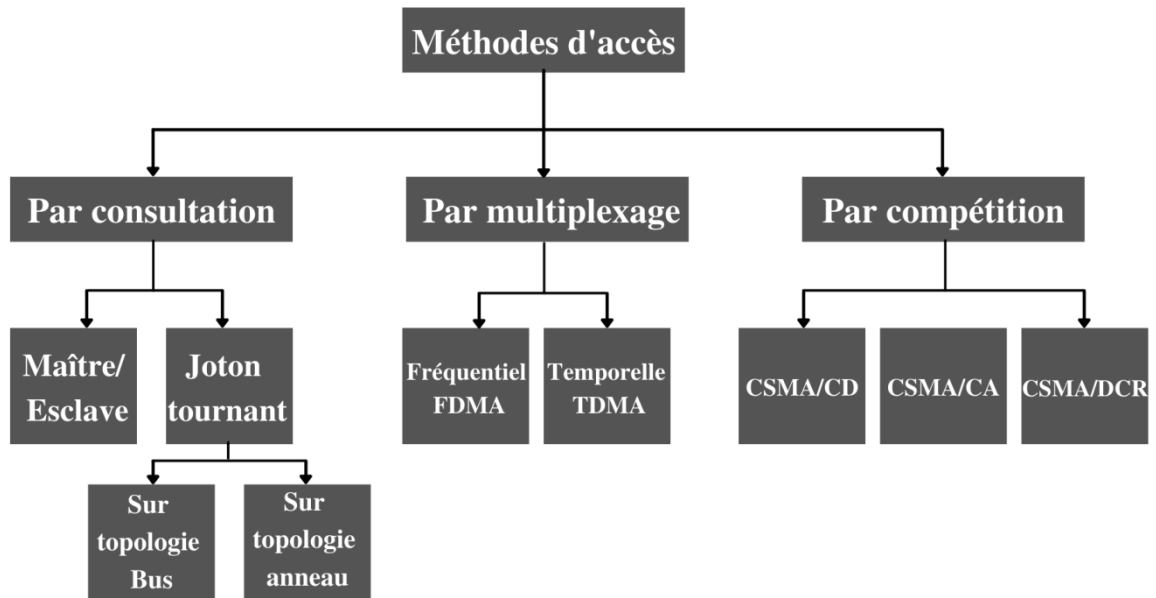


Figure 3.17 : Classes de techniques d'accès au médium.

3.2.2.1.1 Méthodes d'accès par multiplexage

3.2.2.1.1.1 Multiplexage temporel (TDMA : Time Division Multiple Access)

Ce protocole est connu sous le nom de **TDMA** (Time Division Multiple Access). Il est utilisé souvent dans le domaine de la téléphonie, l'adresse est implicite, la position de l'information dans le flot désigne l'émetteur. Le temps d'accès alloué à chaque utilisateur est constant quels que soient ses besoins et chaque utilisateur intervient cycliquement.

L'inconvénient majeur du protocole **TDMA** synchrone est que lorsqu'un nœud n'a pas de données à émettre, le support reste libre, même si d'autres nœuds ont beaucoup de trames à transmettre. Par exemple, nous avons quelques stations reliés entre eux. S'il y a une station qui ne veut pas envoyer ou partager l'information, donc le reste des stations doivent attendre aussi jusqu'à ce que son temps sera fini puis va transmettre l'information.

3.2.2.1.1.2 Multiplexage fréquentiel (FDMA : Frequency Division Multiple Access)

Dans ce protocole, la bande de fréquence du réseau est divisée en sous-canaux, et chaque nœud n'est autorisé à émettre que sur un seul sous-canal qui lui est réservé. Il est à noter que cette méthode est largement utilisée dans le domaine radio (où chaque canal radio émet sur une bande de fréquences qui lui est réservées).

3.2.2.1.2 Méthodes d'accès par compétition

L'accès au médium est aléatoire, il n'y a pas un équipement software ou hardware qui permet aux nœuds de se mettre d'accord pour accéder au support ; chaque nœud peut commencer à transmettre dès qu'il le souhaite. Cela conduit évidemment à des situations de conflit d'accès (collision) quand deux ou plusieurs nœuds transmettent simultanément. Plusieurs solutions

ont été proposées pour gérer ce problème. Dans le contexte des réseaux locaux, c'est essentiellement la technique CSMA et ses variantes qui sont utilisées. Le protocole utilise les composantes suivantes :

- Détection de trafic (pour connaître si la voie est libre ou occupée) ;
- Actions pour démarrer l'émission si la voie est libre ;
- Détection de conflit (collision) ;
- Résolution des conflits détectés.

Les principales techniques d'accès aléatoires sont :

3.2.2.1.2.1 Technique CSMA/CD (Carrier Sens Multiple Access Collision Detect)

Dans un protocole CSMA/CD « Carrier Sense Multiple Access with Collision Detection », le nœud qui veut émettre doit détecter d'abord si la voie est libre. Si la voie n'est pas libre, le nœud annule sa tentative jusqu'à la prochaine libération de la voie. Si la voie est libre, le nœud peut commencer son émission et compare le contenu envoyé avec le contenu reçu, s'il y a une différence entre les deux signaux, il y'a une forte probabilité qu'au moins un autre nœud soit en train de transmettre en même instant que lui. Dans ce cas, il annule sa tentative de transmission, envoie un signal de brouillage pour signaler la collision aux autres nœuds, attend pendant un certain délai aléatoire avant de retenter sa transmission. L'inconvénient de cette méthode est que si le nombre de nœuds qui souhaitent transmettre est important le nombre de collisions devient tel qu'aucun de ces nœuds n'arrivent à transmettre sa trame. Par conséquent, la méthode CSMA/CD n'est pas adaptée aux applications en temps réel. Il peut être combiné avec toutes variantes CSMA. Si un nœud désire émettre une trame, il doit vérifier l'état du médium si 'il est libre ou non :

- Si le support est libre, l'émission peut commencer. Le nœud émetteur vérifie (écoute du support) pendant la transmission qu'il n'y a pas de collision ;
- Si la transmission s'est effectuée sans collision, remise d'un rapport de succès à la couche supérieure ;
- S'il y a collision, le nœud émet une séquence de brouillage puis lance une temporisation aléatoire avant de tester la disponibilité du support pour un nouvel essai. La temporisation aléatoire est tirée dans un domaine qui augmente avec le nombre de collision de la trame afin de réduire le taux de charge (et le risque d'écroulement du réseau) ;
- Le nombre d'essais pour une même trame est limité à 16.

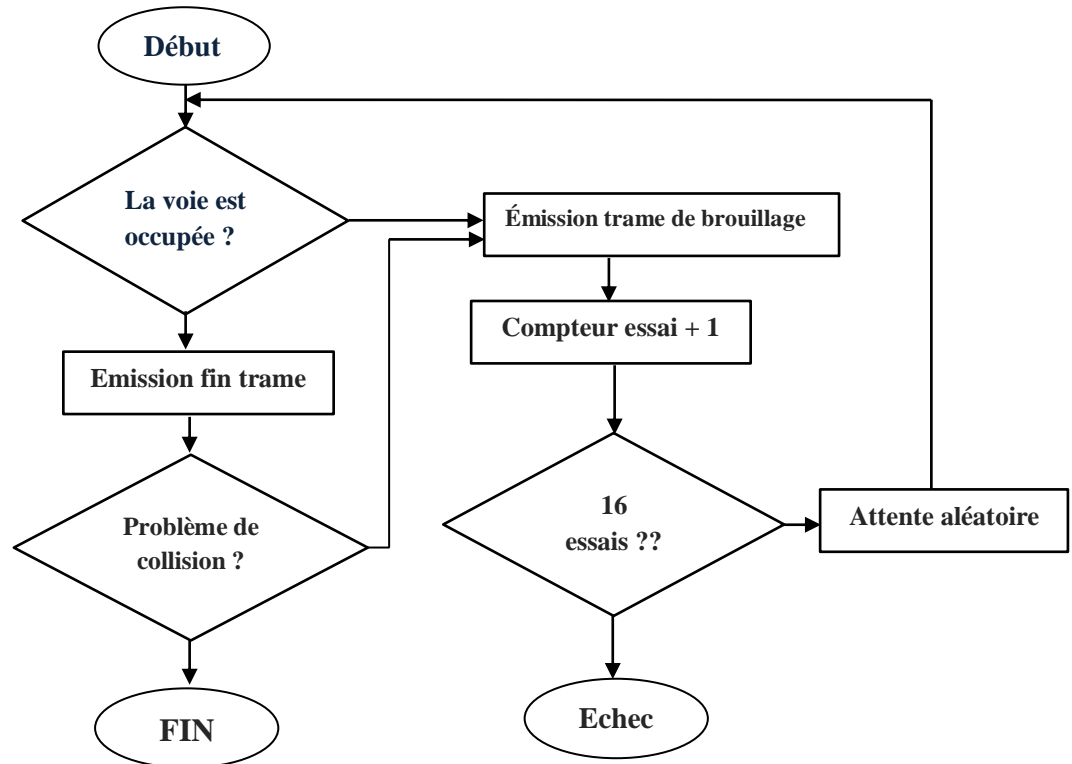


Figure 3.18: L'organigramme de l'algorithme CSMA/CD.

Pour éviter les collisions en chaîne conduisant à des temps de réponse excessifs, des améliorations de la méthode CSMA/CD ont été proposées, notamment la technique CSMA/DCR

3.2.2.1.2.2 Technique CSMA/CA (Collision Avoidance)

Ce protocole s'utilise dans les réseaux sans-fil, il est basé sur un principe d'accusé de réception réciproques entre l'émetteur et le récepteur. Le nœud souhaitant émettre écoute le réseau :

- Si le médium est encombré, la transmission est différée ;
 - Si le médium est libre pendant un temps donné appelé *DIFS* (*Distributed Inter Frame Space*), alors le nœud peut émettre ;
- 1) Le nœud transmet un message **RTS** (Request To Send) c.-à-d. prêt à émettre. Ce message contient des informations sur le volume des données qu'il souhaite émettre et sa vitesse de transmission ;
 - 2) Le récepteur généralement un point d'accès répond un **CTS** (Clear To Send) c.-à-d. le champ libre pour émettre ;
 - 3) Le nœud commence l'émission des données ;
 - 4) Lorsque le nœud reçoit toutes les données, il envoie un accusé de réception (**ACK**).

Tous les nœuds avoisinants patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

Exemple

Nous avons deux nœuds, nœud A et nœud B qui souhaitent envoyer un message au nœud C :

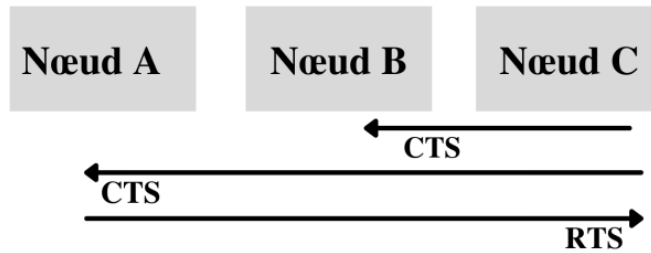


Figure 3.19 : Exemple du protocole CSMA/CA.

- Nœud A transmet un RTS au nœud C ;
- Nœud C transmet un CTS au nœud A ;
- Nœud B entend CTS provenant du nœud C ;
- Nœud B attend la fin de transmission de nœud A.

3.2.2.1.3 Technique CSMA/DCR (*Deterministic Collision Resollision*)

Le protocole CSMA/DCR est une évolution du protocole CSMA/CD, il intègre un algorithme de résolution de collision initié par tous les nœuds qui détectent une collision. L'algorithme utilisé pour cette technique est un algorithme de résolution en arbre binaire : La technique consiste à attribuer un numéro d'index à chacun des nœuds, en cas de conflit, les nœuds sont divisés en deux groupes selon leurs adresses : un groupe des gagnants et un groupe des perdants. Les nœuds appartenant au groupe des perdants cessent d'émettre, les autres tentent de transmettre. Si le groupe des gagnants contient plus d'un nœud, une nouvelle collision est susceptible d'être détectée, auquel cas le groupe est à nouveau partagé en deux, et ainsi de suite jusqu'à ce que le groupe des gagnants ne contienne qu'un seul nœud qui peut alors transmettre tranquillement sa trame. Cette technique permet de limiter le temps d'attente pour transmettre une trame. Toutes les techniques CSMA sont assez intéressantes puisque le problème de collision est en partie ou totalement résolu. La question que l'on peut poser c'est d'imaginer ce qui se passe si une information d'arrêt d'urgence sur un réseau local est envoyée.

Exemple

L'exemple du tableau ci-dessous, 5 nœuds sur 8 souhaitent parler en même temps, on se trouve alors dans un cas de conflit de 5 nœuds.

Le plan de gestion des collisions est le suivant où :

I : interdiction de dialoguer ;

C : collision ;

E : Émission.

Étape	Nœud 1	Nœud 2	Nœud 3	Nœud 4	Nœud 5	Nœud 6	Nœud 7	8	Temps
1	C	C		C			C	C	↓
2	C	C	I	C	I	I	I	I	
3	C	C	I	I	I	I	I	I	
4	E	I	I	I	I	I	I	I	
5	I	E	I	I	I	I	I	I	
6	I	I	I	E	I	I	I	I	
7	I	I	I	I	I	I	C	C	
8	I	I	I	I	I	I	E	I	
9	I	I	I	I	I	I	I	I	
10	I	I	I	I	I	I	I	E	

Tableau 3.4 : Plan de gestion des collisions dans la technique CSMA/DCR.

Puisque 5 nœuds souhaitent parler en même temps, donc il y a 5 collisions sur 8 :

- Étape 01 : collision initiale entre les nœuds (1, 2, 4, 7 et 8) ;
- Étape 02 : Seuls les sites du premier groupe émettent à nouveau (Nœuds 1, 2 et 4) ;
- Étape 03 : Collision entre le nœud 01 et le nœud 02 ;
- Étape 03 : Collision entre le nœud 01 et le nœud 02 ;
- Étape 04 : Nœud 01 du groupe 01 a réussi à émettre ;
- Étape 05 : Nœud 02 du groupe 01 a réussi à émettre ;
- Étape 06: Nœud 04 du groupe 01 a réussi à émettre ; ensuite, on passe au deuxième groupe ;
- Étape 07: Collision entre le nœud 07 et le nœud 08 ;
- Étape 08 : Nœud 07 du groupe 02 a réussi à émettre ;
- Étape 09 : Interdiction d'envoi
- Étape 10 : Nœud 08 du groupe 02 a réussi à émettre.

3.2.2.1.3 Méthodes d'accès par consultation

Le principe de base des techniques par consultation est très simple, les nœuds se consultent pour déterminer qui a le droit d'accéder au médium.

3.2.2.1.3.1 Méthodes d'accès maître-esclave

Dans les techniques maître-esclave, les nœuds sont regroupés en deux catégories : un nœud maître et des nœuds esclaves. Un nœud esclave n'a le droit d'émettre que si le nœud maître l'autorise. Les règles appliquées pour que le maître autorise les esclaves à émettre sont en particulier, dans les installations industrielles, on trouve souvent les deux méthodes suivantes :

Méthode par scrutation régulière

Le nœud maître demande séquentiellement aux autres nœuds s'ils veulent émettre des données. Si la réponse est positive, le nœud maître donne le droit d'accès à l'esclave pendant une durée limitée. Si le nœud esclave n'a pas de trame à transmettre, il rend immédiatement le droit d'émettre au nœud maître. L'inconvénient de cette méthode est qu'il y a parfois une perte de temps à scruter des nœuds qui n'ont rien à transmettre.

Méthode utilisant une table d'arbitre

Dans cette technique, le maître est appelé arbitre du réseau et possède une table qui lui indique à quel moment exactement il faut scruter un nœud esclave. Dans ce cas, le nœud esclave interprète le scan comme une requête à envoyer. Parmi les réseaux de terrain qui utilise cette méthode est le réseau WorldFIP qu'on va voir dans le prochain chapitre.

3.2.2.1.3.2 La méthode d'accès par jeton tournant

Ce type de gestion repose sur la circulation sur la circulation entre les nœuds actifs d'un droit d'accès au médium appelé JETON. Les plus utilisés sont jeton sur bus standardisé ISO 8802.4 et jeton sur anneau standardisé ISO 8802.5.

Protocole sur topologie en anneau

Chaque nœud est connecté au suivant, le dernier étant relié au premier. Un jeton est une trame de bits qui passe d'un nœud à l'autre. L'ordre dans lequel les jetons sont transmis est défini par l'ordre physique dans lequel les nœuds sont connectés. Chaque nœud n'a le droit d'émettre que s'il reçoit le jeton. Si un nœud a une trame à émettre, il attend le jeton, il le capture, il émet la trame, et attend que la trame fasse le tour complet, et retire la trame, c'est-à-dire qu'ayant dû connaître quel était le nœud émetteur, il ne réémet plus la trame mais le jeton passe au nœud suivant et ainsi de suite. Cette méthode retenue par IBM dans son réseau *TOKEN RING*.

Protocole sur topologie en bus

Il présente l'avantage d'être déterministe, et par-là même, de permettre un fonctionnement temps réel d'un réseau de type bus. Le jeton circule entre les nœuds actifs dans un ordre invariable, parcourant ainsi une boucle logique. Cette boucle est ordonnée dans le sens des adresses décroissantes des nœuds, la fermeture étant assurée par le nœud d'adresse la plus faible transmet le jeton à celle d'adresse la plus élevée.

