Matière : Réseaux et communication industriels
pour les étudiants au Master 1 Electronique Instrumentation

Chapitre I : Généralités sur les bus de terrain

I.1. TCP/IP et le modèle OSI

Le Modèle OSI (Open Systems Interconnection) : Le modèle d'Interconnexion des Systèmes Ouverts de l'ISO sert de référence à tous les systèmes de communication (Hard et Soft)

Le modèle OSI possède 7 couches :

- Couches 1 à 4 : couches basses chargées d'assurer un transport optimal des données.
- Couches 5 à 7 : couches hautes chargées du traitement des données.

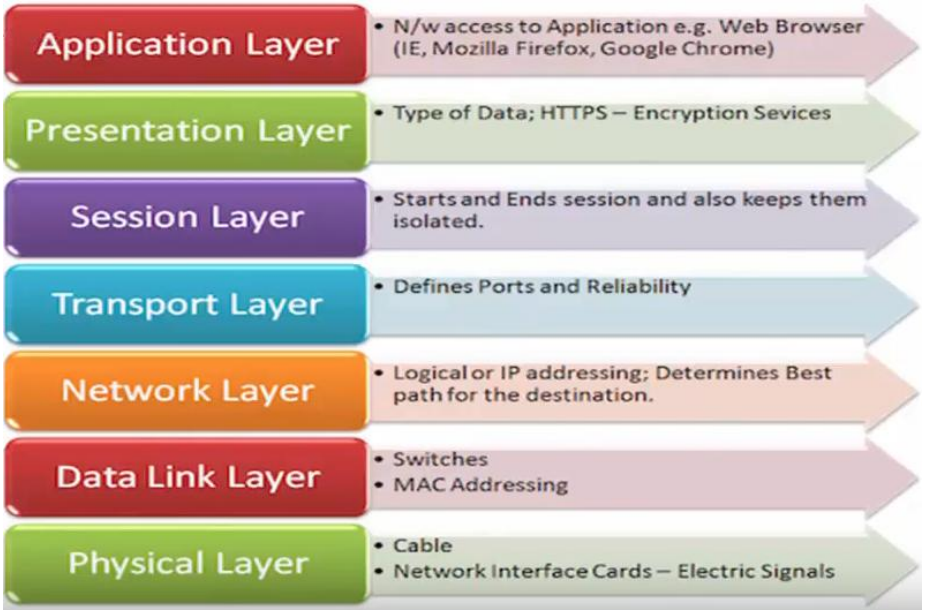


Tableau qui résume le rôle de chaque couche :

Numéro	Nom	Rôle
Couche 7	**Application**	C'est à ce niveau que sont les logiciels: navigateur, logiciel d'email, FTP, chat...
Couche 6	**Présentation**	Elle est en charge de la représentation des données càd du type de la donnée (image, vidéo, texte…) et du chiffrement.
Couche 5	**Session**	En charge d'établir, rompre et maintenir des sessions (càd

		assurer le dialogue de bout en bout) – et isolation entre les différentes sessions avec différents machines.
Couche 4	**Transport**	S'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement – en plus de définition des ports sur une session.
Couche 3	**Réseau**	Adressage IP et déterminer le meilleur chemin (càd routage).
Couche 2	**Liaison de données**	Adressage MAC (unique dans le monde entier) - détection d'erreur de transmission (en queue) – et synchronisation.
Couche 1	**Physique**	Support de transmission + interface réseau + signal physique.

Tableau 1: Modèle OSI

Le protocole TCP/IP étant antérieur au modèle OSI, il ne respecte pas réellement celui-ci. Cependant, on peut faire grossièrement correspondre les différents services utilisés et proposés par TCP/IP avec le modèle OSI, et obtenir ainsi un modèle en 4 couches.

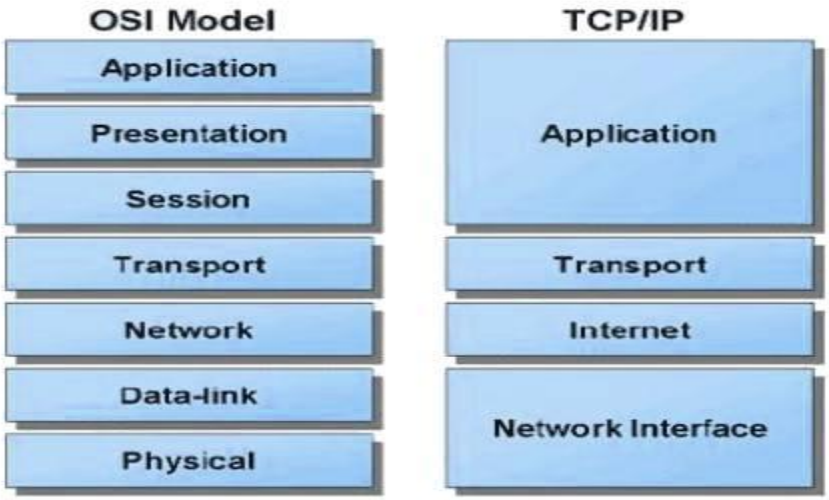


Figure : représentation du modèle TCP/IP

Les services des couches 1 et 2 (physique et liaison) du modèle OSI sont intégrés dans une seule couche (hôte-réseau) ; les couches 5 et 6 (session et présentation) n'existent pas réellement dans le modèle TCP/IP et leurs services sont réalisés par la couche application si besoin est.

Les deux principaux protocoles pouvant assuré les services de la couche Transport sont :

- **TCP** (Transmission Control Protocol) : protocole fiable, assurant une communication sans erreur par un mécanisme : ***question / réponse / confirmation / synchronisation*** (orienté connexion) ;

- **UDP** (User Datagram Protocol) : protocole non-fiable, assurant une communication rapide mais pouvant contenir des erreurs en utilisant un mécanisme ***question / réponse*** (sans connexion).

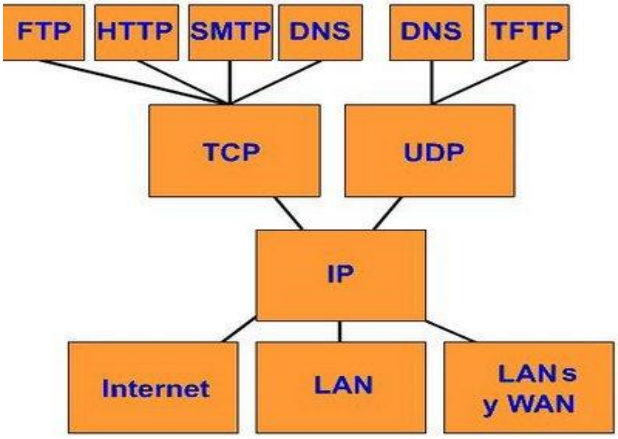


Figure : Structure en couche du modèle TCP/IP

I.2. Définition d'un bus de terrain

Le terme bus de terrain est utilisé par opposition au bus informatique. En effet, le bus de terrain est en général beaucoup plus simple. Il est également plus robuste face aux perturbations externes. L'élément le plus couramment lié à un bus de terrain est l'automate programmable industriel.

Le niveau 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 ou d'un ensemble.
Les distances de communications sont assez faibles par rapport aux autres types de réseaux, souvent inférieures à quelques dizaines de mètres.
Donc, les câbles utilisés en industries sont renforcés selon le cas d'utilisation et les conditions à la quelles sont exposés tel que les températures basses et élevées les produits chimiques, le rayonnement électromagnétique, les chocs, … etc.

Câble RJ45 résistant à la température + 150°

Câble RJ45 résistant à la température + 180°

Câble RJ45 résistant aux perturbations

Câble industriel en fibre

Les réseaux de terrain sont de plus en plus intégrés dans le monde industriel. On trouve aujourd'hui deux types de standards de réseaux de terrain :

- Standards de faits : tel que Interbus qui est un système de communication série qui transmet des données entre les systèmes de contrôle, (par exemple, les ordinateurs, les automates programmables etc) et les modules d'E/S répartis dans l'espace, qui sont reliés à des capteurs et des

actionneurs. LONWorks, Local Operating NetworkWorks (technologie utilisant le NEURON et les composants Echelon).

- Standards internationaux : tel que : WorldFIP(World Factory Instrumentation Protocol Europe), Profibus(Process Field Bus USA)

I.3. Avantages des réseaux de terrain

Le but initial des bus de terrain était de remplacer les anciens systèmes centralisés en distribuant le contrôle, le traitement des alarmes, le diagnostic aux différents équipements qui sont devenus de plus en plus intelligents.