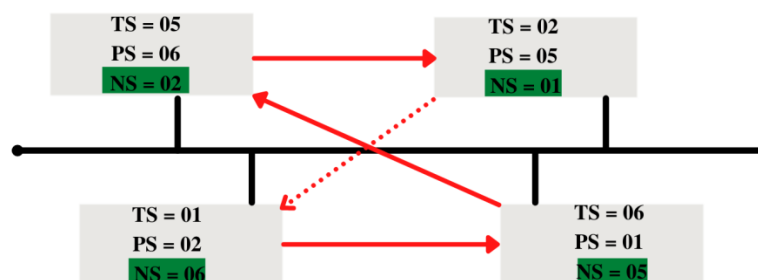


Figure 3.20 : Exemple de circulation du jeton dans une topologie en bus.

La circulation du jeton est réalisée à l'aide de 3 registres, désignant le nœud actif TS (*This Station*), les deux autres un registre désignant respectivement les nœuds précédents PS (*Previous Station*) et NS (*Next Station*) voir (figure 3.20)

3.2.2.2 La sous-couche LLC (Logical Link Control)

La sous-couche LLC de contrôle de la liaison logique est la moitié haute de la couche de liaison de données en particulier de la couche réseau, ou dans **les réseaux locaux** de la couche **d'application**. Elle permet de fiabiliser le protocole MAC par un contrôle d'erreur et un contrôle de flux, puisque l'envoi d'un datagramme ne garantit pas à son émetteur que le ou les destinataires l'on reçu.

3.2.2.2.1 Les SAP (Service Access Point) ou LSAP

LSAP sont des fonctions permettant de créer des accès à la couche application. Chaque SAP est identifié par une adresse codée sur 8 bits. Les 7 bits de poids faible repèrent l'adresse individuelle, tandis que le 8ème bit définit le groupe auquel appartient SAP pour l'accès de groupe.

Les SAP ne sont que des points d'accès (entêtes de fonctions), on distingue trois corps de fonctions qui sont définis par services (qualité):

- LLC1 : est le service minimal sans connexion et sans acquittement ;
- LLC2 : Service avec connexion et avec acquittement ;
- LLC3 : Service sans connexion et avec acquittement.

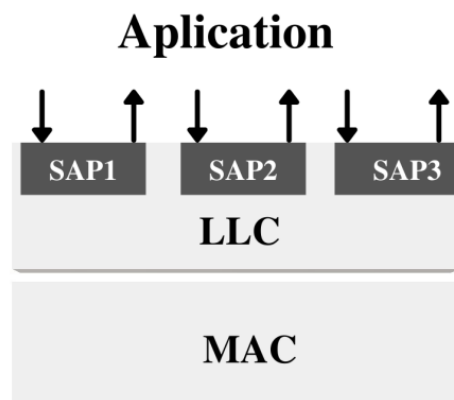


Figure 3.21 : Point d'accès au service LLC.

Fonctionnement type 01 (LLC 1)

Ce mode est le plus simple, il permet juste l'émission et la réception des paquets sans garantir ni le contrôle de flux, ni établissement de connexion logique avec le récepteur, ni même la vérification de bonne réception des données.

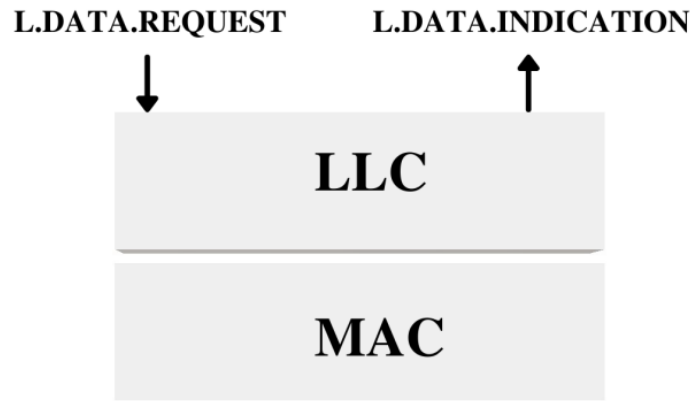


Figure 3.22 : Service de type 01 (LLC 1).

.Ce service dispose de deux commandes au niveau de chaque extrémité, l'une pour l'émission des données (L.DATA.REQUEST), l'autre pour la réception (L.DATA.INDICATION):

Adresse locale	Adresse distante	Données	Niveau de priorité	(facultatif)
----------------	------------------	---------	--------------------	--------------

Dans le cas des réseaux locaux, on a tendance à d'utiliser le type 02 ou le type 03.

Fonctionnement type 02 (LLC 2)

Dans ce type de service, la sous-couche LLC émettrice a une liaison logique avec la sous couche réceptrice, et elle est chargée de la gestion de cette liaison. Le nombre de commandes croit en conséquence, on ne trouve plus uniquement L.DATA. L'ensemble de ces commandes de contrôle est résumés dans le tableau suivant.

Primitive	Suffixe	Fonction
L.Connect	Request	Demande de connexion
	Indication	Indication d'une demande de connexion
	Confirm	Acquittement d'une demande de connexion
L.Data.Connect	Request	Emission d'un paquet
	Indication	Indication de réception d'un paquet
	Confirm	Acquittement de réception d'un paquet
L.Reset	Request	Demande de réinitialisation de connexion
	Indication	Indication de réinitialisation
	Confirm	Acquittement de réinitialisation
L.Disconnect	Request	Demande de fin de connexion
	Indication	Indication de fin de connexion
	Confirm	Acquittement de fin de connexion
L. Connect	Request	Demande de définition du format du LSAP
	Indication	Indication de définition du format du LSAP
	Request	Demande de connexion

Tableau 3.5 : primitive du service LLC2.

Fonctionnement type 03 (LLC 3)

Ce type de service est sans connexion mais avec acquittement, il a été conçu à l'origine pour des applications temps réel, il vise à fiabiliser les échanges sans coûts de gestion difficiles.

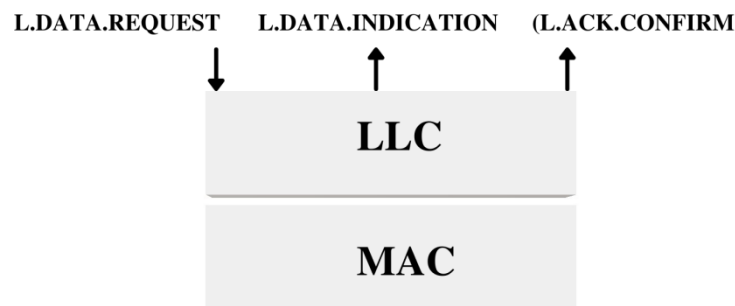


Figure 3.23 : Service de type 03 (LLC 3).

Le service utilise trois primitives : l'émission des données (L.DATA.REQUEST), la réception (L.DATA.INDICATION) et la confirmation de réception (L.ACK.CONFIRM).

3.2.3 Couche Application

La couche d'application comme nous avons dit au chapitre 02, elle représente l'utilisateur, et aussi l'interface graphique, pilotes systèmes (driver), serveurs de données (OPC), la façon dont le logiciel présente ses données qui se caractérisent en général par une incompatibilité des systèmes. Dans les RLI, la couche application crée un lien direct avec la couche de liaison de données.

3.2.3.1 Exemple de la couche Application

3.2.3.1.1 Standard de communication Client-Serveur OPC (Open Platform Communications)

En informatique industrielle, il arrive souvent que l'on souhaite établir une communication entre un PC et un API souvent pour concevoir des systèmes de supervision sur PC. Il existe plusieurs moyens permettant d'établir une communication entre un PC et un API. Par exemple si notre API dispose d'un port RS-485, nous pouvons facilement réaliser une communication PC/API à travers le protocole Modbus. Cependant, dans certains cas, si notre API n'a pas d'interfaces de communications dédiées ou si on nous avons plusieurs marques d'automates au sein de notre installation, l'utilisation d'un serveur OPC reste la meilleure solution.

OPC, anciennement OLE for Process Control, est une technique apparue en 1995 et destinée à l'interopérabilité des systèmes industriels. Il ne s'agit pas d'un protocole de communication mais d'une technique basée sur les techniques OLE (*Object Linking and Embedding*), COM (*Component Object Model*), et DCOM (*Distributed Component Object Model*) développées par Microsoft pour sa famille de systèmes d'exploitation Windows. Depuis 2011, et en raison de son expansion au-delà du contrôle de processus, OPC a été renommé en *Open Platform Communication*.

OPC a été conçu afin de relier les applications Windows et les matériels et logiciels du contrôle de processus. La norme définit une méthode cohérente pour accéder aux données de terrain de dispositifs d'usine. Cette méthode reste la même quels que soient le type et la source de données.

Le serveur OPC permet à différents logiciels d'accéder aux données de l'équipement de contrôle de processus, comme un API. Traditionnellement, chaque fois qu'un programme a besoin d'accéder aux données d'un périphérique, une interface personnalisée, un pilote, devait être écrit. Le but d'OPC est de définir une interface commune, de l'écrire une seule fois, puis de la réutiliser par n'importe quel logiciel d'entreprise, SCADA, IHM, etc. Une fois qu'un serveur OPC est écrit pour un équipement particulier, il peut être réutilisé par n'importe quelle application qui est capable d'agir en tant que client OPC. Un serveur OPC utilise la technique Microsoft COM pour communiquer avec les clients.

La Fondation OPC a développé les spécifications OPC UA pour répondre à ces besoins tout en fournissant une architecture ouverte à plate-forme technologique riche en fonctionnalités, évolutive et extensible.

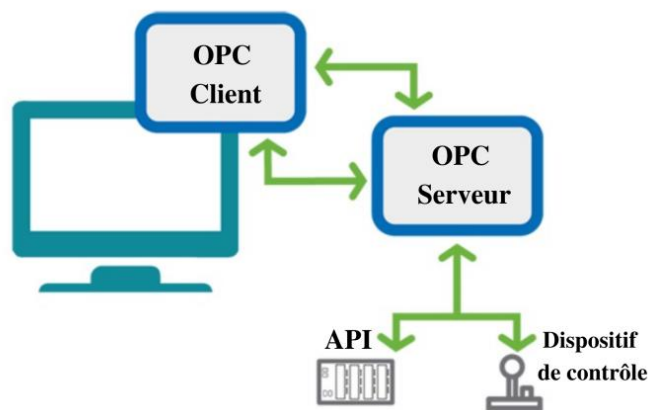


Figure 3.24 : Schéma global d'OPC.

3.3 Étude du modèle TCP/IP

3.3.1 Ethernet

Ethernet est un réseau de type LAN (*Local Area Network*) ou réseau local. Un réseau local peut être défini comme l'ensemble des ressources permettant l'échange de données en les équipements au sein d'entreprise, d'une société ou de tout autre établissement. Ethernet est uniquement un support de transmission de données et supporte plusieurs protocoles réseau : TCP, Apple Talk, DECnet, ...etc.

3.3.2 Modèle TCP/IP

TCP/IP fait généralement référence à l'architecture réseau, mais cet acronyme fait en réalité référence à deux protocoles étroitement liés : le protocole de transmission TCP (Transmission Control Protocol), qui est utilisé en plus du protocole réseau IP (Internet Protocol). Le sens du "modèle TCP/IP" est en fait une architecture de réseau à 4 couches (Application, protocole de transport TCP ou UDP, protocole de réseau IP et protocole physique Ethernet), dans laquelle les protocoles TCP et IP jouent un rôle très important car ils sont la mise en œuvre la plus courante. En abusant du langage, TCP/IP peut donc spécifier deux choses : Le modèle TCP/IP est le résultat des deux protocoles TCP et IP.

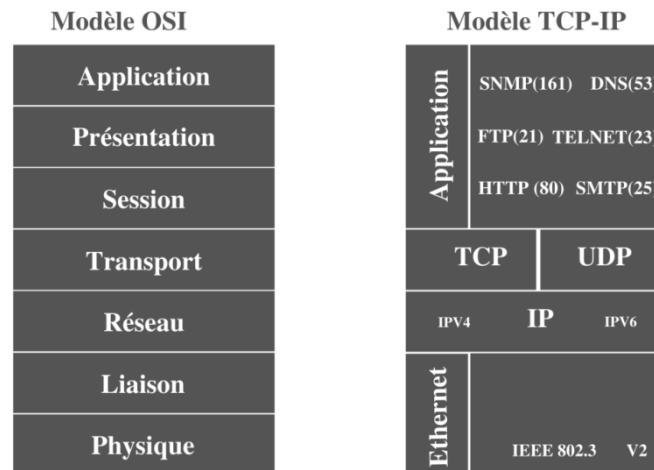


Figure 3.25 : Architecture générale du modèle TCP/IP.

Ethernet TCP/IP fournit des vitesses de communication jusqu'à 1 Gbits/s. Il permet une installation à faible coût et ses systèmes sont flexibles, car il peut être considéré soit comme un protocole de réseau local, soit comme un protocole industriel. En utilisant Ethernet TCP/IP, il est possible d'accéder à distance à un réseau, en privilégiant le partage de données et l'accès aux différents appareils qui composent le réseau. C'est également possible dans les réseaux industriels, puisque les automates programmables industriels ont intégré cette technologie. Étant un protocole basé sur le modèle OSI. Pour les communications de 100 Mbits/s à 1 Gbits/s, ils utilisent pour la transmission physique des données, le câble coaxial fin, la paire torsadée ou la fibre optique. Pour les communications de 10 Mbits/s, ils utilisent le câble coaxial épais. Le mode de transmission de données peut être établi en mode Simplex, Half-Duplex ou Full-Duplex. La technique d'accès au médium est effectuée par CSMA/CD. Néanmoins, dans les grands réseaux, les collisions sont fréquentes. Les réseaux Ethernet permettent généralement de transmettre deux types de trames au format légèrement différent : les trames Ethernet V2 et les trames 802.3.

Le protocole TCP/IP est une architecture non-propriétaire permettant l'interconnexion de systèmes d'exploitation différents par le réseau. C'est donc une architecture du modèle « Client-serveur ».

3.3.3 Trame Ethernet V2

Chaque trame Ethernet V2 est constituée par les champs suivants :

Préambule	Adresse destination	Adresse source	Ether Type	Données	CRC
8 octets	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

Tableau 3.6 : Format de la trame Ethernet V2.

3.3.3.1 Préambule

Il est constitué de 8 octets, il annonce le début de la trame et permet la synchronisation.

3.3.3.2 Adresse de destination

C'est l'adresse physique de la carte Ethernet destinataire de la trame, elle est constituée de 6 octets. La représentation d'une adresse Ethernet comme ses 6 octets en hexadécimal séparés par des ':'.

Exemple

06:07:00:3c:01:a0. La destination peut être une adresse de multi-diffusion. En particulier, l'adresse ff:ff:ff:ff:ff:ff (diffusion ou broadcast) correspond à toutes les stations du réseau physique Ethernet.

3.3.3.3 Adresse Source

C'est l'adresse physique de la carte Ethernet émettrice de la trame, elle composée de (6 octets).

3.3.3.4 EtherType

Indique quel protocole est concerné par le message, elle est composée de 2 octets.

3.3.3.5 Champ de données

Elle est constituée de 46 à 1500 octets des données véhiculées par la trame. Sur une station destinataire de la trame, ces octets seront communiqués à l'entité (protocole) indiquée par le champ EtherType. Notons que la taille minimale des données est 46 octets. Des octets à 0, sont utilisés pour compléter des données dont la taille est inférieure à 46 octets.

3.3.3.6 Champ CRC

Champ de contrôle de la redondance cyclique. Il permet de garantir que la trame a été correctement transmise et que les données peuvent donc être délivrées au protocole destinataire. Le polynôme générateur de ce CRC est :

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \dots \dots \dots (3.4)$$

3.3.4 Trame Ethernet 802.3

Un seul changement par rapport à la trame Ethernet V2, le champ EtherType qui est remplacé par un champ Longueur qui indique la longueur de la trame. Dans ce cas, les données de la trame contiennent un PDU de la sous-couche LLC (de types 1, 2 ou 3).

3.3.5 Principe du modèle Client-Serveur en réseau

Le terme « Serveur » fait référence à toute application informatique qui reçoit une demande de service à travers le réseau sous forme de requête provenant d'une application dite « Client », traite cette demande et renvoie le résultat à l'application « Client ».

Le modèle « Client-Serveur » en réseau se présente comme une relation entre des applications informatiques qui peuvent s'exécuter sur des machines séparées, connectées par un réseau, relation dans laquelle l'application « Serveur » est fournisseur de services et

l'application « Client » consommatrice de services. De ce fait le terme « Serveur » s'applique à tout programme qui offre un service pouvant être utilisé à travers un réseau.

Un programme devient un « Client » lorsqu'il émet une requête vers un serveur et qu'il attend une réponse. Si un nœud est plus particulièrement chargé d'exécuter des programmes serveurs, alors le terme « Serveur » peut s'appliquer au nœud physique comme aux programmes.

3.3.6 Les protocoles réseaux Ethernet (TCP/UDP/IP)

3.3.6.1 Rôle et fonction de TCP (*Transmission Control Protocol*)

Le protocole TCP est un protocole de la couche **transport**. TCP est un protocole de communication orienté "connexion" avec vérification des erreurs. Lorsqu'un « nœud A » envoie des données vers un « nœud B », le « nœud B » est prévenue de l'arrivée des données, et témoigne de la bonne réception de ces données par un accusé de réception. Ici, intervient le contrôle CRC des données. Celui-ci repose sur une équation mathématique, permettant de vérifier l'intégrité des données transmises. Ainsi, si les données reçues sont corrompues, le protocole TCP permet aux destinataires de demander à l'émetteur de retransmettre les données corrompues. Voilà la description des étapes du modèle TCP :

- À l'émission, TCP segmente les messages en paquets ou datagrammes. Ces datagrammes sont alors routés individuellement dans le réseau par le protocole IP, le cas échéant, ils peuvent suivre des chemins différents et arriver ainsi en ordre dispersé.
- À la réception, le protocole TCP replace les datagrammes dans l'ordre correct et les assemble pour restituer le message initial ;
- En cas d'erreur de transmission ou de pertes de datagrammes, TCP prend les mesures correctives nécessaires qui consistent, en général, à demander la réémission des datagrammes en défaut ;
- La technique de segmentation a pour but d'éviter que des messages de grande taille (fichier, plans, etc.) ne puissent accaparer le réseau trop longtemps au détriment d'autres messages ;
- Les numéros de porte identifiant les programmes applicatifs qui utilisent, à un moment donné, l'accès au réseau. Il peut y en avoir plusieurs simultanément et les numéros de porte permettent de les distinguer.

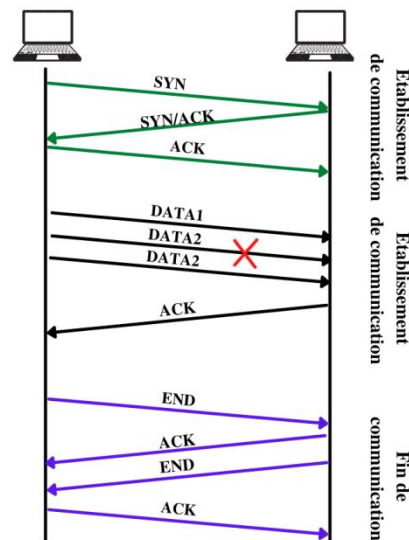


Figure 3.26 : Schéma d'une connexion TCP normale entre deux clients.

3.3.6.1.1 Format du TCP

Un segment TCP est constitué de deux parties : un en-tête et une partie de données. Les principaux champs de l'en-tête TCP sont :

- Le numéro de port source ;
- Le numéro de port destination ;
- Le numéro de séquence qui permet de rétablir l'ordre des paquets reçus et d'écarter les paquets dupliqués ;
- Le numéro d'acquittement qui est attendu par l'émetteur et représente en fait le nombre d'octets qui ont été déjà transmis ;
- La taille de la fenêtre qui indique le nombre d'octets qui seront acceptés par la machine qui envoie le paquet.

3.3.6.2 Rôle et fonction UDP (User Datagram Protocol)

Le protocole UDP est un protocole de la couche **transport**. UDP est un protocole de communication orienté "non connexion". Pour termes simple, lorsqu'un « nœud A » envoie un paquet au « nœud B », le flux est unidirectionnel. En effet, la transmission des données se fait sans notifier le récepteur « nœud B », et le récepteur reçoit les données sans confirmation de réception vers l'émetteur « nœud A ». Ceci est dû au fait que l'encapsulation des données envoyées par le protocole UDP ne permet pas de transmettre les informations concernant l'émetteur. En conséquence, le destinataire ne connaît pas l'émetteur des données hormis son IP, donc :

- UDP prend en charge la détection d'erreurs via le calcul de CRC, mais lorsqu'une erreur détectée, le paquet de données sera rejeté ;
- UDP permet d'envoyer des données sans remise de messages garantie. Ainsi les données sont envoyées sans que l'on sache si le récepteur l'a bien reçu ;

- UDP est plus rapide que TCP, puisque le protocole ne nécessite pas d'aller-retour pour vérifier la bonne livraison des paquets de données ;
- UDP est généralement utilisé pour les applications sensibles au temps de réponse tels que les jeux ou la transmission vocale.

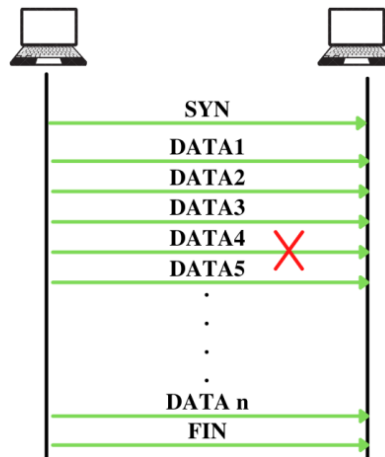


Figure 3.27 : Schéma d'une connexion UDP normale entre deux clients.

3.3.6.2.1 Pourquoi le protocole TCP ?

Le protocole TCP :

- Est plus fiable que UDP, les connexions par TCP sont donc généralement plus fiables car le protocole garantit que les paquets de données arrivent correctement; TCP est plus courant que UDP, il peut donc fonctionner dans la plupart des cas ;
- Est lourd, cela à cause de l'établissement de la connexion qui nécessite de multiples échanges et paquets de données à réaliser ;
- Est utilisé par les protocoles d'application qui nécessitent une remise de messages garantie. On l'utilise donc pour la communication de données pour les protocoles applicatifs tels que HTTP, FTP, SMTP, ...etc ;
- La taille des paquets est plus importante qu'en UDP.

3.3.6.3 Rôle et fonction d'IP (*Internet Protocole*)

Le protocole IP est un protocole de niveau **réseau** sans connexion et dont la sécurisation est assez faible. Comme expliqué ci-dessus, c'est TCP qui a pour rôle de fiabiliser la communication. En fait, IP a pour mission principal de trouver un chemin dans le réseau pour les datagrammes qui lui sont transmis par TCP. Avec l'expansion foudroyante d'Internet, le protocole IP original (actuellement dénommé IPv4) se trouve à bout de souffle, notamment au niveau de la capacité d'adressage. C'est pourquoi une nouvelle génération du protocole IP, IPv6, est en cours d'introduction.

Les hôtes sont connectés entre eux par un ou plusieurs réseaux. L'adresse IP de n'importe quel hôte est le rassemblement de :

- Une adresse du réseau où il se trouve ;
- Une adresse personnelle sur ce réseau.

3.3.6.3.1 Formats d'adressage en IPv4

L'adressage IPv4 s'effectue sur 32 bits soit 4 octets. Pour la facilité, on décrit généralement une adresse IP en considérant l'équivalent décimal des octets successifs séparés par des points.

Exemple

10000000 00000011 00000011 00000001 \equiv 128.3.3.1

Classe d'adresse

La classe d'adresse est définie par les deux derniers bits de l'adresse IP. Ces bits de poids fort définissent l'adresse du réseau et les bits de poids faible définissent l'adresse d'un équipement dans le réseau.

Un réseau de la classe A réserve 7 bits pour le réseau et 24 bits pour le matériel. On peut dire plus le poids fort est petit, plus le nombre de machines connectables dans un même réseau est important.

Un réseau de classe B réserve 14 bits pour le réseau soit 16384 réseaux et 16 bits pour le matériel.

Un réseau de classe C réserve 21 bits pour le réseau et 8 bits pour le matériel.

Classe	Préfixe	Nombre de réseaux possibles	Nombre d'hôtes possible
A	0	126	$2^{24}-2 = 16777214$
B	10	16384	$2^{16}-2 = 65534$
C	110	2097152	$2^8-2 = 254$
D	1110	Multicast	Multicast
E	1111	Réservé	réservé

Tableau 3.7 : Classe d'adresse.

D : adresses de groupe : diffusion de messages à des groupes d'hôtes.

E : réservé pour des besoins futurs

Classe	Plage de numéros de réseau	Plage de numéros d'hôte
A	0-127	0.0.1 à 255.255.254
B	128.0 à 191.255	0.1 à 255.254
C	192.0.0 à 223.255.255	1 à 254

Tableau 3.8 : plages d'adresse.

Dans chaque réseau, deux adresses sont toujours réservées : la 1ère et la dernière.

- La 1ère est l'adresse du réseau ;
- La dernière est l'adresse de broadcast (diffusion).

Exemple

Un réseau de classe C, comme par exemple le réseau 192.168.1.0 cela donne :

- 192.168.1.0 : C'est le réseau complet
- 192.168.1.1 à 192.168.1.254 : c'est l'ensemble des machines
- 192.168.1.255 : c'est l'adresse de broadcast.

L'adresse de broadcast est particulière, car lorsqu'un ordinateur envoie un paquet à cette adresse, ce n'est pas un seul ordinateur qui va recevoir le paquet, mais l'ensemble des ordinateurs du réseau. C'est toujours la dernière adresse du réseau.

Exemple

Quels équipements peuvent communiquer entre eux, et lesquels ne peuvent pas.

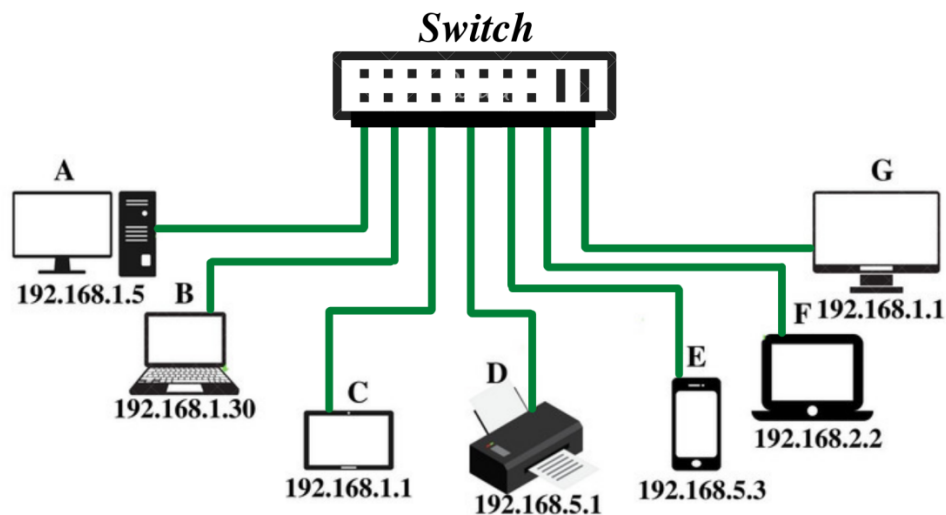


Figure 3.28 : schéma les équipements qui peuvent communiquer entre eux.

Réponse

Sur ce schéma : voici les équipements qui peuvent communiquer entre eux :

- A, B, C, et G (192.168.1) ;
- D et E (192.168.5) ;
- L'ordinateur F ne voit aucun autre équipement (personne ne voit le F) (192.168.2.2).

3.3.6.3.2 Masque de sous-réseaux

Le masque de sous-réseaux permet de définir le découplage entre les bits de l'adresse qui servent à définir l'adresse de réseau et ceux servant à définir l'adresse de machine.

Il est obtenu en mettant à 1 bit qui servent à définir l'adresse de réseau et à 0 les bits qui définissent les adresses des machines.

Classe	Masque de sous-réseaux
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Tableau 3.9 : Masque de sous-réseaux.

3.3.7 Principe de fonctionnement du TCP/IP sur Ethernet

3.3.7.1 Quel est le lien entre l'adresse IP et l'adresse Ethernet ?

Le modèle TCP/IP sur Ethernet montre que les données de l'application étaient encapsulées dans un segment TCP, qui lui-même était encapsulé dans un datagramme IP. Le datagramme IP est alors encapsulé dans une trame Ethernet dont l'en-tête comprend notamment l'adresse matérielle de la machine source et l'adresse matérielle de la machine destination.

L'adresse physique appelée adresse « MAC », doivent référencer un matériel unique qui peut être un serveur, un routeur, ou tout autre appareil doté d'une interface Ethernet. L'adresse MAC est une adresse fixe et unique, c'est le constructeur de l'interface réseau qui l'établit.

Il est nécessaire donc d'établir un lien entre l'adresse IP (qui peut être modifiée) et l'adresse MAC (qui est fixe). C'est le rôle du protocole ARP (*Adress Resolution Protocol*). Le protocole ARP permet d'associer une adresse logique à une adresse matérielle. Lorsqu'une station émettrice sur le réseau ne connaît pas l'adresse physique d'une machine dont elle connaît l'adresse logique, elle envoie une trame spéciale de requête d'identification à l'ensemble des dispositifs du réseau. La machine concernée lui répond ; la station prend connaissance de son adresse MAC (présence de l'adresse MAC source dans l'en-tête de la trame Ethernet) et met à jour sa table de correspondance.

3.3.7.2 Exercice : Application

3.3.7.2.1 Extrait BTS Informatique et Réseaux pour l'Industrie et les Services technique (IRIS)

La trame reproduit ci-dessous est extraite d'un relevé réalisé par un analyseur réseau. L'analyseur présente la description des différents protocoles utilisés :

Trame	Heure	Adr MAC src	Adr MAC dst	Protocole	Description
13	5.643554	000BDB14E06B	LOCAL	TC	

Frame ; Total frame length : 60 bytes

ETHERNET : Etype =0x0800 :Protocol =IP :DOD Internet Protocol

+ETHERNET : Destination adress : 00E018B96B0B

+ETHERNET : source adress : 000BDB14E06B

ETHERNET : Frame Length : 60 (0x003C)

ETHERNET : Ethernet type : 0x0800 (IP : DOD Internet Protocol)

ETHERNET : Ethernet Data : Number of data bytes remaining = 46x (0x002E)

IP : ID = 0x6C12 ; Proto =TCP ; Len : 43

IP : Version =4 (0 x 4)

IP : Header Length = 20 (0 x 14)

IP : Precedence = routine

IP : Type of Service = Normal Service

IP : Total Length =43 (0 x 2B)

IP : Identification = 27666 (0 x 6C12)

IP : Flags Summary = 2 (0 x 2)

IP :0 = Last fragment in datagram

IP :1. = Cannot fragment in datagram
 IP : Fragment Offset = 0 (0 x 0) bytes
 IP : Time to Live = 128 (0 x 80)
 IP : Protocole = TCP – Transmission Control
 IP : Checksum = 0xEB49
 IP : Source Adress = 192.168.17.22
 IP : Distination Adress = 192.168.17.10
 IP : Data Number of data bytes remaining = 23 (0 x 0017)
 IP : Padding : Number of data bytes remaining = 3 (0 x 003)
 TCP : AP...., len : 3, seq :2700201124-2700201127, ack : 2053738035, src : 2467 dst : 4425
 TCP : Source Port = 0 x 09A3
 TCP : destination Port = 0 x 1149
 TCP : Sequence Number = 2700201124 (0 x A0F1CCA4)
 TCP : Acknowledgement Number = 2053738035 (0 x 7A698E33)
 TCP : Data Offset = 20 (0 x 14)
 TCP : Flags = 0 x 18 : .AP
 TCP : ..0..... = No urgent data
 TCP : ...1.... = Acknowledgement field significant
 TCP :1... = Push
 TCP :0.. = No Reset
 TCP :0. = No Synchronize
 TCP :0 = No Fin
 TCP : checksum = 0 x 3D42
 TCP : Data : Number of data bytes remaining = 3 (0 x 0003)

1. Indiquez les adresses Ethernet et les adresses IP de la machine source et de la machine destination en précisant la classe d’adresse retenue.
2. Indiquez le numéro de port source et le numéro de port destination.

Solution

1. Les adresses des machines

	Adresse source	Adresse destination
Adresse IP	192.168.17.22	192.168.17.10
Adresse MAC	000BDB14E06B	00E018B96B0B

Classe d’adresse : classe « C »

2. Numéros de port source et de port destination

en :	Numéros de port source	Numéros de port destination
HEX	0 x 09A3	0 x 1149
DEC	2467	4425

3.3.8 Principaux services de la couche application

- **FTP** (*File Transfert Protocol*) : permet le transfert des fichiers d’une machine à une autre ;
- **Talent** : sert à connecter sur une machine à distance et de fonctionner en mode terminal à travers le réseau ;
- **SMTP** (*Simple Mail Transfert Protocol*) : protocole de messagerie électronique ;

- **DNS** (*Domaine Name Server*) : permet de convertir un nom de machine en adresse réseau et vice versa ;
- **SNMP** (*Simple Network management protocol*) : permet d'effectuer une gestion du réseau.

3.3.9 Conclusion

Dans ce chapitre, nous avons étudié le modèle OSI à trois couches et le modèle TCP-IP. Pour les RLI, les quatre couches : réseau, transport, session et présentation sont souvent absentes. Elles sont généralement utilisées pour les très gros réseaux ou pour des systèmes multi-réseaux à architecture maillée.

Pour le modèle OSI des RLI, nous avons étudié la couche physique, cette dernière gère les connexions matérielles. Elle peut transmettre des informations et convertir une séquence de bits (0 ou 1) en une séquence de grandeurs physiques adaptées au médium. Elle fournit aussi les caractéristiques mécaniques, fonctionnelles, ainsi que les signaux. Cette couche est matérialisée par le câble, les connecteurs de niveau «hardware» et les microcontrôleurs et pilotes «software».

Ensuite, la couche Liaison de données, est responsable du codage, de l'adressage, et de la transmission des données. Cette couche fournit les moyens fonctionnels et procéduraux indispensable à l'établissement, au maintien et à la libération des connexions entre entités de réseaux et est chargée d'acheminer sans erreur les données sur chaque liaison du réseau en masquant aux autres couches les différences physiques du réseau. Elle assemble les données en blocs et rajoute des informations de contrôle afin de constituer une trame de données : l'adresse de destination, la longueur du message, l'information de synchronisation, de détection de problèmes, etc.

La couche application, C'est elle qui contient l'application informatique, elle gère le transfert des informations entre programmes. L'objectif de cette couche est de fournir des services aux utilisateurs d'un réseau. Nous avons vu le serveur OPC comme exemple de la couche application, ce dernier, permet de créer un environnement pour accéder aux données d'usine en temps réel. Sur le plan technique, OPC utilise une architecture « client/serveur » mettant l'accent sur l'objet, ce qui facilite l'échange de données entre les différents logiciels. Les objets du serveur sont décrits à l'aide d'interfaces d'objets dont les fonctions sont accessibles au client.

Pour le modèle TCP/IP, on a vu :

- Comment décrire les différentes couches du protocole TCP/IP ;
- Les règles régissant les classes d'adresses IP et les masques de réseau.