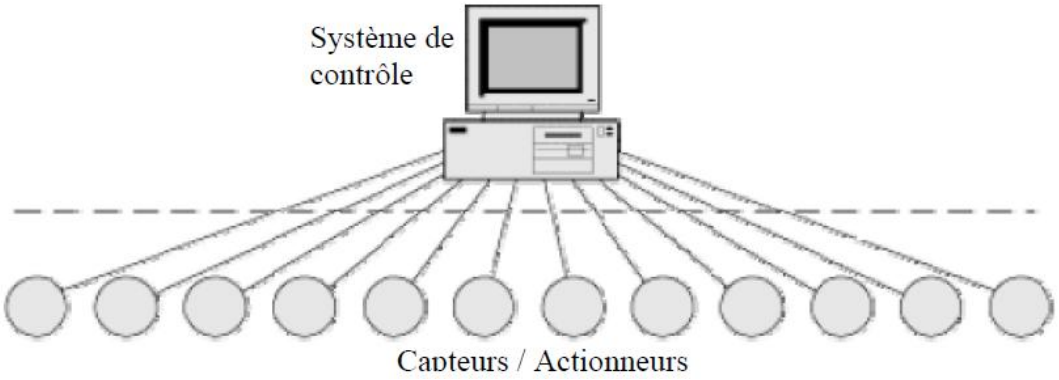


Figure : Système de contrôle centralisé

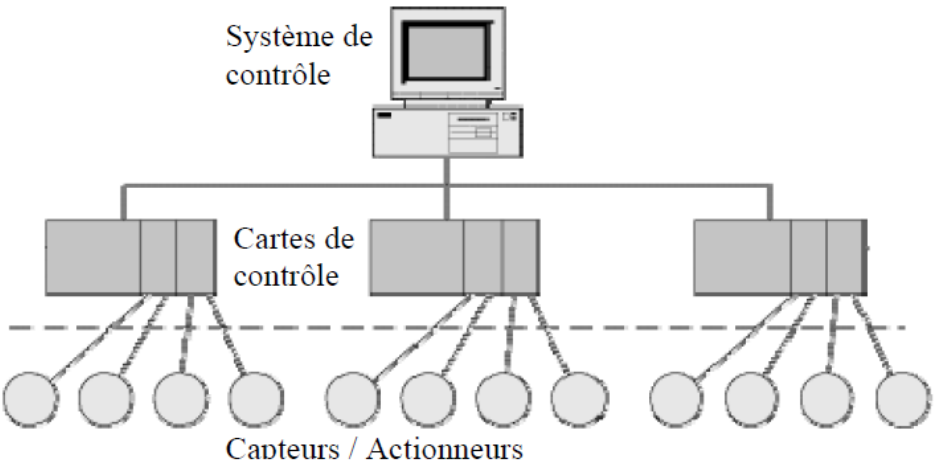


Figure : Système de contrôle distribué

Cela permet plusieurs avantages :

1- Réduction des coûts initiaux : Réduction massive du câblage : un seul câble en général pour tous les équipements au lieu d'un par équipement. Ainsi que réduire le temps d'installation.

2- Réduire le coût d'exploitation en : Augmentant les performances de l'automatisme

3- Réduction du coût de maintenance : moins de complexité, donc moins de maintenance (fiabilité accrue). Temps de dépannage réduit, localisation des pannes possibles grâce à des diagnostics en ligne («on line»).

4- La distribution du contrôle et sa numérisation permettent d'atteindre des performances intéressantes dans les réseaux de terrain :

- Précision : communications numériques.
- Les données et mesures sont généralement disponibles à tous les équipements de terrain.
- Communications possibles entre deux équipements sans passer par le système de supervision.

Remarque : Pour les standards WorldFIP, INTERBUS, ASi, LonWorks et Ethernet font partie du programme de la matière : Réseaux Locaux Industriels supposés vus en 3ième année Licence.

Chapitre II. Le bus 485 MODBUS

II.1. Rappel sur la Norme RS232 (V28)

Il y a trois organismes de normalisation :

- UIT : Union Internationale des Télécommunications (CCITT : Comité Consultatif International des Téléphones et Télégraphes).
- ISO : International Standardisation Organisation.
- EIA : Electrical Industry Alliance

Une liaison série est une ligne où les bits d'information (1 ou 0) arrivent successivement, soit à intervalles réguliers (transmission synchrone), soit à des intervalles aléatoires, en groupe (transmission asynchrone).

La liaison RS232 est une liaison de communication ***série***, ***asynchrone***, ***full-duplex***, dans laquelle pour chaque signal, ***le support est un fil référencé par rapport à la masse***. Sa vitesse de transmission peut aller jusqu'à 115 kbits/s. La distance séparant les deux équipements ne dépasse pas généralement 15 m.

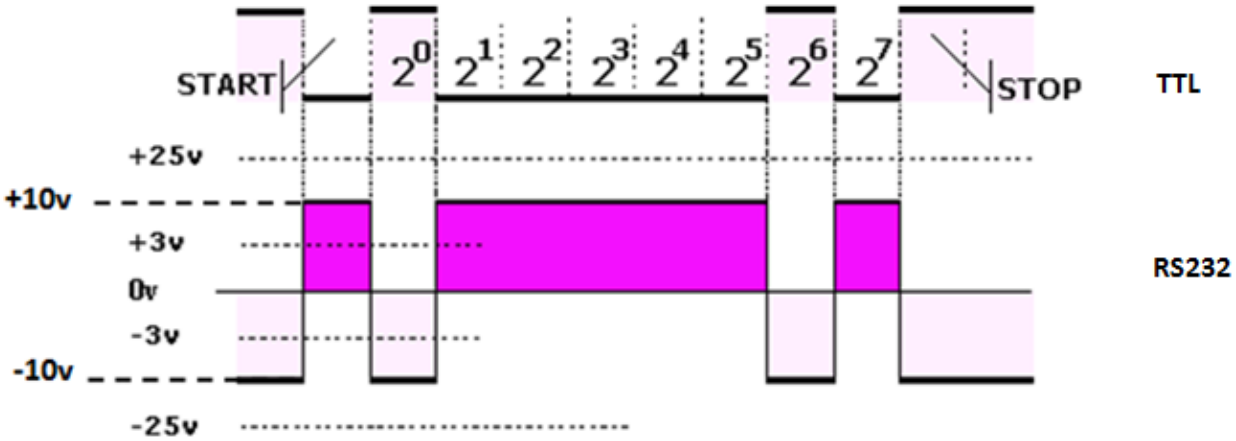
Son principe :

Dans la norme RS232, les bits de poids faibles (LSB) sont envoyés en-tête, inversement à la notation ASCII ordinaire ($b_6\, b_5\, b_4\, b_3\, b_2\, b_1\, b_0$, où le MSB à gauche et LSB à droite). La norme permet d'adapter les signaux logiques « 0 » « 1 » comme suit :

« 1 » logique = 5V devient après adaptation de -3V à -25V, (Typiquement ***-12V***).

« 0 » logique = 0V devient après adaptation de +3V à +25V,, (Typiquement ***+12V***).

Les deux tensions -12V et +12V peuvent être adaptées à -10V et +10V pour des raisons pratiques par le biais d'un circuit intégré (MAX 232 à 16 pins) comme l'illustre la figure ci-dessous :



Forme du connecteur DB9 :

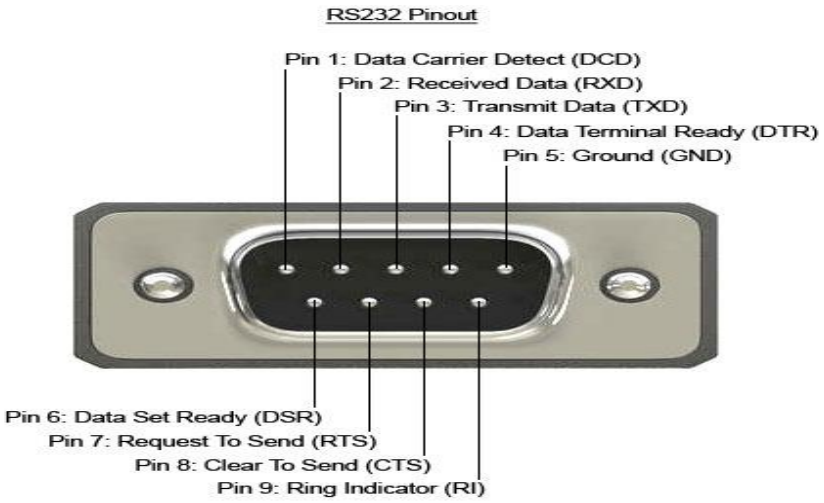


Figure : Interface RS232 appelée DB9 (male)

Le broche « 2 » : appelé ***RXD*** représente le circuit de réception de données (Received Data), alors que le broche « 3 » appelé ***TXD***, représente le circuit d'émission (Transmited Data), et le broche « 5 » définit une masse commune pour toutes les circuits (***GND***).
Les broches 7 et 8 sont appelées RTS et CTS respectivement, pour assurer le contrôle de flux.