La pile de protocole utilisé sur Internet est IP. Il est généralement appelé TCP/IP, d'après deux de ses protocoles les plus importants, cependant, il existe également d'autres protocoles.

Le modèle TCP/IP est basé sur un modèle à quatre couches pour la mise en réseau, il s'agit des couches (1 et 2 fusionné, 3, 4 et 7). Toutes les couches ne sont pas complètement définies par le modèle, de sorte que ces couches sont remplies par des normes et des protocoles

externes. Les couches ont des noms mais pas de numéros, et bien que parfois les gens parlent de la couche 2 ou de la couche 3, ce ne sont pas des termes TCP/IP. Des termes comme ceux-ci proviennent en fait du modèle de référence OSI. La pile TCP/IP est ouverte, ce qui signifie qu'il n'y a aucun secret sur son fonctionnement.

Chapitre 04 : Les réseaux de terrain

4.1 Introduction

Si l'on se réfère à la pyramide du CIM, les réseaux terrain se situent en fait aux niveaux cellule, terrain ou capteurs/actuateurs voir (figure 1.1). Le terme « réseau de terrain » regroupe tous les bus de communication utilisés dans le monde industriel, néanmoins, il existe trois bus de complexités différentes : le réseau d'usine (basé sur Ethernet), le réseau d'atelier : pour la connexion des équipements intelligents et le réseau de terrain ou capteurs/actionneurs pour relier les nœuds à intelligence limitée.

Le réseau de terrain est le plus proche de la production; il correspond aux différentes machines qui assurent la fabrication, la transformation, l'assemblage autour d'un objet. Dans le niveau de terrain, la taille des messages échangés est assez faible (bits 0 ou 1) comparativement aux autres niveaux. Les flux d'informations sont plutôt périodiques et l'aspect contraint de temps (temps réel) est prioritaire. Les réseaux de terrain fonctionnent au sein du milieu perturbé du point de vue électromagnétique, les médiums utilisés sont généralement des câbles coaxiaux blindés ou des paires torsadées travaillant en mode différentiel ou encore la fibre optique pour une plus grande immunité au bruit. Les distances de communications sont assez faibles par rapport aux autres types de réseaux, souvent à quelques dizaines de mètres.

Parmi les topologies les plus utilisées c'est la topologie bus, car elle est facile de mise en œuvre, d'évolution et d'extension. Les réseaux de terrain sont de plus en plus intégrés au monde industriel. En 2000, il y avait plus de 700 000 réseaux de terrain utilisés en Europe, de sorte que chaque fabricant essayait frénétiquement de rassembler autant d'utilisateurs que possible dans leurs solutions afin d'en faire un standard de fait.

Dans le présent chapitre, nous allons voir une vue d'ensemble des réseaux et protocoles de communication industriels développés pour surveiller et contrôler les processus industriels. Les protocoles qu'on va voir sont : WorldFIP, AS-I, CAN, Modbus et Profibus.

4.2 Les réseaux de terrain et la boucle 4-20 mA

Les anciens systèmes de communication industriels utilisaient la boucle de courant 4-20 mA voir (figure 4.1). Cette boucle est l'ancêtre du réseau de terrain apparu dans les années 60, elle permet de transmettre un signal analogique sur une grande distance sans perte ou modification de signal.

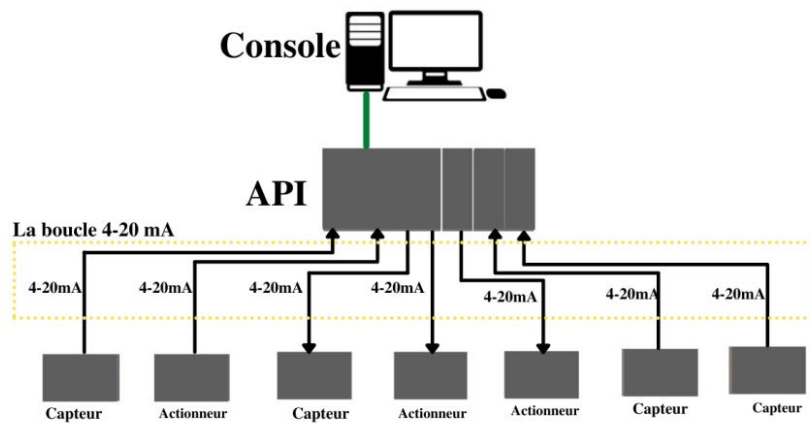


Figure 4.1 : Boucle de courant 4-20 mA.

Cependant, après l'apparition de la communication numérique, cette technique a été rapidement remplacée par les bus de terrain voir (figure 4.2). Par conséquent, l'objectif principal des bus de terrain était de remplacer les anciens systèmes centralisés en décentralisant le contrôle, le traitement des alarmes, le diagnostic aux différents équipements qui sont devenus de plus en plus intelligents.

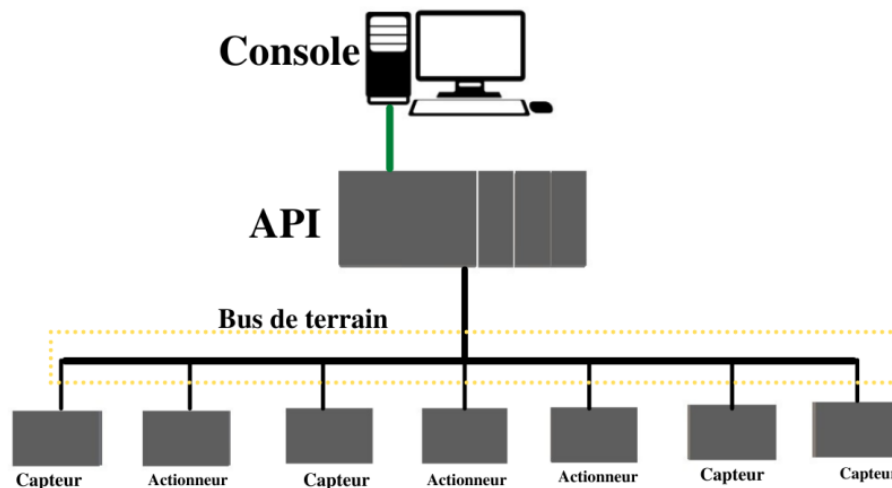


Figure 4.2 : Bus de terrain.

Parmi les avantages d'utilisation des réseaux de terrain, on peut citer quelques points :

- Réduction des coûts de câblage, généralement un seul câble lie tous les appareils ;
- Réduction des coûts de maintenance : diagnostics à distance, complexité moindre outils de test intégrés, flexibilité d'extension ;
- Réduction du temps d'installation ;
- Réduction du matériel nécessaire à l'installation ;
- Possibilité de réutiliser le câblage analogique existant dans certains cas ;

- facilité de conception des applications : les données sont disponibles en tout point du réseau.
- possibilité de communication entre deux équipements, sans notion de « superviseur ».
- Possibilité de connexion d'équipements de différents fournisseurs ;
- Existence de nombreuses « passerelles » ;
- Accès au bus : conflit, arbitrage, temps de latence... ;
- Sécurité des informations transportées : gestion des erreurs, redondance d'accès... ;
- Augmentation de l'efficacité (précision, formalisation des échanges entre les appareils) ;
- Echange de données par des mécanismes standards (protocoles).

4.3 Critères de comparaison

Afin de permettre une comparaison entre les réseaux, un ensemble de critères explicite ci-après. Le Comité Interprofessionnel pour l'Automatisation et la Mesure propose un ensemble de 46 critères. Ils sont répartis en deux sous-groupes : Techniques et Stratégiques.

4.3.1 Les critères techniques

4.3.1.1 Topologiques

- Longueur maximale du réseau en fonction du nombre de répéteurs et du type de médium utilisé ;
- Distance maximal entre deux nœuds du réseau ;
- Architecture physique et implantation des nœuds connectés au réseau, structure de câblage de toutes les stations.

4.3.1.2 Temporels

- Vitesse de transmission physique maximale possible pour le réseau ;
- Temps écoulé entre le début d'une demande de requête d'émission par un nœud et la transmission de toutes les données ;
- Délai maximal possible qui peut survenir lors de l'envoi d'informations. Ce temps dépend du temps de cycle, du nombre d'abonnés, de la longueur du réseau, du médium et de la vitesse physique de transmission ;
- Temps nécessaire à l'interrogation de tous les esclaves dans le cas de système maître esclave ;
- Possibilité de synchronisation.

4.3.1.3 Autres

- Nombre maximal d'équipements sur le réseau ;
- Hiérarchie entre les équipements (API maître ou esclave);
- Mode d'accès au réseau ;
- Mode d'adressage ;

- Priorité (droit d'émission);
- Longueur des informations ;
- Efficacité du protocole ;
- Sécurité de transmission de données ;
- Détection des erreurs de transmission (CRC);
- Réaction sur occurrence d'erreurs de transmission de données ;
- Réaction en cas de défaillance d'un nœud ;
-etc

4.3.2 Critères stratégiques

4.3.2.1 Standards

- Définition des couches du modèle OSI utilisées ;
- Certification : Entité responsable de la réalisation de tests et de la certification (tests des produits développés pour assurer la compatibilité).

4.3.2.2 Disponibilité de composants, de logiciels et de prestation de services

Disponibilité des composants existants tels que : composants électroniques, module connectables, cartes PC, passerelle vers autres bus, software,...etc.

4.4 Étude de cas

Nous allons faire une présentation rapide sur quelques réseaux de terrain.

4.4.1 Le bus World FIP (Factory Instrumentation Protocol)

Le World FIP est l'aboutissement d'un travail de développement franco-italien. Il a été conçu comme un réseau temps réel complètement numérique d'un interlocuteur à un autre. Il permet de lier tous les appareils d'une installation automatisée (les automates programmables, HMI, les capteurs, l'instrumentation, les actionneurs, les variateurs, ...etc). C'est un standard de fait qui respecte la norme OSI de l'ISO (couches 1, 2, 7). La principale caractéristique de "WorldFIP" est d'utiliser un protocole simple et unique pour répondre simultanément aux exigences de communication en temps réel et aux exigences de communication en arrière-plan du système de contrôle ou d'instrumentation.

4.4.1.1 Fonctionnement de bus World FIP

4.4.1.1.1 Termes utilisés

Information : la plus petite unité d'échange entre les stations, n'est pas produite que par un seul producteur et est référencé par un identifiant unique ;

Message : unité d'échange plus grande et plus explicite quelques variables ;

Station : élément du bus pouvant être, un ordinateur, un automate, un capteur ou un actionneur ;

Unité de traitement : automate programmable, ordinateur ou régulateur ;

Consommateur : station qui a besoin de lire une variable ;

Producteur : station qui fournit une variable aux autres stations ;

Les abonnés : les stations connectées au réseau peuvent être définies comme producteurs ou consommateurs d'informations ;

Identifiant : adresse globale d'une variable ;

Arbitre de bus : chef d'orchestre du bus, sans son accord les stations ne peuvent ni émettre des informations ni en recevoir.

4.4.1.2 Couche physique

- Utilise une paire torsadée blindée de 150 Ω avec une paire supplémentaire en cas de défaillance ;
- Nombre maximum de nœuds est au plus 32 par segment ;
- Nombre de répéteurs : 4 répéteurs au plus ;
- Codage utilisé : Manchester ;
- Débits normalisés : 31.25 Kb/s jusqu'à 10 km et 40 km avec 4 répéteurs; 1 Mb/s jusqu'à 1 km et 4 km avec 4 répéteurs, 2.5 Mb/s jusqu'à 700 m et 3.5 km avec 4 répéteurs, 25 Mb/s grâce à FIP HSF (High Speed FieldBus) ;
- Avec un débit de 1Mbits/s, longueur maximale d'un segment est de 750 m et le nombre maximum de réseau est de 256.
- La topologie utilisée : étoile, anneau ou bus.

4.4.1.3 Couche liaison

- Utilisation du modèle producteur / consommateur pour transmettre ;
- Le WorldFIP utilise le code CRC 16 bits ;
- L'accès au réseau s'effectue selon un cycle de fonctionnement décomposé en 3 phases: trafic périodique de Variables (capteur); trafic aperiodique de Variables (alarme); trafic périodique de messages (maintenance) ;
- L'accès au bus s'effectue de la manière suivante : un arbitre qui gère l'accès au bus ; le producteur de l'objet diffuse la réponse ; la trame est reçue par tous les nœuds et est exploitée seulement par les consommateurs de la variable.

4.4.1.4 Couche application

- Modèle client/serveur ;
- Messagerie MMS.

4.4.1.5 Méthode d'accès du réseau WorldFIP

Le réseau WorldFIP est basé sur une structure centralisée dans laquelle un nœud, dit arbitre de bus, accorde le droit de transmettre aux autres nœuds. En fonction des contraintes (essentiellement les périodes) de consommation des nœuds, nous construisons une table dite table d'arbitre de bus, qui permet d'indiquer l'ordre dans lequel les objets doivent être échangés sur le bus.

Identificateur	Période de transmission
25	100 ms
26	200 ms
27	500 ms
28	100 ms
29	200 ms

Tableau 4.1 : Exemple de table d'arbitre de bus WorldFIP.

Pour les transferts périodiques, la table d'arbitre de bus est construite hors ligne (c'est-à-dire de manière statique). La taille de cette table correspond au PPCM (Plus Petit Commun Multiple) des périodes de transmission. La plus petite période de transmission est appelée microcycle de l'arbitre de bus. Les transferts apériodiques (c'est-à-dire les transferts échangés de manière aléatoire) sont intégrés dynamiquement dans la table d'arbitre de bus pour être échangés quand il reste du temps libre dans un microcycle après échange des transferts périodiques (figure 4.4). Le macrocycle est répété indéfiniment jusqu'à l'arrêt de l'application. Le tableau 4.1 montre un exemple de table d'arbitre de bus pour cinq nœuds périodiques. Dans un réseau WorldFIP, à chaque nœud identifié, on associe un tampon, au niveau du nœud producteur, pour déposer la dernière valeur de transfert et un tampon, au niveau de nœud consommateur, pour stocker la dernière valeur véhiculée par le réseau. Le premier tampon est appelé tampon de production, et le second, tampon de consommation. Comme le montre la (figure 4.3), le processus d'échange de données s'effectue selon les étapes suivantes :

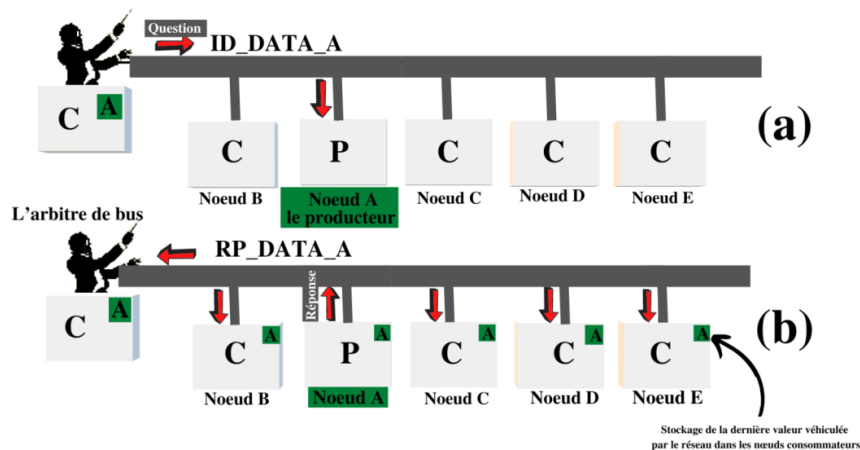


Figure 4.3 : Méthode d'accès du réseau WorldFIP.

- A l'aide de sa table, l'arbitre de bus diffuse une trame « appelée ID-Dat » qui contient un identifiant d'un nœud, ce sont les nœuds indiqués par la table de l'arbitre de bus comme des transmissions à échanger en même temps voir (figure 4.3a) ;
- En “lisant” l'identificateur diffusé, le producteur et le consommateur du nœud diffusé se reconnaissent ;
- Après un temps dit temps de retournement qui est fixé à quelques dizaines de μs pour un débit de 1 Mb/s. Le producteur diffuse une trame « dite RP-Dat » contenant la valeur du tampon de production associé au nœud dont l'identificateur a été diffusé par la dernière trame ID-Dat ;
- Les consommateurs de nœuds mettent à jour la valeur de leur tampon de réception à partir de la valeur contenue dans la trame RP-Dat voir (figure 4.3b) ;
- Après un intervalle de temps égal délai d'exécution, l'arbitre de bus passe à l'identificateur suivant dans la sa table, lorsque le dernier identificateur de la table a été diffusé, l'arbitre de bus recommence à partir du premier identificateur de la table.

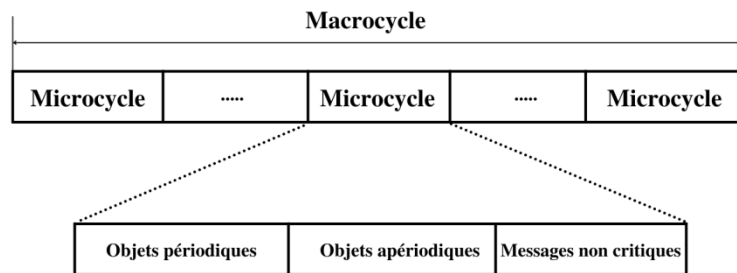


Figure 4.4 : Décomposition du temps de fonctionnement de l'arbitre de bus.

4.4.1.6 Conclusion

Le réseau WorldFIP est un réseau flexible dans lequel la transmission périodique de données d'entrées-sorties numériques et la communication d'informations non périodiques avancées sont possibles (par exemple : transmission de paramètres).

Même sur de longues distances, des taux de transmission élevés peuvent être atteints grâce à WorldFIP. La possibilité de trafic périodique fait de WorldFIP un réseau déterministe, assurant la cohérence temporelle des informations.

4.4.2 Le bus AS-I (Actuators Sensors Interface)

Le bus ASI repose sur la norme internationale CEI, c'est un système de câblage non propriétaire, les produits ASI sont certifiés par des laboratoires indépendants des constructeurs. C'est un bus de terrain qui respecte la norme OSI (1, 2, 7). En moyenne, il permet de réaliser jusqu'à 20 % d'économies globales par rapport au câblage traditionnel. Il résulte de l'association d'un groupe de 11 sociétés spécialisées dans les capteurs et les actionneurs (Baumer, Elesta, Festo, Ifm, Leuze, Pepperl & Fuchs, Sick, Siemens, Turck, Visolux).

4.4.2.1 Topologie de bus ASI

Topologie de type bus composé physiquement de deux fils non blindés supportant l'alimentation et la communication des capteurs et des actionneurs. Le protocole de communication repose sur un maître qui interroge les esclaves par scrutation cyclique (polling), dont la durée est en fonction du nombre d'esclaves consultés (5ms pour 31 esclaves). Le contenu de la trame, d'une longueur très courte de 14 bits, dépend de la requête du maître : données, paramètres, adressage, commandes. Son utilisation systèmes. Il existe de nombreuses passerelles vers Interbus, Profibus-DP, Profibus-FMS, Suconet, CAN, Modbus Plus, Device Net, etc. le tableau 4.2 indique les caractéristiques de bus de terrain AS-I.

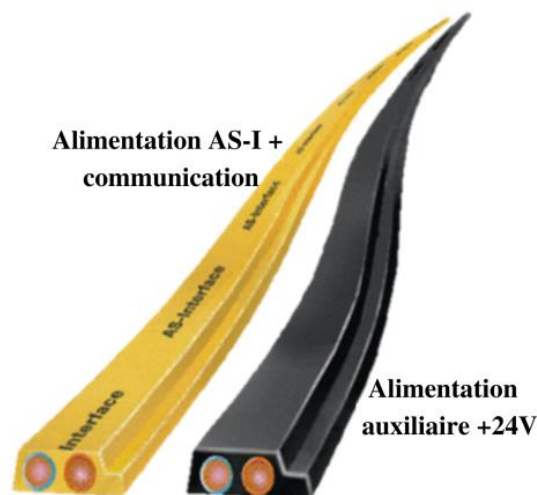


Figure 4.5 : le câble ASI **jaune** pour l'alimentation et la transmission des données, le câble **noir** ASI pour l'alimentation auxiliaire.

Longueur maximale	100 m sans répéteur 300 m avec répéteurs (2 répéteurs max entre le maître et l'esclave le plus éloigné)
Topologie	Libre
Débit	167kbit/s 1 transaction (data exchange) dure 150 micro-sec. Temps de cycle = 5 ms pour 31 esclaves 10 ms pour 62 esclaves
Détection d'erreurs	Codage NRZ Manchester Parité
Nombre max d'Equipment	ASi V1 : 1 maître + 31 esclaves ASi V2 : 1 maître + 62 esclaves A/B
Efficacité du protocole	38% max (8 bits sur 21). I4 du maître distingue entre données et paramètre.

Tableau 4.2 : Caractéristiques de bus de terrain AS-I.

4.4.2.2 Couche physique

Le médium de transmission est un câble blindé à deux fils (2 x 1,5 mm²) pour les données et 2A max d'énergie auxiliaire par gaine AS-I. La tension d'alimentation vaut 30 V DC. Le

signal de transmission de données est modulé. Il est possible de rajouter une alimentation 24V DC d'énergie auxiliaire.

Les deux câbles remplacent le câblage multifilaire. Les figures ci-après représentent l'alimentation du bus ASI.

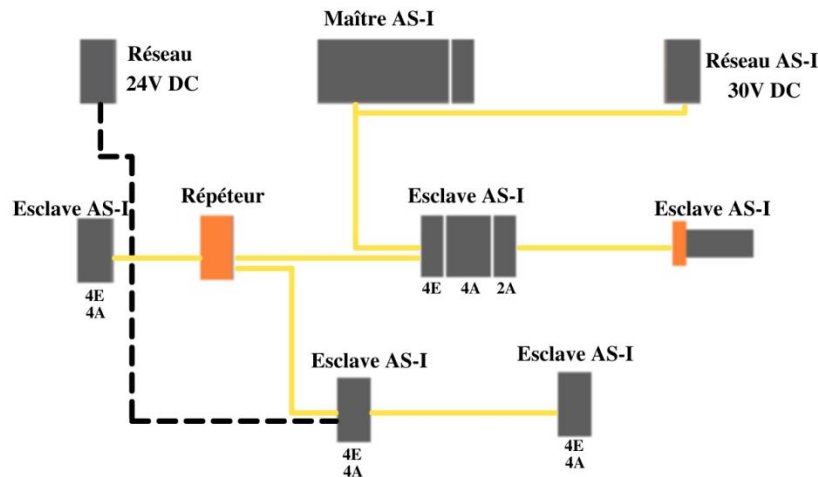


Figure 4.6 : configuration d'une interface AS

La longueur du câble est de 100 m au maximum, pour des distances plus importantes il faut rajouter des répéteurs (300m avec répéteur et 2 répéteurs max entre le maître et l'esclave) (figure 4.7). Ils existent différents types de câble : Le câble plat AS-i auto-cicatrisant est caractérisé par un détrempeage mécanique, ambiance normale et la mise en œuvre rapide. L'installation se fait simple au plus près des capteurs et des actionneurs. Le câble rond : (exemple: H05VV-F2x1.5) est caractérisé par une ambiance difficile (huile de coupe, étincelage...) et une homologation particulière. Le câblage peut suivre toutes les topologies de la machine :

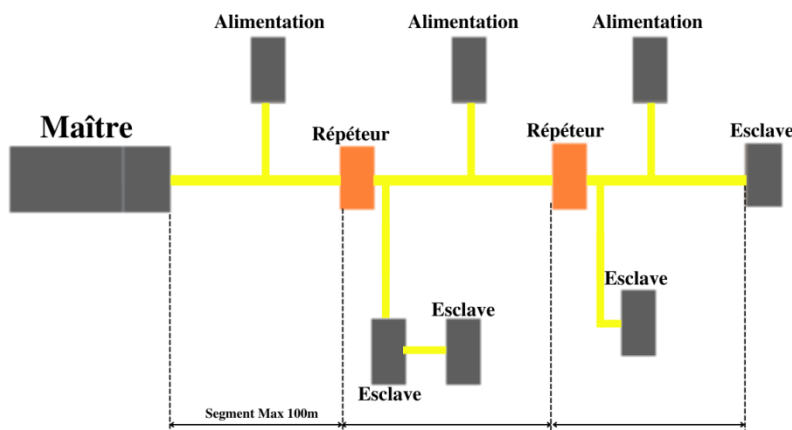


Figure 4.7 : Deux répéteurs max entre le Maître et l'esclave

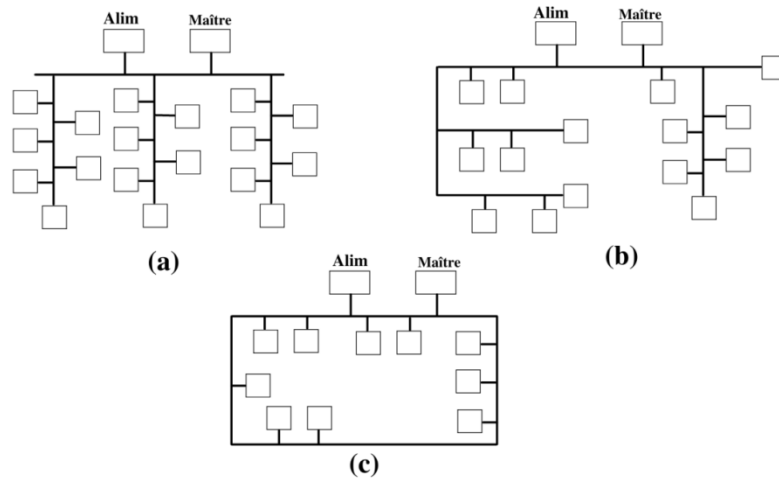


Figure 4.8 : (a) : Topologie étoile (b) : Topologie arbre (c) : Topologie anneau.

4.4.2.3 Composition de la trame

Le transfert des messages se fait à l'aide de deux types de trames spécifiques séparés d'un intervalle de temps :

Les trames de données : ces trames transmettent des données d'un producteur vers des consommateurs.

Les trames de requête : ces trames de polling sont envoyées du maître à l'esclave pour demander la transmission de trames de données. La figure suivante montre la requête de la station maître et la réponse de la station esclave.

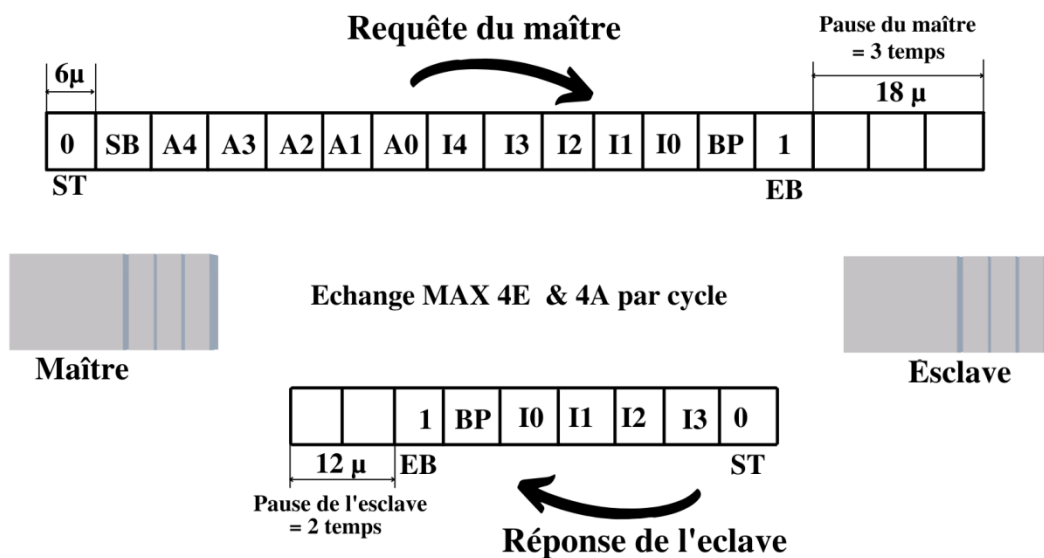


Figure 4.9 : La structure du message AS-I.

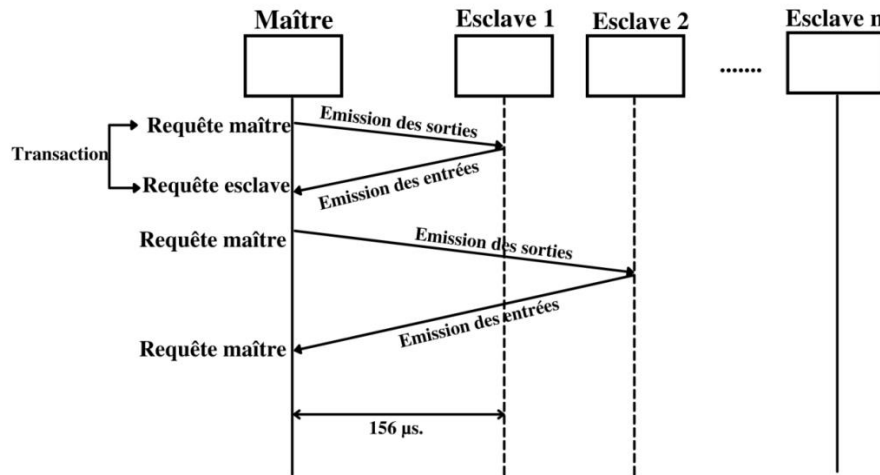


Figure 4.10: Transaction entre la station maître AS -i et les stations esclaves.

Dans celle-ci, les bits suivants sont indispensables pour la transmission des données :

- ST = Bit de démarrage ;
- SB = Bit de commande ;
- A4 ... A0 = Adresse des esclaves (5 bits) ;
- I4 I0 = Partie d'information du maître à l'esclave (5 bits) ;
- I3 I0 Partie d'information de l'esclave au maître (4 bits) ;
- PB = Bit de parité ;
- EB = Bit de fin.

Pour l'interface AS, l'appel de la station maître vers la station esclave répond comme suit :

4.4.2.4 Appel du maître :

- Le bit de démarrage indique le début de l'appel du maître (ST = 0) ;
- Le bit de commande SB identifie les appels de données (SB = 0), d'adresses (SB = 0), de paramètres (SB = 0) et de commandes (SB = 1) ;
- Les adresses des esclaves appelés se trouvent dans les 5 bits A4...A0 ;
- Transmission de la partie d'information depuis le maître vers l'esclave dans les 5 bits I4...I0 ;
- Le bit de parité PB vérifie que la somme de tous les « 1 » dans l'appel du maître est paire. Par conséquent, l'esclave peut reconnaître si la transmission est réussie ou non ;
- Le bit de fin indique la fin de l'appel du maître (EB = 1) ;
- La durée de pause du maître est 3 temps. Cette durée est une garantie de la sécurité de transmission.

4.4.2.5 Réponse de l'esclave :

- Le bit de démarrage ST indique le début de la réponse de l'esclave (ST = 0) ;
- La partie information de l'esclave au maître est transmise dans les 4 bits I3...I0 ;
- Le bit de parité PB garantit que la somme de tous les « 1 » dans l'appel de l'esclave est un nombre pair. Par conséquent, le maître peut reconnaître si la transmission de la réponse est réussie ou non ;
- Le bit de fin EB indique la fin de la réponse de l'esclave (EB = 1) ;
- La durée de pause de l'esclave est 2 temps. Cette durée est une garantie de la sécurité de transmission.

Il existe deux types de bus ASI notamment ASi V1 et ASi V2.

L'AS-i V1 peut contrôler jusqu'à 124E / 124S binaires soit 31 esclaves de 4 entrées et de 4 sorties. Le temps total de scrutation du maître est de 5 ms maximale.

L'AS-i V2 peut contrôler jusqu'à 248E / 186S binaires soit 62 esclaves de 4 entrées et de 4 sorties. Le débit est à 200Kbps et le temps total de scrutation du maître pour traiter les entrées et les sorties et de 10 ms. Chaque esclave est défini par un code d'identification (numéro d'esclave) et une configuration de n nombre d'entrées/sorties. Le codage de la trame se fait par parité, Manchester, NRZ.

4.4.2.6 Conclusion

Le protocole AS-Interface permet une bonne transmission des données d'entrées-sorties numériques et peut atteindre jusqu'à 300 m avec deux répéteurs Max. Les deux fils remplacent le câblage multifilaire. Il existe deux versions de bus ASI notamment ASi V1 et ASi V2. L'AS-i V1 peut contrôler jusqu'à 124E / 124S binaires soit 31 esclaves de 4 entrées et de 4 sorties. Le temps total de scrutation du maître est de 5 ms maximale. L'AS-i V2 peut contrôler jusqu'à 248E / 186S binaires soit 62 esclaves de 4 entrées et de 4 sorties. Le temps total de scrutation du maître est de 10 ms maximale.

4.4.3 Le bus CAN (Control Area Network)

C'est un standard de fait développé par Robert Bosch GmbH et Intel en 1985 pour l'industrie des automobiles. Il a été ensuite généralisé pour l'automatisme et les applications de contrôle. Le protocole CAN ne couvre seulement que trois des sept couches du modèle d'interconnexion des systèmes ouverts OSI de l'ISO (1, 2,7), très utilisé dans les automobiles, les équipements médicaux, avionique, automates industriels machines à outils, bâtiments, distribution automatique, ...etc.

4.4.3.1 Le protocole CAN

CAN (Control Area Network) est un protocole de communication série qui prend en charge les systèmes en temps réel avec une grande fiabilité. Ses domaines d'application vont des réseaux à moyen débit aux réseaux multiplexés à faible coût. Il est principalement classé dans la catégorie des réseaux de terrain utilisés dans l'industrie pour remplacer les boucles analogiques de 4-20 mA. La structure du protocole du bus CAN possède implicitement les principaux attributs suivants :

- Garantie des temps de latence ;
- Souplesse de configuration ;
- Réception de multiples sources avec synchronisation temporelle ;
- Fonctionnement multimètre ;
- Détections et signalisations d'erreurs ;
- Retransmission automatique des messages altérés dès que le bus est de nouveau au repos ;
- Déconnexion automatique des nœuds défectueux.

Nous présentons les trois couches du modèle OSI :

4.4.3.2 Couche physique

- Topologie Bus avec résistance de terminaison de ligne ;
- Une paire blindée (ou non) ;
- Conçu pour de courtes distances < 40 m (1000m à 50kbit/s, 40m à 1Mbit/s. Pas de répéteur) ;
- Codage NRZ ;
- Nombre de nœuds < 120 ;
- Débit brut 10 Kb/s à 1 Mb/s selon la longueur du réseau (voir le tableau ci-dessous).

Débit	Longueur	Longueur d'un bit
1Mbits/s	30 m	1 μ s
800 Kbits/s	50 m	1.5 μ s
500 Kbits/s	100 m	2 μ s
250 Kbits/s	250 m	4 μ s
125 Kbits/s	500m	8 μ s
62.5Kbits/s	1Km	16 μ s
20 Kbits/s	2.5 Km	50 μ s
10 Kbits/s	5 Km	100 μ s

Tableau 4.3 : Le débit en fonction de la distance et longueur d'un bit.