L'octet à transmettre est envoyé bit par bit ***(bit de poids faible (LSB) en tête)*** par l'émetteur sur la broche ***TXD***, vers le récepteur sur la broche ***RXD.*** La vitesse de transmission de l'émetteur doit être identique à la vitesse d'acquisition du récepteur. Ces vitesses sont exprimées en ***Bauds*** (1 baud correspond à 1 bit / seconde, dans notre cas). Il existe différentes vitesses normalisées: 300, 600, 1200, 2400, 4800, 9600 ou 19200, 38400, 57600, 115200 Bauds (ou « bits/sec » dans ce cas).

- ***Transmission asynchrone :***

La transmission étant du type asynchrone (pas d'horloge commune entre l'émetteur et le récepteur), des bits supplémentaires sont indispensables au fonctionnement: un bit de début de mot (***START***) ayant un niveau d'un '0' logique, et un bit(s) de fin de mot (***STOP***) ayant un niveau d'un '1' logique. D'autre part, l'utilisation éventuelle d'un bit de ***parité***, permet la détection d'erreurs de transmission, comme le montre la figure suivante :

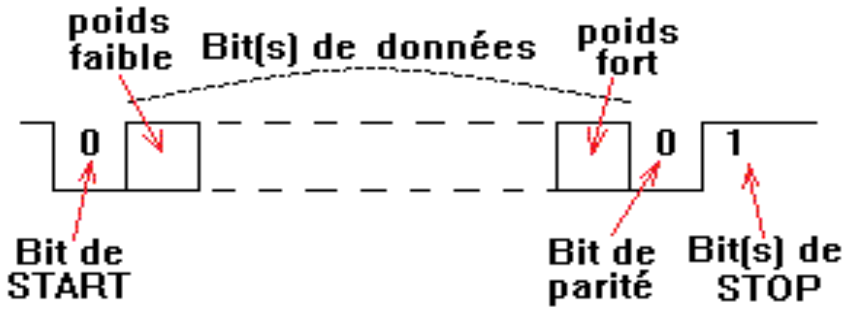
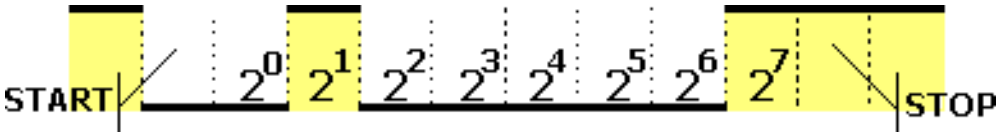


Figure : Transmission asynchrone

Exemple :

Transmission du code $82 avec 1 bit de stop et sans bit de parité : $82 donne %1000 0010 :

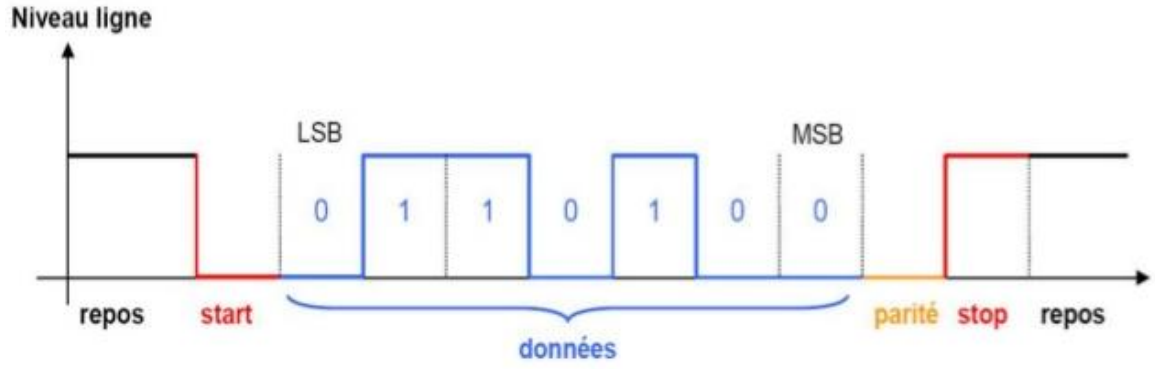


- ***Bit de parité :***

La parité est une technique qui permet de vérifier que le contenu d'un mot n'a pas été changé accidentellement lors de sa transmission. L'émetteur compte le nombre de '**1**' logiques dans le mot et met le bit de parité à **1** si le nombre trouvé est impair, ce qui rend le total pair : on dit que la parité est '***paire***'.

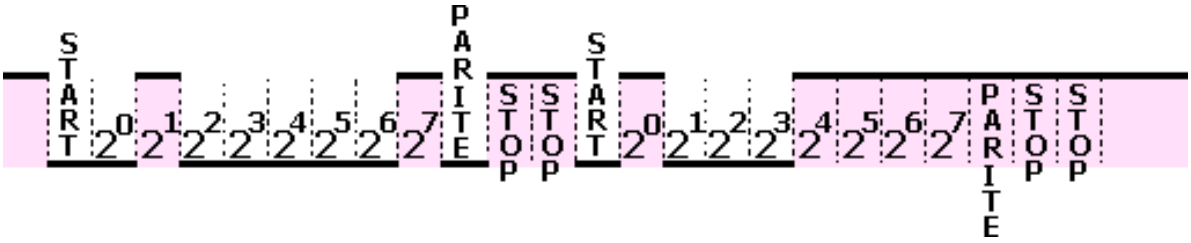
NB : On peut aussi utiliser la parité impaire en procédant inversement.

Exemple 01 :



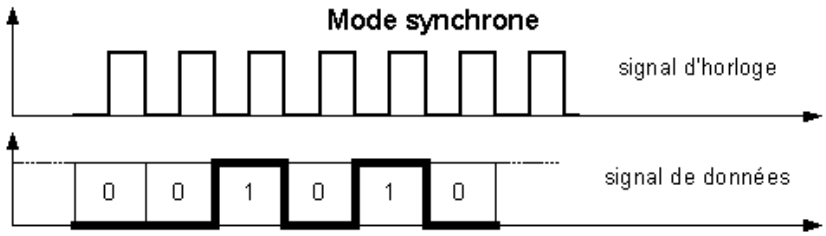
Transmission du mot 0010110
avec une parité impaire et 1 bit de Stop

Exemple 02: transmission de $82, puis $F1, avec parité paire et 2 bits de " stop ", soit : %1000 0010 puis %1111 0001, ce qui donne la suite des bits suivante :



- **Transmission synchrone**

Dans le mode synchrone l'émetteur et le récepteur sont cadencés à la même horloge. Le récepteur reçoit de façon continue (même lorsque aucun bit n'est transmis) les informations au rythme où l'émetteur les envoie. C'est pourquoi il est nécessaire que l'émetteur et le récepteur soient cadencés à la même vitesse. De plus, des informations supplémentaires sont insérées afin de garantir l'absence d'erreurs lors de la transmission.

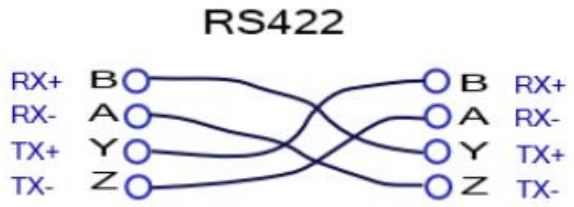


Lors d'une transmission synchrone, les bits sont envoyés de façon successive sans séparation entre chaque caractère, il est donc nécessaire d'insérer des éléments de synchronisation, on parle alors de **synchronisation au niveau trame** (il faut savoir le début de chaque trame).

Avantages de la transmission série :

- ✓ nombre de fils réduits: la communication la plus simple peut être faite sur 3 fils (1 TXD, 1 RXD et une Masse).
- ✓ communication sur de grandes distances à travers le réseau téléphonique, par utilisation d'un MODEM (MODulateur-DEModulateur): exemple : Liaison ADSL pour Internet.

Remarque : Il existe une liaison appelée ***RS422*** qui est une amélioration de la norme RS232 en version ***différentielle***, qui a l'avantage sur cette dernière de pourvoir transmettre des données jusqu'à 10 nœuds récepteurs et permet une transmission sur une distance allant jusqu'à 1200 m. Pour des communications sur longue distance, l'utilisation d'une résistance de terminaison spéciale de 120 ohms devient obligatoire. Elle est installée pour éviter la réflexion du signal à chaque extrémité de la ligne.