4.4.3.3 Support de transmission

La transmission des données est effectuée sur une paire filaire différentielle. La ligne est donc constituée de deux fils :

- CAN L (CAN LOW) ;
- CAN H (CAN HIGH).

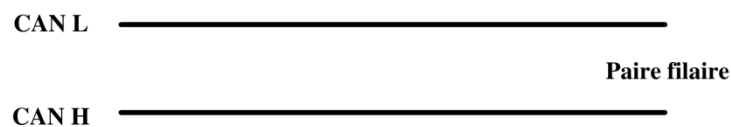


Figure 4.11 : paire filaire de bus CAN.

Le CAN est un bus de terrain, soumis à des parasites importants. Pour les niveaux physiques sur le bus, il est important de distinguer les deux types de transmissions possibles :

- transmission en bus CAN low speed,
- transmission en bus CAN high speed.

Le tableau ci-dessous résume les principales différences entre les deux types de bus notamment sur les débits supportés.

Paramètres	CAN <i>low speed</i>	CAN <i>high speed</i>
Débit	125 kb/s	125 kb/s à 1 Mb/s
Nombre de noeuds sur le bus	2 à 20	2 à 30
Courant de sortie (mode émission)	> 1 mA sur 2,2 k Ω	25 à 50 mA sur 60 Ω
Niveau dominant	CAN H = 4V CAN L = 1V	CAN H = 3,5 V CAN L = 1,5 V
Niveau récessif	CAN H = 1,75V	CAN H = 2,5 V

	CAN L = 3,25V	CAN L = 2,5 V
Caractéristique du câble	30 pF entre les câbles de ligne	2*120Ω
Tensions d'alimentation	5V	5V

Tableau 4.4: Les deux types de bus CAN.

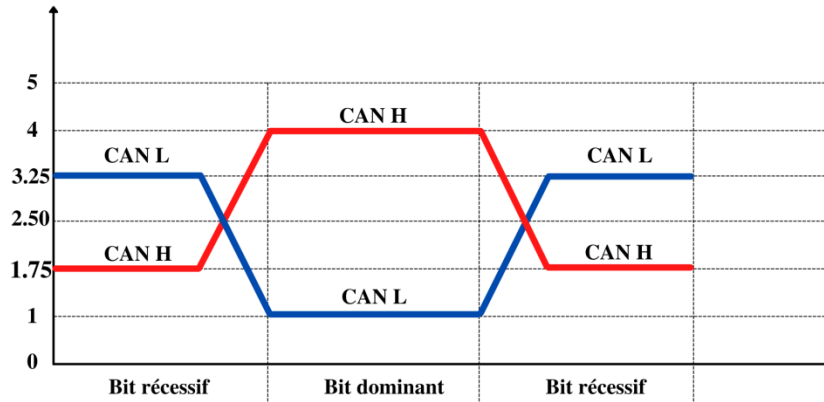


Figure 4.12 : Niveaux de tension du bus CAN *Low speed*.

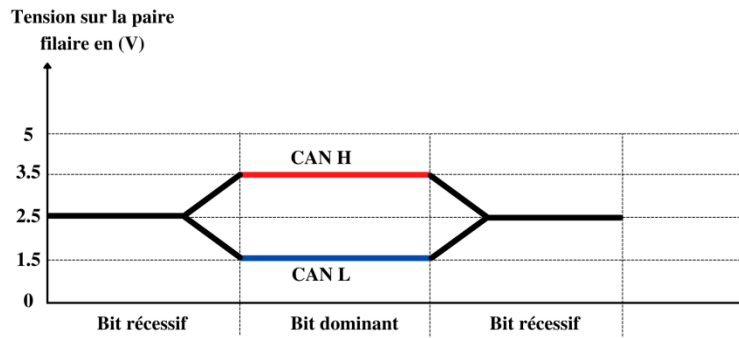


Figure 4.13 : Niveaux de tension du bus CAN *High speed*.

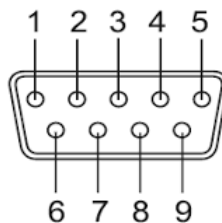


Figure 4.14 : le brochage sur le bus CAN est normalisé et utilise le connecteur D-B9.

Broche	description
1	Réservé
2	CAN L
3	Masse
4	Réservé
5	Blindage optionnel
6	Masse
7	CAN H
8	Réservé
9	Alimentation externe

Tableau 4.5 : description de différentes broches du connecteur D-B9.

4.4.3.4 Méthode de codage ‘ Bit Stuffing’

La méthode de codage NRZ a été retenue. Et pour sécuriser la transmission des messages on utilise la méthode dite de BitStuffing (bit de transparence). Cette méthode consiste, dès que l’on a envoyé 5 bits de même polarité sur le bus, à insérer un bit de polarité contraire pour casser des chaînes trop importantes de bits identiques. On obtient ainsi dans le message un plus grand nombre de transitions ce qui permet de favoriser la synchronisation lorsque le nœud est en réception. Cette technique est uniquement active sur les champs de SOF, d’arbitrage, de contrôle, de CRC (délimiteur exclu). Pour le bon fonctionnement de l’ensemble du réseau, cette technologie doit être mise en œuvre lors de la réception et de la transmission.

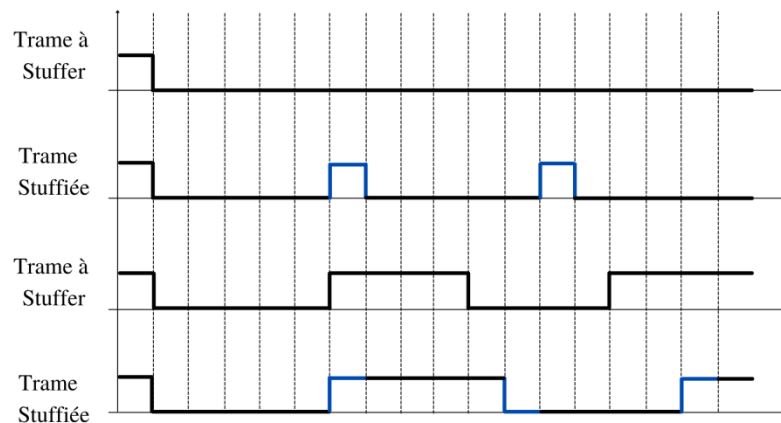


Figure 4.15 : Technique de Bit-Stuffing.

Exemple

Compléter le diagramme suivant (données du tableau) en respectant la méthode de BitStuffing

Données	1	1	0	0	0	0	0	0	1	1	0	1	1	1	1	1	0		
Bits émis	1	1	0	0	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0

4.4.3.5 Couche liaison

- Communication multimètres ;
- Accès au medium de type CSMA/CA ;

- Utilise trois types de trames ;
 - Data frame : pour les données ;
 - Remote frame pour demander l'émission des données ;
 - Error frame : pour signaler les erreurs.

La sous-couche MAC représente le cœur du protocole CAN. Sa fonction est de présenter les messages reçus de la sous-couche LLC et d'accepter les messages à transmettre à la sous-couche LLC. Elle est responsable des fonctions suivantes :

- La mise en trame du message ;
- L'arbitrage ;
- L'acquittement ;
- la détection des erreurs ;
- la signalisation des erreurs.

La couche inférieure de LLC est responsable de :

- du filtrage des messages ;
- de la notification de surcharge (overload) ;
- de la procédure de recouvrement des erreurs.

4.4.3.6 Couche application

Le standard CAN ne définit aucune application, c'est à l'utilisateur ou le concepteur de choisir ou développer l'application dont il a besoin. On trouve plusieurs applications basées sur CAN développées par le groupe CIA (CAN in Automation).

4.4.3.6.1 Définition

Nœud

Est un sous-ensemble relié à un réseau de communication et capable de communiquer sur le réseau selon un protocole de communication (ici le protocole CAN). Chaque nœud peut détecter des erreurs sur un message qui ne lui est pas destiné et en informer les autres nœuds.

Valeurs du bus

Le bus peut avoir l'une des deux valeurs logiques complémentaires définies, contrairement aux habituels 0 et 1, mais est appelé bit **dominant** ou **récessif**.

Message

Chaque information est émise sur le bus à l'aide d'un message (trame de bits) de format défini mais de longueur variable et limitée. Dès que le bus est libre, n'importe quel nœud relié au réseau peut émettre un nouveau message.

Routage des informations

Des nœuds peuvent être ajoutés au réseau sans qu'il n'y ait rien à modifier tant au niveau logiciel que matériel. Chaque message possède un identificateur qui n'indique pas la destination du message mais la signification des données du message. Par conséquent, tous les nœuds reçoivent le message, et grâce au système de filtrage des messages, chaque nœud peut savoir si ce dernier est pour lui ou non.

Trame de données et de requête

Une trame de données transporte, comme son nom l'indique, des données. Une trame de requête est envoyée par un nœud souhaitant recevoir une trame de données (dans ce cas, les identifiants des deux trames sont les mêmes).

Débit (bit/s)

Le débit peut varier entre différents systèmes, mais il doit être fixe et uniforme au sein d'un même système.

Priorités

En cas de demandes de prise du bus simultanées les identificateurs de chaque message permettent aussi de définir quel message est prioritaire sur tel autre.

Fonctionnement multi-maître

Lorsque le bus est libre, chaque nœud peut décider d'envoyer un message. Seul le message de plus haute priorité prend possession du bus.

Arbitrage

Le problème de l'arbitrage résulte du fonctionnement multi-maître. Si deux nœuds ou plus tentent d'émettre un message sur un bus libre il faut régler les conflits d'accès.

On effectue alors un arbitrage bit à bit non destructif tout au long du contenu de l'identificateur. Ce mécanisme garantit qu'il n'y aura ni perte de temps, ni perte d'informations. Dans le cas de deux identificateurs des trames de requête et de données identiques, la trame de données gagne le bus. Lorsqu'un bit récessif est envoyé et qu'un bit dominant est observé sur le bus, l'unité considérée perd l'arbitrage, doit se taire et ne plus envoyer aucun bit.

Canal de liaison simple

Le bus consiste en un simple canal bidirectionnel qui transporte les bits. À partir des données transportées, il est possible de récupérer des informations de resynchronisation.

Acquittement, validé

Tous les récepteurs vérifient la validité d'un message reçu, et dans le cas d'un message correct ils doivent acquitter en émettant un flag.

Sécurité de transmission

Dans le but d'obtenir la plus grande sécurité lors de transferts sur le bus, des dispositifs de signalisation, de détection d'erreurs, et d'autotests ont été implémentés sur chaque nœud d'un réseau CAN. On dispose ainsi d'un monitoring bus (vérification du bit émis sur le bus), d'un CRC (*Cyclic Redundancy Check*), d'une procédure de contrôle de l'architecture du message et d'une méthode de Bit-Stuffing.

Signalement des erreurs et temps de recouvrement des erreurs

Tous les messages entachés d'erreur(s) sont signalés au niveau de chaque nœud par un flag. Les messages erronés ne sont pas pris en compte, et sont retransmis automatiquement.

Erreurs de confinement

Un nœud CAN doit être capable de faire les distinctions entre des perturbations de courtes durées et des dysfonctionnements permanents. Les nœuds considérés comme défectueux doivent passer en mode switched off en se déconnectant (électriquement) du réseau.

Mode Sleep (sommeil) et Mode Wake-up (réveil)

Afin de réduire la consommation d'énergie, chaque élément CAN peut se mettre en Sleep mode. Dans ce mode il n'y a aucune activité interne au nœud CAN considéré et ses drivers sont déconnectés du bus. La reprise de fonctionnement (mode Wake-up) s'effectue lorsqu'il y a une activité sur le bus ou par décision interne à l'élément CAN.

Nominal Bit Time

Une période d'horloge correspond à ce que l'on appelle le Nominal Bit Time. Le Nominal Bit Time représente donc la durée d'un bit sur le bus. Le niveau de tension est maintenu constant pendant la durée d'un bit (NRZ). Chaque station reliée sur le bus doit être cadencée avec le même Nominal Bit Time pour pouvoir émettre et recevoir correctement les données circulant sur le bus.

4.4.3.7 Trames du bus CAN

Le bus CAN utilise quatre types de trame :

- Une trame de données : une trame au format standard (spécification CAN 2.0A) et une trame au format étendu (spécification CAN 2.0B).
- Une trame de requête.
- Une trame d'erreurs.
- Une trame de surcharge.

4.4.3.8 Format de la trame de données CAN

Une trame de données se décompose en 7 champs différents :

- 1) le début de trame SOF (*Start Of Frame*), 1 bit dominant.
- 2) le champ d'arbitrage, 12 bits pour CAN 2.0A et 32 bits pour CAN2.0B.
- 3) le champ de contrôle, 6 bits.
- 4) le champ de données, 0 à 64 bits.
- 5) le champ de CRC (*Cyclic Redundancy Code*), 16 bits.
- 6) le champ d'acquiescement (*Acknowledge*), 2 bits.
- 7) le champ de fin de trame EOF (*End Of Frame*), 7 bits récessifs.

Les formats des trames de messages CAN sont donnés par les tableaux suivants :

SOF	Champ d'arbitrage	Champ de contrôle	Champ de données	Champ CRC	Champ Acq.	Fin trame
1 bit	12 bits	6 bits	0-8 octets	2 octets	2 bits	7 bits

Tableau 4.6 : Spécification des messages au format standard (spécification CAN 2.0A).

SOF	Champ d'arbitrage	Champ de contrôle	Champ de données	Champ CRC	Champ Acq.	Fin trame
1 bit	32 bits	6 bits	0-8 octets	2 octets	2 bits	7 bits

Tableau 4.7: Spécification des messages au format étendu (spécification CAN 2.0B).

On distingue sept parties :

4.4.3.8.1 Début de trame

Start Of Frame (1bit dominant) pour la synchronisation des stations. Le début de trame n'est effectif que si le bus était précédemment au repos. Tous les nœuds du réseau doivent se resynchroniser sur le bit de SOF.

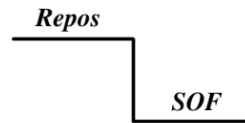


Figure 4.16 : Début de trame.

4.4.4.8.2 Champ d'arbitrage (12 bits)

Le champ d'arbitrage est composé de 11 bits de l'identificateur (figure ci-dessous) et d'un bit de RTR (Remote Transmission Request) qui est dominant pour une trame de données et récessif pour une trame de requête. Pour les identifiants, les bits sont transmis dans l'ordre, de ID₁₀ à ID₀ (le bit de poids faible est ID₀). De plus, les 7 bits de poids fort (de ID₁₀ à ID₄) ne peuvent pas tous être récessifs. Pour la compatibilité avec les circuits plus anciens, les 4 derniers bits de l'identifiant (ID₃ à ID₀) ne sont pas utilisés, ce qui réduit le nombre de combinaisons possibles par 9.

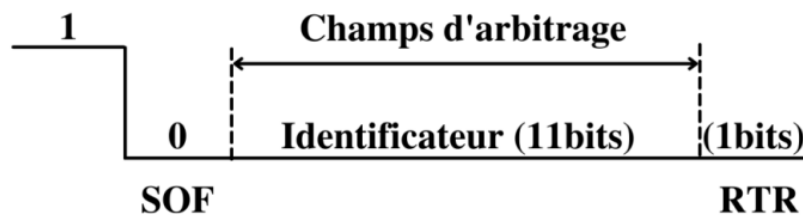


Figure 4.17 : Champ d'arbitrage (12 bits).

Exemple

Compléter le chronogramme (bus) et indiquer la station qui a réussi à émettre sa trame.

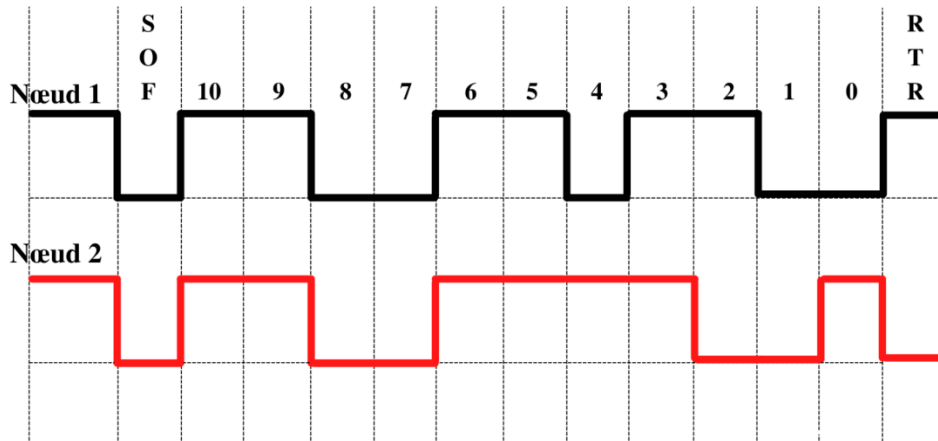


Figure 4.18 : chronogramme indiquant la station qui a réussi à émettre sa trame.

Réponse

Nœud 01	SOF	110 0110 1100	DLC	DATA	CRC	ACK	P
---------	-----	---------------	-----	------	-----	-----	---

Nœud 01 : 0X66C

En décimale : 1644

Nœud 02	SOF	110 0111 1001	DLC	DATA	CRC	ACK	P
---------	-----	---------------	-----	------	-----	-----	---

Nœud 02 : 0X679

En décimale : 1657

Le message le moins élevé qui a réussi à émettre sa trame. C'est le **Nœud 01**

4.4.3.8.3 Champ de contrôle

Le champ de contrôle est composé de 6 bits (figure ci-dessous). Les deux premiers (**R₀** dans une trame standard, et **R₁**). Le **R₁** est utilisé pour différencier le type entre le format standard (état dominant) et les formats étendus (état récessif). Le bit **R₀** est réservé pour l'utilisation au futur. Les quatre derniers bits sont utilisés pour déterminer le nombre d'octets de données contenus dans le champ de données de la trame de données ou le nombre d'octets de données requis par le nœud de réseau pendant la trame de requête. Le nombre d'octets de données ne peut pas dépasser la valeur 8.