Pour raccorder plusieurs stations sur le même bus de données, une version plus évoluée sera présentée dans le paragraphe suivant.

II.2. Liaison Modbus RS485 (V11) Symétrique ou différentielle

RS485 est une liaison ***série***, de type ***asynchrone, symétrique***, ***half duplex***, comporte deux conducteurs actifs par sens de transfert. L'émetteur possède un amplificateur différentiel qui va transmettre les états logiques à la double ligne de transmission sous forme de deux tensions complémentaires V+ et V- ou V- et V+ selon le niveau logique.

Le récepteur est également un montage à amplificateur opérationnel, il n'est donc concerné que par la différence de tension entre les deux fils de ligne.

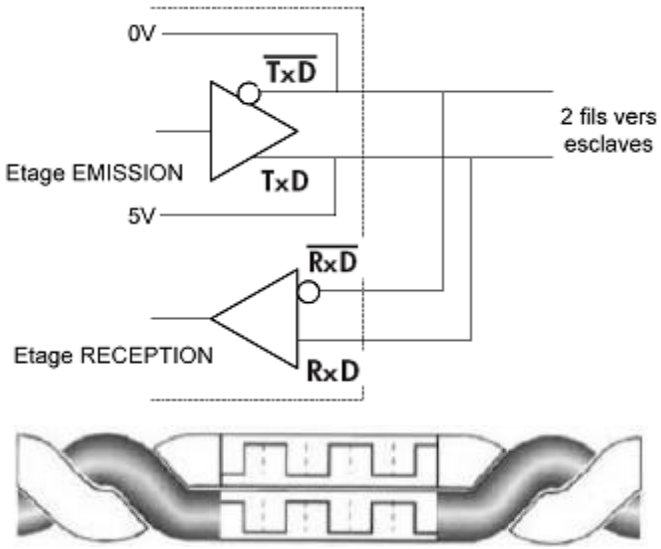
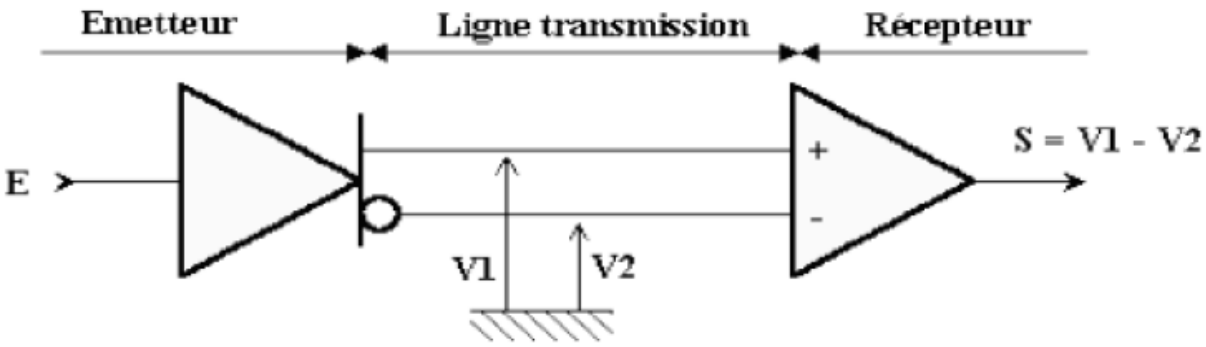
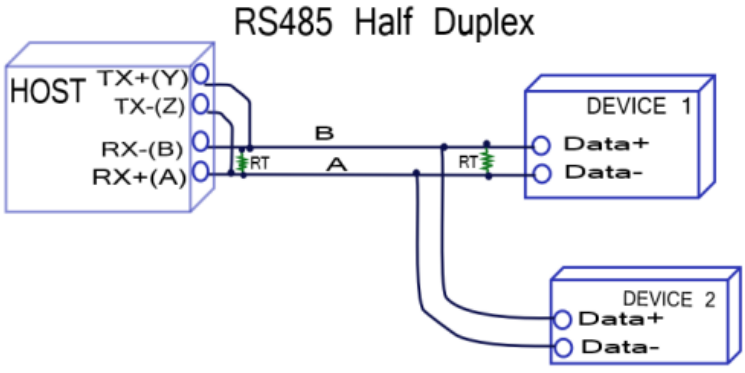


Figure : Structure des connecteurs et forme torsadée des fils



En half-duplex, une seule paire de signaux (A, B) est utilisée. Il ya deux configurations possibles qui sont : 2 fils (half-duplex) et 4 fils (full-duplex). La connexion RS-485 à 2 fils est illustrée ci-dessous :

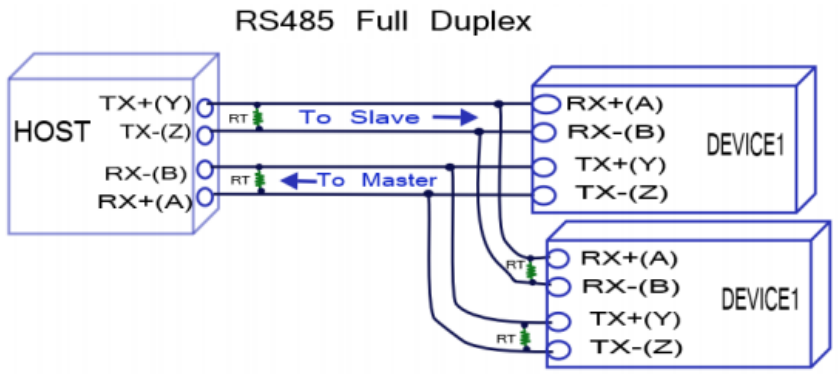


Cette dernière configuration différentielle permet de transmettre des données sur de **grandes distances** (jusqu'à 1200 m) à des **vitesses élevées** (jusqu'à 100kbit/s). De plus, elle est peu sensible

aux parasites induits, ceux-ci affectent les deux fils de la ligne et se trouvent inhibés par l'entrée différentielle du récepteur.

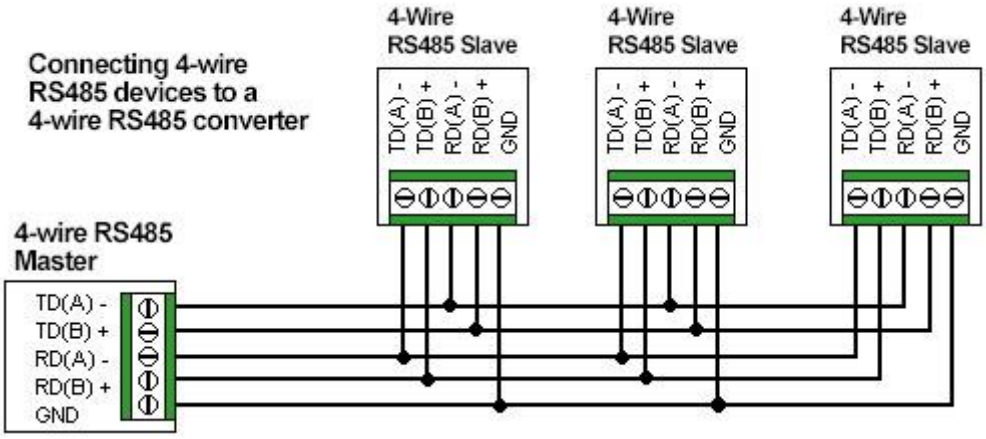
E	V1	V2	Parasites	S = V1 - V2
0	-V	+V	Vp	(-V + Vp) - (+V + Vp) = -2V
1	+V	-V	Vp	(+V + Vp) - (_V + Vp) = +2V

L'implémentation en Full-Duplex nécessite deux paires de signaux (quatre fils), voir la figure ci-dessous :

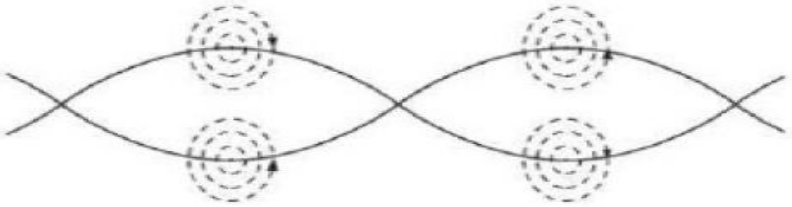


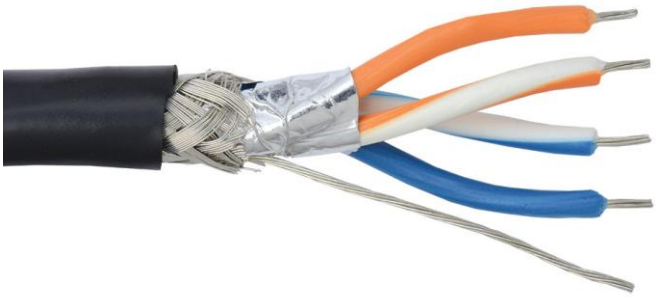
Cette dernière structure offre une ligne de transmission équilibrée qui peut être également partagé en mode multipoint selon une topologie "en bus". La norme spécifie jusqu'à 32 équipements qui peuvent être raccordés dans un tel réseau en bus, avec deux résistances de terminaison sur les deux extrémités pour éviter un signal réfléchi.