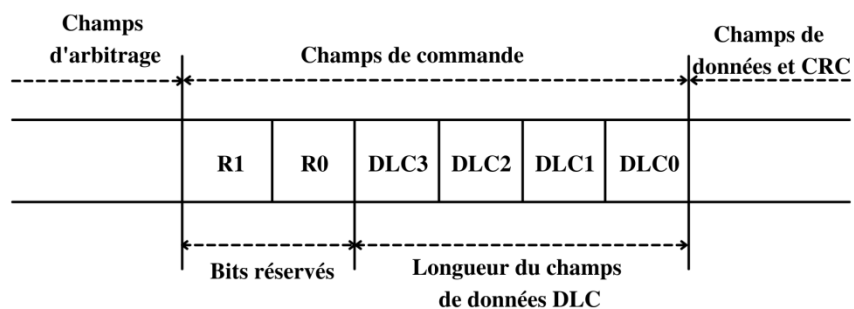


Figure 4.19 : Champ de contrôle.

4.4.3.8.4 Champ de données

La longueur du champ de données peut varier de 0 à 64 bits. Cette longueur est déterminée lors de l'analyse du champ de contrôle. Dans le cas d'une trame de requête, le champ de données est vide.

4.4.3.8.5 Champ de CRC

Le champ de CRC est composé de 16 bits. La séquence CRC calculée est contenue dans les 15 premiers bits tandis que le dernier bit est le délimiteur de fin de champ de CRC (bit toujours récessif). Ce champ de CRC assure la validité du message transmis, et tous les récepteurs doivent se conformer à ce processus de vérification. Seuls les champs de SOF, d'arbitrage, de contrôle et de données sont utilisés pour calculer de la séquence CRC. Les codes utilisés par les contrôleurs de bus CAN sont des codes linéaires. En réalité, pour une séquence CRC de 15 bits, la longueur maximale du début de trame ne doit pas dépasser 2^{15} bits.

4.4.3.8.6 Champ d'acquittement

Le champ d'acquittement a deux bits comme le montre la figure ci-dessous. La station émettrice de la trame laisse le bus libre pendant deux coups d'horloge (cela correspond à l'émission de deux bits récessifs) et elle passe en mode réception pendant le premier coup d'horloge.

Le premier bit correspond à l'acquittement par l'ensemble des nœuds qui ont reçu le message. Si le nœud ne détecte aucune erreur (après calcul du CRC), ce dernier émet un bit dominant sinon il émet une trame d'erreur. La station qui a envoyé le message d'origine doit alors être capable de réagir en fonction de l'émission d'un bit dominant ou non par les autres stations sur le premier bit du champ d'acquittement.

Le second bit est un bit délimiteur d'acquittement qui doit toujours être récessif.

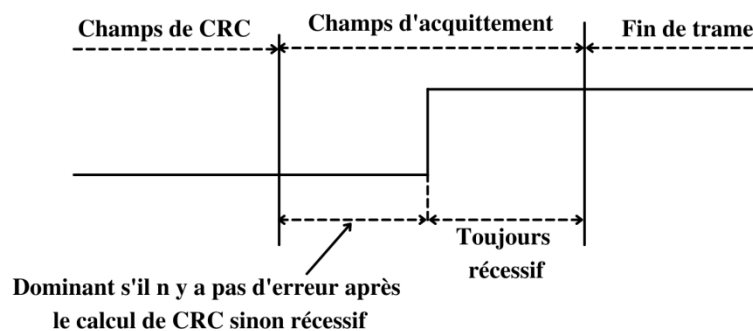


Figure 4.20 : Champ d'acquittement.

4.4.3.9 Les trames de requête

Ces trames de polling sont envoyées du maître à l'esclave pour demander la transmission de trames de données. La composition de la trame de requête est la même que celle de la trame de données sauf que le champ de données est vide et dans le champ d'arbitrage, le bit de RTR est récessif.

4.4.3.10 Les trames d'erreurs

Ces trames sont transmises lorsqu'une station détecte une erreur de transmission sur le bus.

4.4.3.11 Champ de fin de trame

Ce champ de fin de trame est constitué de 7 bits récessifs (1111111), il permet d'identifier la fin de la trame ce qui déroge à la règle de Bit-Stuffing. Étant donné que ce champ est fixe, l'encodage (lors de la transmission) et le décodage (lors de la réception) doivent être désactivés conformément à la règle du Bit-Stuffing.

4.4.3.12 Les trames de surcharge (*Overload*)

Ces trames sont envoyées pour demander un laps de temps supplémentaire entre des trames (de données ou de requête) successives. Il existe un espace inter trame de trois bits récessifs entre les trames de données et les trames de requête.

4.4.3.13 Conclusion

Le réseau CAN permet une bonne transmission des données d'entrées-sorties numériques. Il dispose d'un traitement d'erreur performant et d'un débit de transmission très élevé. Dans les installations en temps réel importantes, nous avons des contraintes relativement fortes lors de la conception pour assurer les caractéristiques temporelles. Le réseau CAN n'est pas adapté à la transmission de données de grandes distances un fort débit. Grâce à la gestion décentralisée d'accès au bus, CAN permet un temps de réaction très court.

4.4.4 Le bus Modbus

Modbus est un protocole de communication non-propritaire, créé en 1979 par Modicon (Modular Digital Controller) qui a été absorbé par Schneider Electric en 1996. Il est utilisé dans le réseau des automates programmables et appartient au niveau applicatif. c'est-à-dire du niveau 7 du modèle OSI. Ce protocole est basé sur une structure hiérarchique entre un seul client et plusieurs serveurs dans le domaine public, et ses spécifications sont publiques. Modbus est un protocole de dialogue permettant d'assurer la communication entre deux ou plusieurs stations, il permet aussi de communiquer des HMI dans un réseau local industriel du type maître-esclave. Dans le réseau Modbus standard, il existe une station maître et plus que 247 esclaves chacun à une unique adresse allant de 1 à 247. Seule la station maître peut écrire des informations aux esclaves.

Il se compose d'une trame contenant l'adresse de l'automate concerné, la fonction à traiter (écriture/lecture), des données et un code de contrôle d'erreur appelé contrôle de redondance cyclique 16 bits ou CRC16.

4.4.4.1 Caractéristique du réseau Modbus

- Topologie bus ;
- Nombre théorique d'abonnés 247. Peut-être plus faible suivant les constructeurs ainsi que par la limitation de la couche physique ;
- Transmission en semi-duplex, pas de médium particulier (paire torsadée, coaxial, fibre optique...) fixé en fonction des distances et des interfaces disponibles ;
- Transmission en bande de base de 50 à 19 200 bits/s ;
- Supporte les liaisons RS232, RS422, RS485 ;

- Méthode d'accès par protocole maître-esclaves.

Le protocole Modbus peut être implémenté :

- Sur une liaison série asynchrone de type RS-232, RS-422, RS-485 (Multi-point) ou TTY, avec des débits et sur des distances variables ;
- Sur TCP/IP (Ethernet), on parle alors du Modbus TCP/IP ;
- Sur Modbus plus. Le Modbus plus est un réseau à passage de jetons à 1 Mb/s pouvant transporter les trames Modbus et d'autres services propres à ce réseau.

4.4.4.2 Topologie

La topologie utilisée est maître-esclave. Le maître envoie une requête à l'esclave et attend sa réponse.

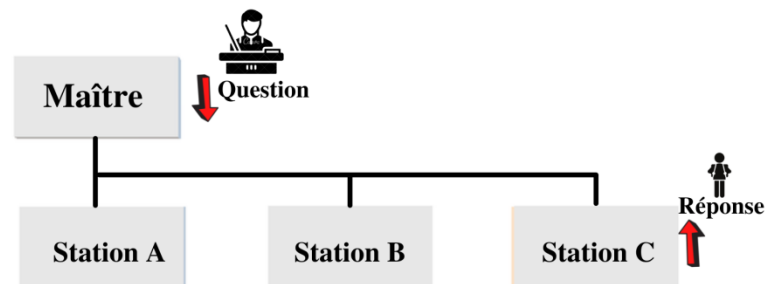


Figure 4.21: Topologie Maître/esclave Modbus.

Les règles de fonctionnement sont les suivantes :

- Les esclaves sont identifiés par une adresse (sur 8 bits soit un octet) ;
- Aucun esclave ne peut envoyer un message sans une demande préalable du maître ;
- Le dialogue entre les esclaves est impossible ;
- Le maître peut diffuser un message à tous les esclaves présents sur le réseau (diffusion générale ou broadcast). Pour cela, il utilise l'adresse 0.tv

4.4.4.3 Le réseau Modbus RS-485 ou RS-232

MODBUS RS-485 est un bus utilisant un media maître/esclave avec une vitesse de transmission allant de 1200 à 115 Kbits/s.

7	Application	Modbus
6	Présentation	Vide
5	Session	Vide
4	Transport	Vide
3	Réseau	Vide
2	Liaison	Maître/Esclave
1	Physique	RS-485 ou RS-232

Tableau 4.8 : Modèle OSI du réseau Modbus RS-485.

4.4.4.4 Le réseau Modbus TCP/IP avec Ethernet

MODBUS TCP/IP utilise TCP/IP et Ethernet pour transmettre des messages MODBUS à 10 Mbit/s ou 100 Mbit/s. Selon des recherches récentes, Modbus TCP/IP est le protocole Ethernet industriel le plus utilisé au monde.

7	Application	Modbus
6	Présentation	Vide
5	Session	Vide
4	Transport	TCP
3	Réseau	IP
2	Liaison	CSMA/CD
1	Physique	Ethernet V2 ou 802.3

Tableau 4.9 : Modèle OSI du réseau Modbus TCP/IP.

Le TCP/IP est une variante du protocole Modbus. Fondamentalement, Modbus TCP/IP est un protocole de communication qui permet à deux appareils ou plus de communiquer entre eux via un réseau Ethernet. Sur le réseau Modbus TCP/IP, un nœud peut être un automate programmable, HMI, un variateur de vitesse,...etc.

4.4.4.1 Principe de fonctionnement

Dans un réseau TCP/IP, on aura un client au lieu d'un maître, et au lieu d'un esclave, nous aurons un serveur. Le principe de fonctionnement est simple, le client (maître) demande des informations au serveur (l'esclave) via des trames de requête, et le serveur lui envoie à son tour des trames de réponse. Sur le réseau Modbus TCP/IP, divers appareils sont identifiés de manière unique par des adresses IP. L'adresse IP est une séquence de 4 chiffres pour IPV4, et 6 chiffres pour IPV6, ils sont séparés par un point. Un exemple d'adresse IPV4 : 192.168.6.1 Ces mêmes appareils peuvent être physiquement reliés via des câbles Ethernet équipés de prises RJ45.

4.4.4.5 Le réseau Modbus Plus

Modbus plus est un réseau de haut débit (1 Mbit/s) qui utilise la structure du message Modbus.

7	Application	Modbus
6	Présentation	Vide
5	Session	Vide
4	Transport	TCP
3	Réseau	IP
2	Liaison	802.4 token passing
1	Physique	RS-485

Tableau 4.10 : Modèle OSI du réseau Modbus plus.

Modbus Plus est dédié aux applications de terrain. Il propose un débit de 1Mbits/s, sur une topologie bus de longueur max. 450m (1800m avec répéteurs). Le mode d'accès au médium se fait par passage de jeton entre maximum 32 abonnés (64 avec répéteurs) ; l'échange de données d'une longueur maximale de 512 bits, s'effectue avec acquittement. Les données et l'identificateur de l'émetteur, échangés à travers la trame jeton, sont stockés dans une base de données globale propre à l'anneau et consultable uniquement par les abonnés de l'anneau.

Il est possible de connecter plusieurs réseaux Modbus Plus par l'intermédiaire de ponts (max. 4 ponts), établissant ainsi une topologie étoile ou arborescente au sein de laquelle chaque sous-réseau a son propre jeton circulant indépendamment des autres.

4.4.4.6 Les modes de transmissions

Deux modes de transmission, sont définis : Le mode RTU et le mode ASCII.

- Les modes de transmission doivent être identiques pour tous les participants à un même réseau ;
- Le mode ASCII est une option.

4.4.4.6.1 Transmission en mode ASCII

(American Standard Code for Information Interchange) les données sont codées (Il faut deux caractères pour représenter un octet, exemple 0X04 sera codé sur « 0 » et « 4 »).

Exemple

L'octet 0111 1011 soit en Hexa : x7B devient x37, x42 soit en binaire 0011 0111 0100 0010 (x37 est le code ASCII de 7, et x42 et le code ASCII de B)

Les octets envoyés sont donc tous compris dans [A à F et de 0 à 9], c'est-à-dire en hexa [x41-x46 et x30-x39] La longueur maximale d'une trame est de 525 octets. Chaque trame débute par un entête, l'octet x3A, code ASCII du caractère ":".

Chaque trame se termine par un délimiteur de fin, 2 octets x0D et x0A, code ASCII des caractères "CR/LF".

A chaque trame est associée une clé de contrôle LRC8 (cheksum de 1 octet : somme de tous les octets de données avant codage ASCII, cette somme est ensuite complémentée à 2, puis codée en ASCII).

3A	Adresse esclave	Code fonction	Données	CRC	0D 0A
1 car	2 car	2 car	≤525 octets	2 car	2 car

Tableau 4.11 : Format de la trame Modbus en mode ASCII.

Chaque caractère ASCII est transmis suivant l'un des deux formats :

- Start, 7 bits de données, 1 Bit de parité, 1 Bit de Stop ;
- Start, 7 bits de données, 2 Bits de Stop.

4.4.4.6.2 Transmission en mode RTU

Les trames RTU n'ont pas d'en-tête ni de délimiteur de fin. La station réceptrice vérifie le temps pour séparer deux caractères consécutifs. S'il est supérieur à trois caractères et demi, le caractère suivant est considéré comme le début de la trame. Le format de trame en mode RTU est le suivant :

Start	Adresse esclave	Code fonction	Données	CRC	End
≥3.5 char	1 octet	1 octet	0 à 252	2 octet	≥3.5 char

Tableau 4.12: Format de la trame Modbus en mode RTU

Le principal avantage du mode RTU est qu'il transmet plus rapidement les informations, par contre le mode ASCII permet d'avoir un intervalle de temps d'une seconde entre 2 caractères sans générer d'erreur de transmission.

La structure d'une trame Modbus est la même pour les requêtes (message du maître vers l'esclave) et les réponses (message de l'esclave vers le maître) sont présentés par les tableaux ci-après :

Start	Adresse esclave	Code fonction	Données	CRC	End
≥3.5 char	1 octet	1 octet	n octet	2 octet	≥3.5 char

Tableau 4.13 : Trame de requête.

Start	Adresse esclave	Code fonction	Données	CRC	End
≥3.5 char	1 octet	1 octet	n octet	2 octet	≥3.5 char

Tableau 4.14 : Trame de réponse.

Les octets (00 à FF), d'une trame RTU, est transmis selon le format recommandé suivant :

1 bit de Start	8 bits de données	1 bit de parité	1bit de stop
----------------	-------------------	-----------------	--------------

Les deux octets du CRC sont transmis poids faible en tête. Le CRC est calculé sur l'ensemble des champs d'adresses, fonction et données. Une clé de contrôle de deux octets est ajoutée à la fin de la trame. C'est un CRC16 dont le polynôme générateur est : $G(x) = x^{16} + x^{15} + 1$.

Le protocole Modbus offre 19 fonctions différentes et standardisées. Ca peut-être que des équipements ne supportent pas tous les codes fonctions.

Code Hex	Nature des fonctions Modbus
1	Lecture de n bits de sortie consécutifs
2	Lecture de n bits de sortie consécutifs
3	Lecture de n mots de sortie consécutifs
4	Lecture de n mots consécutifs d'entrée
5	Écriture de 1 bit de sortie
6	Écriture du statut d'exception
7	Lecture du statut d'exception
8	Accès aux compteurs de diagnostic
9	Téléchargement et mode de marche
A	Demande de CR de fonctionnement
B	Lecture du compteur d'événements
C	Lecture des événements de connexion
D	Téléchargement et mode de marche
E	Demande de CR de fonctionnement
F	Écriture de n bits de sortie
10	Écriture de n mots de sortie

11	Lecture d'identification
12	Téléchargement et mode de marche
13	Reset de l'esclave après erreur non recouverte

Tableau 4.15 : Code des fonctions Modbus.

4.4.4.7 Trame d'exception

Des trames d'exception sont prévues pour permettre la gestion du réseau et le traitement des erreurs (11 caractères en ASCII et 5 octets en RTU). Le format de la trame d'exception est la suivante :

Champs d'adresse	Champ code	Champ code d'erreur	CRC
1 octet	1 octet	1 octet	2 octet

Tableau 4.16 : Format de la trame d'exception.

Le code fonction retourné est celui de la commande avec le bit de poids le plus fort forcé à 1. Les codes d'erreurs sont donnés par le tableau suivant :

Erreur	Code
Fonction inconnue	1
Adresse incorrecte	2
Donnée incorrecte	3
Esclave non prêt	4
Acquittement	5
Défaut d'écriture	8

Tableau 4.17 : Codes d'erreurs.