En pratique la connectique entre un maitre et 3 esclaves est de cette manière :



La liaison RS485 utilise comme medium de communication des ***câbles à paires torsadés*** avec ou sans blindage, qui sont moins sensibles aux champs magnétiques car les tensions induites par les variations de flux s'annulent mutuellement.





II.3. Différences majeures entre les différents standards RS232/RS422/RS485

Les principales différences sont le medium de communication (une paire torsadée), un mode de tensions différentielles, et la possibilité de travailler en réseau (Topologie en bus).

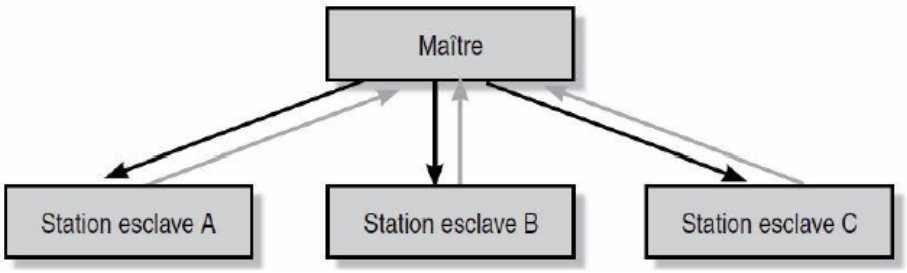
Le tableau suivant illustre les caractéristiques de différents standards RS232/422/485 en termes de Débit et distance maximal du câble.

EIA CCITT	RS232C V24 / V28	RS422 V11 / X27	RS485 V11 / X27
Type d'interface	unipolaire	Différentiel	Différentiel
Distance	15 m	1200 m	1200 m
Débit max.	19200 Bauds	10 MBds	10 MBds
Multipoint	non	oui	oui
Nombre d'émetteurs	1	1	32
Nombre récepteurs	1	10	32

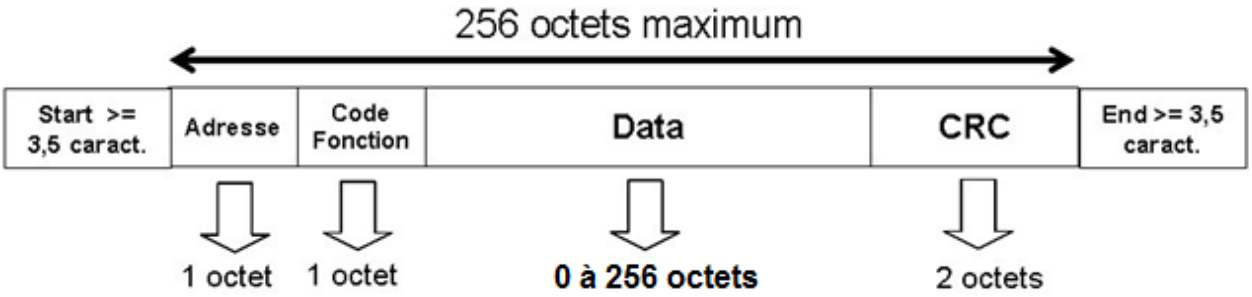
II.4. Adressage et Trame MODBUS RTU (Remote Terminal Unit)(couche liaison)

Le mode de transmission utilisé est le mode RTU.

Le protocole Modbus est un protocole de dialogue basé sur une structure hiérarchisée entre un maître et plusieurs esclaves (stations). Il permet de lire et d'écrire certaines valeurs.

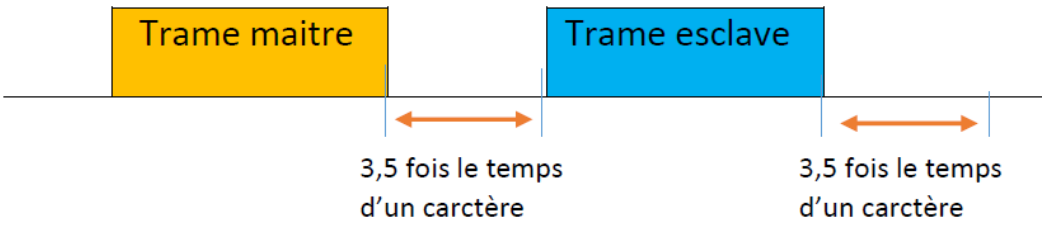


La trame ne contient ni octet d'en-tête de message, ni octet de fin de message. Elle est définie de la manière suivante :



- Adresse (esclave) : Ces adresses vont de 1 à 247 et ne doivent pas obligatoirement être attribuées de manière séquentielle. Deux stations esclaves ne peuvent pas avoir la même adresse.
- Code Fonction : Il va de 1 à 24, il contient un code fonction indiquant à l'esclave adressé le type d'action à réaliser.
- Data : Les données contiennent des informations complémentaires dont l'esclave a besoin pour exécuter cette fonction.
- CRC : Cyclical Redundancy Check permet à l'esclave de s'assurer de l'intégrité du contenu de la question.

Avant et après chaque message (trame), il doit y avoir un silence minimum de 3,5 (START/END) fois le temps de transmission d'un octet. L'ensemble du message doit être transmis de manière continue. Le temps maximum entre 2 octets (caractères) doit être inférieur à 1,5 fois le temps de transmission d'un octet. Dans le cas contraire, il y a une erreur de transmission.



Si un silence de plus de (3,5 x temps de transmission d'un caractère) intervient en cours de transmission, le destinataire du message considérera que la prochaine information qu'il recevra sera le début d'un nouveau message. Dans le cas contraire, il y a une erreur de transmission.

Chaque octet composant un message est transmis en mode RTU de la manière suivante :

Sans contrôle de la parité :

Start	B0	B1	B2	B3	B4	B5	B6	B7	Stop	Stop

Avec contrôle de la parité

Start	B0	B1	B2	B3	B4	B5	B6	B7	Parité	Stop

Dans le cas d'un contrôle de parité, il vous est demandé de confirmer l'état du contrôle : paire (even) ou impaire (odd).

Exemple : Si le débit de transmission est 9600 bits/s, on aura un silence de :

3,5 caractère = (3,5 * 11 * (1/9600)) = 4.0104 ms

Calcul du CRC

Le contrôle appelé CRC (Cyclical Redundancy Check), codé sur 2 octets (16 bits), Il est basé sur la fonction XOR et démarre sur un polynôme arbitraire, et il est souvent calculé en binaire.

Le CRC est calculé par l'émetteur puis inclus dans la trame avant d'être transmise. Le récepteur recalcule le CRC et le compare avec le CRC reçu. Si les valeurs sont différentes alors il y a une erreur dans la transmission du message.

Exemple :

Polynôme générateur : $C(x) = x^3 + x^2 + 1$ → 1101

Message à transmettre : $M(x) = x^7 + x^4 + x^3 + x$ → 10011010

Le degré de $C(x)$ est 3, donc on écrit 3 zéros à droite de notre message : 10011010**000**

On applique le XOR avec la séquence de contrôle $C(x)$, en éliminant les zéros qui se trouvent à gauche du résultat, et chaque étape on fait descendre des bits pour compléter le sous-message à 4, et on fait le XOR avec $C(x)$ de nouveau et ainsi de suite, le reste est appelé CRC. Le message envoyé sera donc le message précédent à lequel on rajoute le CRC à droite. Ainsi, au niveau réception, le récepteur effectue la même opération XOR sur le message reçu est calculera le CRC, s'il est nul donc pas d'erreur, dans le cas contraire, on sera en présence d'une erreur de transmission.

10011010000

1101

1001

1101

1000

1101

1011

1101

1100

1101

1000

1101

---

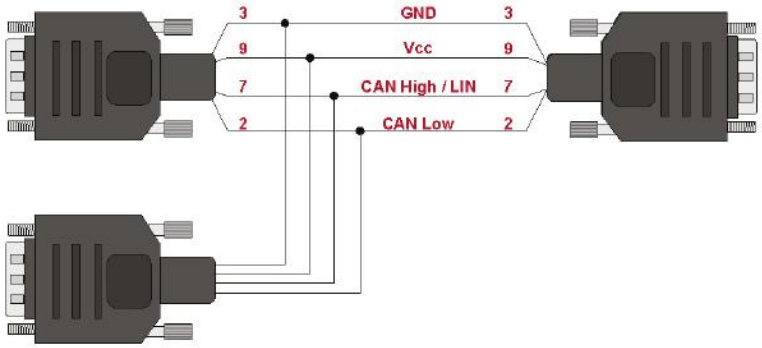
101 → R=M modulo C

Le message à transmettre sera le message $M(x)$ suivi du reste de la division : 10011010101.

Le récepteur recalcule de la même manière le CRC, s'il trouve un reste « zéro » donc pas d'erreur, et vice versa.

Chapitre III : Le bus CAN (Controller Area Network)

Le CAN (Controller Area Network) fait partie des bus de terrain les plus utilisés dans les applications industrielles (automobile, automatisme, etc.), dans lesquelles la communication entre les différents modules nécessite un bus d'échange d'information en temps réel. Le bus CAN permet de raccorder plusieurs équipements et unités de contrôle sur un seul bus ayant seulement deux lignes, où la communication se fait par tour de rôle. L'autre avantage de ce bus est de permettre une communication de longue distance qui se diffère selon le débit de transmission.



III.1. Le Bus CAN et le modèle OSI

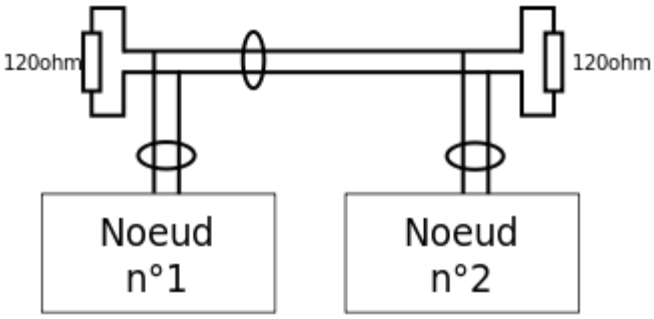
Le bus CAN est basé sur les 3 couches du modèle OSI à savoir : la couche physique, la couche liaison et la couche application, les autres couches ne sont pas présentes.

Couche physique :

Le CAN est un bus de données ***série half-duplex***, utilise des paires différentielles torsadées (souvent blindées) conformes à RS485 (réduction des perturbations), on en distingue deux normes pour la couche physique :

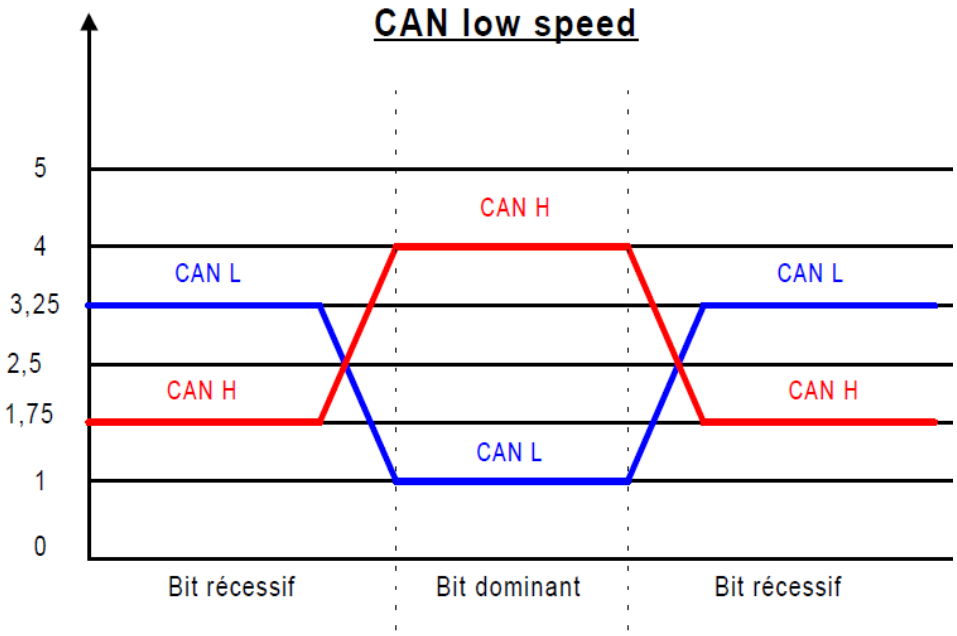
- CanL ou CAN Low speed ISO 11898-3 : (jusqu'à 125 Kbits/s, 2 à 20 nœuds, longueur limitée par la capacité parasite).
- CanH ou CAN High speed ISO 11898-2 : (jusqu'à 1 Mbits/s, 2 à 30 nœuds, 30m à 1 Mbits/s).

Chaque nœud connecté sur le bus CAN peut communiquer avec tous les autres. Les deux extrémités du bus doivent être rebouclées par des résistances de 120 Ω.



Les états logiques et les niveaux électriques utilisés entre les deux lignes de la paire différentielle pour le CAN low-speed sont les suivants :

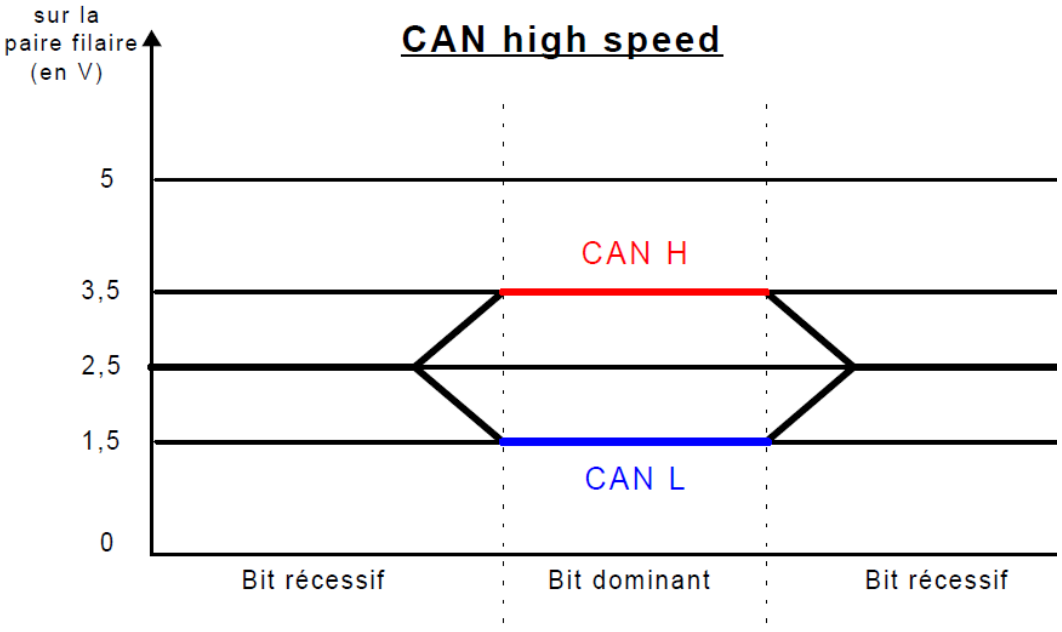
Niveau	CANH <> masse	CANL <> masse	CANH <> CANL
Récessif ou « 1 »	1,75 V	3,25 V	-1,5 V
Dominant ou « 0 »	4 V	1 V	3 V



Niveaux de tension du bus CAN *low speed*

Les états logiques et les niveaux électriques utilisés entre les deux lignes de la paire différentielle pour le CAN high-speed sont les suivants :

Niveau	CANH <> masse	CANL <> masse	CANH <> CANL
Récessif ou « 1 »	2,5 V	2,5 V	de 0 à 0,5 V
Dominant ou « 0 »	3,5 V	1,5 V	de 0,9 à 2 V



Niveaux de tension du bus CAN *high speed*

Le brochage sur le bus CAN est normalisé et utilise un connecteur DB-9 comme celui de RS232 avec une nomination des broches montrée sur le tableau ci-dessous.