4.4.4.8 Conclusion

Le protocole Modbus TCP est bien connu dans le milieu industriel. Ce protocole peut être considéré comme une évolution du Serial Modbus (RS485) qui circule désormais sur les réseaux TCP/IP. Le modèle client-serveur du Modbus TCP flexible et très facile à mettre en œuvre, il résout une vaste gamme d'applications. Cependant, avec l'avènement de concepts tels 3G/4G et appareils sans fil distribués géographiquement, de nouveaux besoins ont paru, ce qui rend difficile l'utilisation de Modbus TCP et son modèle client-serveur.

4.4.5 PROFIBUS (PROcess FIeld BUS)

**Figure 4.22** : Câble normalisé PROFIBUS RS-485.

PROFIBUS, un autre protocole largement utilisé, il a été développé en Allemagne (Bosch, Siemens,) et est populaire dans le monde entier. Le protocole PROFIBUS se caractérise d'être un système ouvert, qui peut être utilisé pour assembler des réseaux avec des capteurs, des actionneurs et des contrôleurs. Avec ce protocole, il est possible d'utiliser des équipements de

différents fabricants sans trop de problèmes de configuration. Sa transmission physique de données s'effectuant via le protocole RS-485, ce protocole présente des caractéristiques telles que la transmission asynchrone non-retour à zéro (NRZ), un débit en bauds de 9,6 Kbit/s à 12 Mbit/s (sélectionnés en fonction de la distance souhaitée (voir le tableau ci-après), qui peut varier entre 1200 et 100 m, respectivement), il utilise un câble à paire torsadée (RS-485) avec blindage, il permet le raccordement de 32 stations par segment (jusqu'à 127 stations). Il est également possible d'étendre l'étendue de ce réseau grâce à l'utilisation de répéteurs. Le protocole est synchrone et fonctionne dans les couches OSI 1, 2, 4 et 7. En utilisant RS-485. Une autre caractéristique importante de ce protocole, en raison de sa topologie en bus, est la simplicité de connexion ou de retrait d'équipement, n'interférant pas avec le fonctionnement des autres appareils, lorsque le réseau PROFIBUS est configuré, un débit de transmission commun est établi. Actuellement, le protocole PROFIBUS peut être trouvé dans trois configurations :

4.4.5.1 PROFIBUS-DP (*Decentralized Periphery*) : Il est fixé dans la norme DIN E 19245 Partie 3 et intégré dans la norme de bus à champs européennes EN 50170. Le profil DP est plutôt adapté à la communication entre équipements intelligents et équipements basiques tels que des capteurs et actionneurs, commandes analogiques ou binaires. On reconnaît facilement un réseau PROFIBUS-DP à la couleur de son câble : Violet. En l'ouvrant, il y a deux fils : un vert et un rouge, nommé "A" et "B". En général, les connecteurs PROFIBUS sont des connecteurs DB9 plus ou moins standards. Le fil "A" est relié au pin n°3 du connecteur DB9, tandis que le fil "B" est connecté au pin n°8. Il est possible d'exploiter le PROFIBUS-FMS et le PROFIBUS-DP simultanément sur un même.

4.4.5.2 PROFIBUS-FMS (*Fieldbus Message Specification*) : Il relie la couche réseau à la couche liaison. Il est conforme à la norme DIN 19245 et est intégré à la norme européenne de bus de terrain EN 50170. Le protocole de communication FMS est adapté à la communication entre des appareils dits intelligents tels que des ordinateurs ou des automates programmables.

4.4.5.3 PROFIBUS-PA (*Process Automation*) : Est conçu spécifiquement pour le domaine de la technique des procédés et permet la liaison des capteurs/actuateurs, même dans des domaines explosifs, à une ligne de bus à champ commune. Les appareils PROFIBUS PA peuvent être intégrés dans les réseaux PROFIBUS DP. En utilisant des couplages de segment de manière simple. La liaison d'un segment de bus PA à un PROFIBUS DP s'effectue à travers un coupleur de segment ou d'une liaison DP/PA.

Le PROFIBUS-FMS et le PROFIBUS-DP utilisent les mêmes techniques de transmission, ainsi la méthode d'accès aux bus homogène. C'est pourquoi ils peuvent être ouverts en même temps.

Ces trois variantes compatibles du PROFIBUS avec leurs propriétés votées et leurs domaines d'applications permettent une communication transparente depuis les capteurs/Actionneurs jusqu'aux systèmes de la couche de transport. Par conséquent, la planification, l'installation et la maintenance sont faciles à réaliser économiquement et techniquement.

Débits (kbit/s)	9,6	19,2	45,45	93,75	187,5	500	1 500	3 000	6 000	12 000
Longueur segment (m)	1200	1200	1200	1200	1000	400	100	100	100	100

Tableau 4.18 : Distances autorisées en fonction de la vitesse de transmission.

Les maîtres connectés au bus forment un anneau à jeton virtuel et sont classés par rapport à leur adresse de la plus petite à la plus grande. C'est au démarrage du réseau que la liste des maîtres est élaborée, ensuite le maître possédant l'adresse la plus petite acquiert le jeton en premier, il peut ainsi communiquer avec les autres maîtres ou avec ses esclaves ou tout simplement passer son tour, il retransmet ensuite le jeton au maître ayant l'adresse supérieure. La liste est mise à jour automatiquement lors d'un retrait ou d'une insertion d'un maître. La station maître qui possède le jeton est une station active.

4.4.5.4 Méthode d'accès au bus

La méthode d'accès au bus est évidemment liée à la topologie du système PROFIBUS. On distinguera fondamentalement les topologies de communication entre les topologies en étoile, les topologies en anneau et enfin les topologies en bus. Dans une topologie en étoile tous les nœuds communiquent à travers un calculateur central, qui détermine finalement la qualité et la sécurité de fonctionnement.

Le PROFIBUS utilise le réseau en bus. Dans ce système, tous les utilisateurs sont liés à un câble commun par l'intermédiaire d'une courte ligne de raccord. C'est pour cette raison, toute information transitant dans le câble sera reconnue de chaque nœud. L'autorisation d'envoi doit être régulée par la méthode d'accès au bus.

En PROFIBUS, on peut utiliser deux méthodes, à savoir la méthode par Passage de jeton (les maîtres sont classés par rapport à leur adresse de la plus petite à la plus grande) et la méthode « Maître/ Esclave ». C'est pour cela, on désignera aussi souvent la méthode d'accès PROFIBUS par procédé hybride. Pour la méthode Maître/Esclave, seul le maître possède le droit d'accès bus. Les esclaves ont seulement le droit de répondre aux ordres du maître. Cela est différent par rapport à la méthode passage de jeton (Token Passing). Dans ce cas -là, le droit d'accès est attribué au cours du passage du jeton et adjugé successivement aux seuls participants actifs. Seul le maître qui a le jeton peut accéder au bus et communiquer avec les autres participants actifs et passifs.

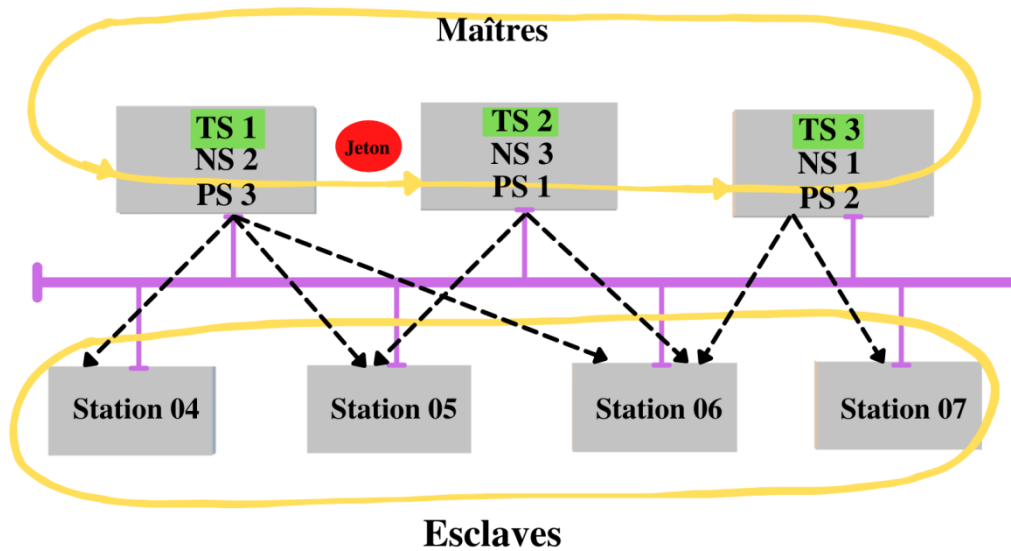


Figure 4.23 : Représentation du procédé d'accès hybride.

4.4.5.5 Terminaison de ligne

Résistances de terminaison équivalentes à l'impédance du câble pour polariser la ligne en l'absence de signal, le premier et le dernier nœud d'un réseau PROFIBUS doivent avoir une impédance de terminaison. Généralement, il est intégré dans le connecteur et activé par un interrupteur.

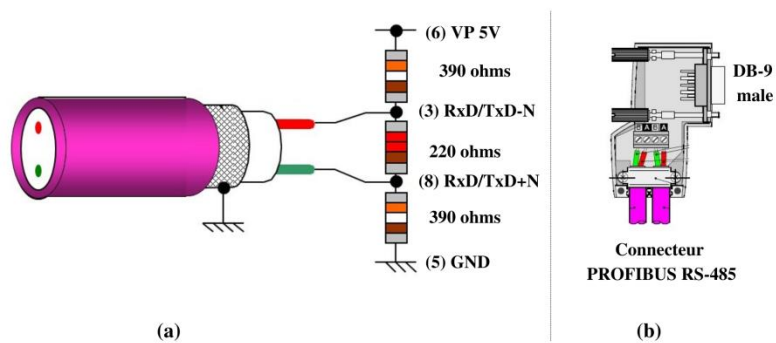


Figure 4.24 : (a) Terminaison pour RS-485 (b) Connecteur PROFIBUS RS-485.

4.4.5.6 Structure général Télégramme PROFIBUS DP

Trame maximum 255 Octets, transmission asynchrone, caractère sur 11 bits : 1 Start, 1 Stop, 8 data Bits, parité paire.

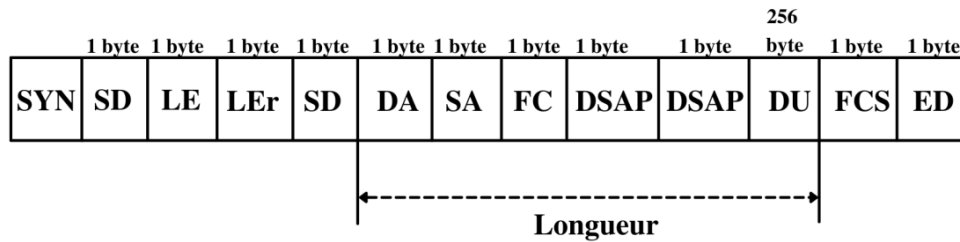


Figure 4.25 : Structure commune des télégrammes.

- **Sync Time** : La transmission de chaque trame est précédée d'une attente de synchronisation égale à 33 Temps Bits à ' 1 '. (1 Tbit = 83 ns pour 12 Mbit/s) ;
- **SYN** Temps de synchronisation (33 Tbits) ;
- **SD** Délimiteur de début de trame ;
- **LE** Longueur de la trame de DA à FCS ;
- **LEr** Répétition de la longueur de la trame ;
- **DA** Adresse Destination ;
- **SA** Adresse Source ;
- **DSAP** Point d'accès du service de destination ;
- **SSAP** Point d'accès du service de la source ;
- **DU** Données (244 octets Maximum) ;
- **FC** Contrôle (Requête/Réponse/Acquittement) ;
- **FCS** Clef de contrôle (Checksum) ;
- **ED** Délimiteur de fin (16H).

Différents types de télégrammes sont identifiés par leur SD, et les fonctions possibles de chaque type sont identifiées par leur FC. Le télégrammes de réponse a le même format que la trame envoyée ou adopte un format court sur l'octet de confirmation selon le type de télégrammes.

4.4.5.7 Conclusion

Le protocole PROFIBUS-DP peut être considéré comme une sous-famille du protocole PROFIBUS-FMS, optimisé pour la mise à jour rapide des données d'entrées-sorties. Le temps de cycle de produits comparables (ayant les mêmes objectifs) n'est pas totalement atteint pour 1.5 Mbits/s. cependant, cette vitesse est suffisante pour la majorité des applications. À 12 Mbits/s des temps de cycle très brefs sont réalisables.

Conclusion générale et Références Bibliographiques

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

De plus en plus d'équipements « intelligents » utilisés dans l'automatisation des sites de production vont générer de plus en plus de besoins de communication. Ethernet est sans aucun doute le système de base qui les satisfera dans les prochaines décennies.

Les réseaux de terrain classiques ont mis du temps à s'imposer mais ils font désormais partie de presque toutes les installations. Ils donnent satisfaction dans la majorité des cas, cependant, il faudrait basculer vers Ethernet.

La première chose à noter est qu'une telle migration n'est pas nécessaire, et le bus série peut encore fournir de nombreux services. En d'autres termes, Ethernet industriel présente des avantages importants qui doivent être évalués. Ne parlez que d'améliorations réelles, pas d'avantages théoriques:

- En ce qui concerne la vitesse, par exemple le bus de terrain le plus rapide (PROFIBUS DP) fonctionne à une vitesse maximale égale à 12 Mbits/s, l'essentiel des différents Ethernet industriel est fondé sur 100Mb/s ;
- Pour les séparations galvaniques, sur un bus de terrain tous les appareils d'un même segment utilisent le même média. Un problème sur un appareil, un connecteur, ou un câble peut affecter la communication de l'ensemble des nœuds. Avec Ethernet, le médium n'est pas partagé, le problème n'affectera que le nœud concerné par le lien ;
- Pour le champ électromagnétique, Ethernet s'avère plus robuste qu'un bus de terrain par rapport aux perturbations électromagnétiques, ce qui ne veut pas dire qu'il est totalement insensible ;
- Cohabitation de protocoles : Il n'est pas possible de faire cohabiter sur un même câble des équipements PROFIBUS et Modbus même si les 2 fonctionnent sur RS485. Grâce à Ethernet, vous pouvez vous connecter sur le même réseau, tel que les nœuds PROFINET et MODBUS/TCP, et utiliser le même réseau pour consulter une page web et envoyer un mail ;
- La technologie Ethernet permet d'accéder beaucoup plus facilement à l'appareil y compris à distance, que s'il se trouvait sur un bus série.

Références bibliographiques

1. « Réseaux locaux industriels - Cours et travaux pratiques » Pascal Vrignat, Editeur : Morin (gaetan) 1999, ISBN : 2-910749-19-3.
2. « Informatique industrielle et réseaux en 20 fiches », Jean-François Hérold, Olivier Guillotin, Patrick Anaya, Editeur : Dunod 2010, ISBN : 978-2-10-053051-9.
3. Réseaux de terrain. Description et critères de choix. CIAME. Editions Dunod. 1999.
4. Le bus CAN. D. Paret. Editions Dunod. 1998.
5. Le bus CAN. Applications. D. Paret. Editions Dunod. 1999.
6. Pujolle G., Les réseaux. Eyrolles.
7. Comer D., TCP/IP : architectures, protocoles et applications. InterEditions.
8. Tanenbaum A., Réseaux : architectures, protocoles et applications. InterEditions.
9. Les réseaux locaux industriels, F. LEPLACE et al. Editions Hermes, 1991.
10. Réseaux locaux industriels, Zoubir Mammeri et Jean-Pierre Thomesse, Edition Eyrolles, 1994.
11. Introduction aux Réseaux Locaux Industriels, P. Hoppenot, Université d'Evry Val d'Essonne 1999.
12. Réseaux et bus de terrain, Frank Singhoff, Université de Bretagne occidentale, 2002
13. Communication industrielle pour l'automatisation, Brochure SimaticNet, Siemens, Avril 2006.
14. Introduction aux bus et réseaux temps réel, Bertrand Dupouy, ENST 2007.
15. LES RESEAUX DE TERRAIN, Patrice KADIONIK, ENSEIRB, 2003.
16. Réseau Profibus, Eddy BAJIC & Bruno BOUARD, Techniques de l'ingénieur S8140.
17. CENELEC EN 50170 (1996a).General Purpose Field Communications System, volume 2/3 (PROFIBUS).
18. CENELEC EN 50170 (1996b).General Purpose Field Communications System, volume 3/3 (WorldFIP).
19. Mariño, P., Poza, F., Domínguez, M., and Nogueira, J. (1997).Transformation-Based Reactive Systems Development (ARTS'97), chapter Specification and Verification of a Real-Time Field Bus with Formal Description Languages, pages 415–429. Springer-Verlag.
20. Alexis Ferréro, Ethernet et ses évolutions, Edition AddisonWesley France, 1995.
21. Mariño, P., Poza, F., and Nogueira, J. (1996).Balanced Automation Systems II (BASYS'96), chapter Information System Based on Industrial Standard Protocols, pages 201–208. Chapman & Hall.
22. Mariño, P., Domínguez, M., Poza, F., and Nogueira, J. (1999).Fieldbus Technology (FET'99), chapter Formal Description Software for WorldFIP Industrial Fieldbus, pages 157–163. SpringerVerlag.
23. Mariño, P. (2003).Enterprise Communications: Standards, Networks and Services.RA-MA, 2nd edition.
24. <https://www.electronique-mixte.fr/wp-content/uploads/2018/07/Formation-Interface-communication-15.pdf> [Date de dernière consultation (20/08/2021)].

Conclusion générale et références bibliographiques

25. Jean Demartini, Introduction aux Automates programmables industriels et aux Réseaux locaux industriels, 1999 –2000.
26. Mohamad Khalil, Les réseaux locaux industriels, Université Libanaise.
27. Dominique Paret, Le bus CAN Description de la Théorie à la pratique, Edition DUNOD, Paris, 1999.