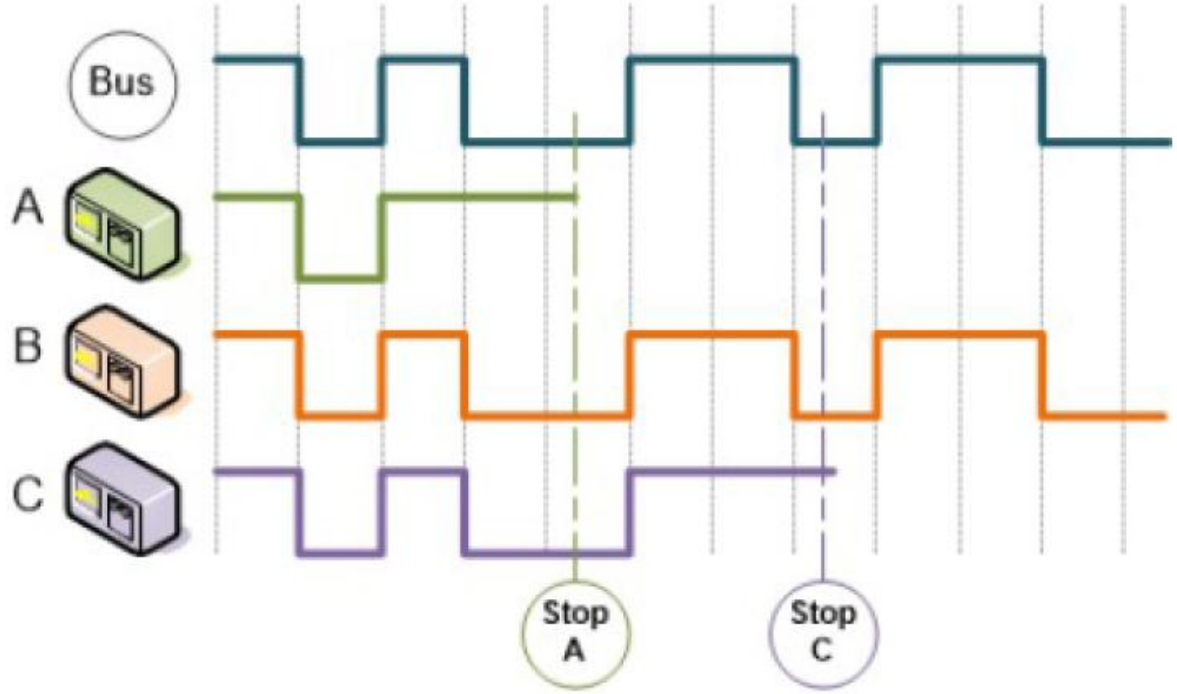
Broche	Description
1	(Réservé)
2	CANL
3	Masse
4	(Réservé)
5	Blindage (optionnel)
6	Masse
7	CANH
8	(Réservé)
9	Alimentation externe (optionnel)

III.2. Méthode d'accès au bus CAN et code utilisé

L'accès au bus CAN suit la technique CSMA/CR (écoute de chaque station avant de parler mais pas de tour de parole, résolution des collisions par priorité).

Cette méthode est légèrement plus évoluée que la méthode CSMA/CD : si plusieurs stations transmettent un message, elles appliquent un ET logique entre le signal reçu et le signal émis. Dans le cas d'une inégalité, la station s'arrête de transmettre. Comme le 0 est une valeur dominante, elle

écrase donc le 1 (état récessif) : cela signifie que la communication de l'une des stations n'est pas modifiée (pour laquelle il y a égalité) et permet ainsi de terminer cette communication sans délai d'attente ou de retransmission (voir la figure ci-dessous) :



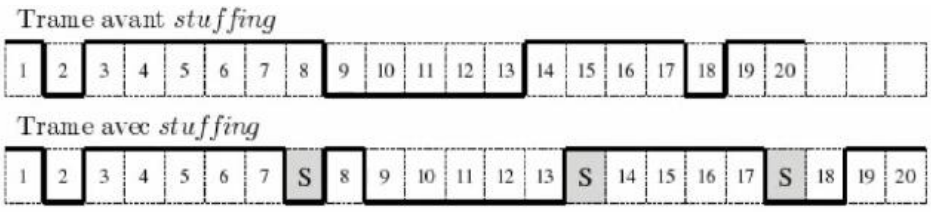
Exemple : Message émis par la station A : **1 1 0 1 0 1 1 0 0**

Message reçu par la station A : **1 1 0 1 1 0 1 0 1**

« ET » logique → **1 1 0 1 0 0 1 0 0**

Le CAN utilise un codage NRZ. Afin de ne pas laisser de grande suite de 1 ou de 0, après 5 bits de valeur identique, un bit de la valeur opposée est inséré (retiré à la réception), ce qui permet un plus grand nombre de transitions : éviter les problèmes de désynchronisation de l'horloge. Cette méthode est appelée « **bit stuffing** ».

Exemple : Message à transmettre : 1011111101000000101 → 10111110101000001**0**101



Il y a évidemment un mécanisme pour que le récepteur arrive à distinguer les bits stuffing de ceux de l'information pour les éliminer systématiquement.

Couche liaison CAN

III.3. La trame de données CAN

Pour la couche de liaison de données il existe également 2 standards:

- ISO 11898 part A → CAN 2.0A « standard frame format » (identification sur 11 bits),
- ISO 11898 part B → CAN 2.0B « extended frame format » (identification sur 29 bits).

Il existe plusieurs types de trames CAN échangées entre les nœuds :

- Trame de données,
- Trame de requête,
- Trame d'erreur,
- Trame de surcharge.

Entre 2 trames successives, les émetteurs doivent respecter une pause (période d'inter-trame) équivalente à au moins la durée de 3 bits pendant laquelle le bus est maintenu à l'état récessif.

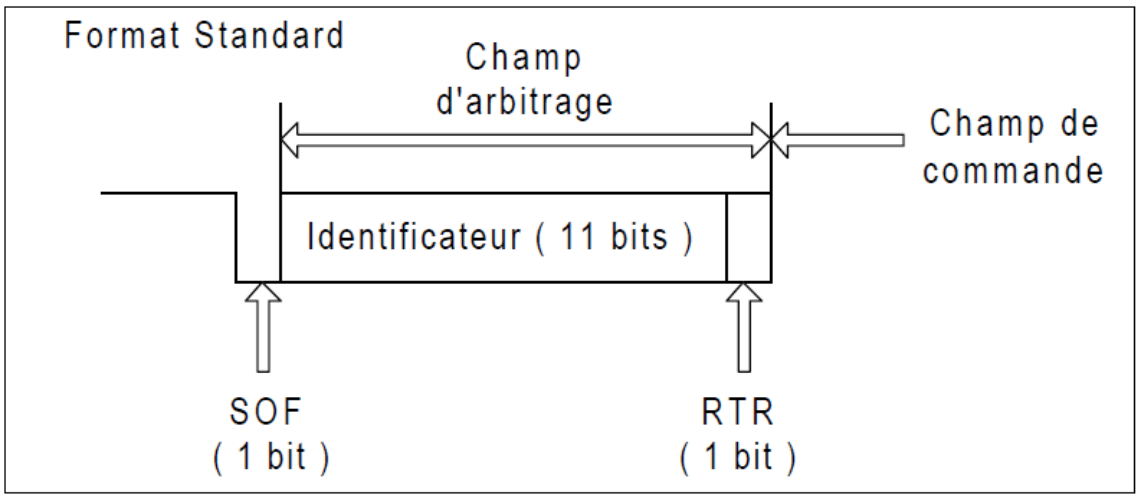
La trame de données sert à envoyer des informations aux autres nœuds et elle se compose de 7 champs différents :

- Le début de trame ou SOF (Start Of Frame) matérialisé par un bit dominant « 0 »,
- Le champ d'arbitrage (identificateur de la donnée du champ 'données') composé de 12 ou 30 bits, (ISO 11898 part A / ISO 11898 part B). Le dernier bit est un RTR (Remote Transmission Request) qui soit dominant pour les trames de données et récessif pour les trames de requête.
- Le champ de commande (indiquant le nombre d'octets dans 'le champ de données DATA) composé de 6 bits,
- Le champ de données composé de 0 à 64 bits (de 0 à 8 octets),
- Le champ de CRC composé de 16 bits,
- Le champ d'acquittement composé de 2 bits,
- La fin de trame ou EOF (End of Frame) matérialisée par 7 bits récessifs « 1 » sans bits stuffing.

Start of frame	Arbitration Field	Control Field	Data Field	CRC Field	ACK Field	End Of Frame
1 bit	12 ou 30 bit	6 bit	de 0 à 8 octets	16 bit	2 bit	7 bit

Les champs sont transmis dans l'ordre du SOF vers EOF, et dans chaque champ de la trame, les bits sont transmis du plus fort (MSB) au plus faible (LSB).

Le champ d'arbitrage permet de déterminer la priorité de la trame, plus il est petit, plus il contient des bits de poids forts à 0 (dominant), plus la trame sera prioritaire (puisque le MSB est en-tête). Il est composé de 11 bits d'identification pour CAN 2.0A et 29 bits pour CAN 2.0B suivis par le bit RTR (Remote Transmission Request).



Ce champ sert d'identifiant pour la donnée transportée dans le champ de données.

Les 11 bits de CAN 2.0A autorisent 2^{11} = 2048 combinaisons.

Les 29 bits de CAN 2.0B autorisent 2^{29} = 536 870 912 combinaisons.

Le champ de commande (contrôle) est composé de 6 bits.

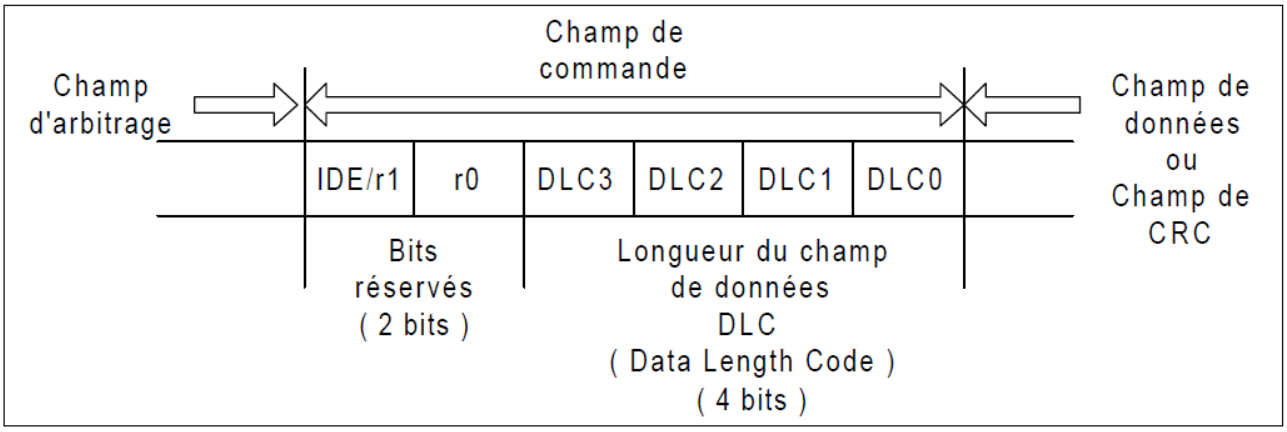
Le bit de poids fort est utilisé pour différencier le type de trame :

- Dans le cas d'une trame standard (sur 11 bits), le bit de poids fort MSB est dominant « 0 »,
- Dans le cas d'une trame étendue (sur 29 bits), le bit de poids fort MSB est récessif « 1 »,

Le bit suivant n'est pas utilisé (réservé).

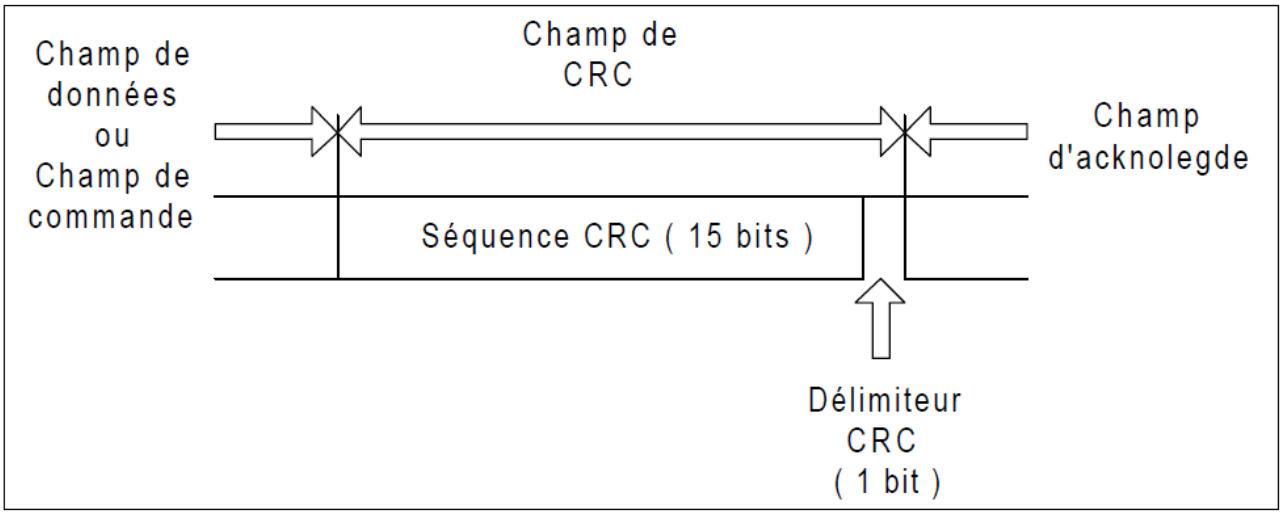
Les 4 bits de poids faibles appelés DLC (Data length Code) représentent le nombre d'octets du champ de données (PAYLOAD) embarqué.

Ce nombre d'octets peut varier de 0 à 8, soit 9 valeurs stockées avec les 4 bits du champ DLC. Les valeurs DLC supérieures à 9 ne seraient donc pas utilisées (de 9 à 15).



Le champ de données peut varier de 0 à 8 octets (au max) avec MSB en tête. Dans le cas d'une trame de requête le champ de données est vide (de longueur nulle).

Le champ de CRC est composé de 15 bits et d'un bit dit délimiteur (« CRC delimiter ») qui est toujours récessif '1'.

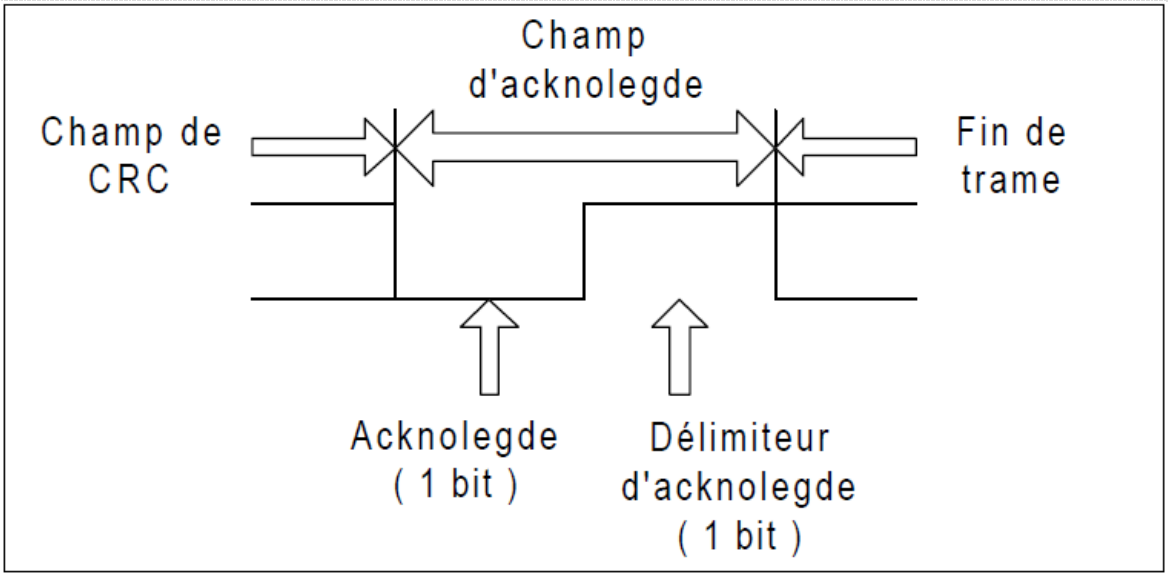


Le CRC est calculé à partir de l'ensemble des champs transmis jusque là (c'est-à-dire le SOF, le champ d'arbitrage, le champ de commande et le champ de données; les bits de transparence (stuffing) ne sont pas pris en compte). L'ensemble constitue le polynôme f(x).

Le polynôme ainsi formé est divisé (modulo 2) par le polynôme $g(x)=x^{15}+x^{14}+x^{10}+x^{8}+x^{7}+x^{4}+x^{3}+x^{0}$ soit donc : 1100010110011001.

Une fois les divisions successives effectuées (XOR), le reste constitue la séquence de CRC.

Le champ d'acquittement ACK est composé d'un bit d'acquittement ACK (ACKnowledge) et d'un bit dit délimiteur (« ACKnowledge delimiter ») toujours récessif.



Tous les récepteurs qui ont bien reçu le message doivent l'acquitter en émettant un bit dominant pendant la durée du bit ACK, ce qui permet au nœud émetteur de savoir qu'au moins un des nœuds récepteurs a reçu le message.

Si un nœud récepteur n'a pas ou mal reçu le message, il ne peut pas se servir de ce mécanisme pour signaler l'erreur, puisqu'il suffit qu'une station réceptrice envoie un bit dominant pour masquer tous les bits récessifs. Pour signaler le dysfonctionnement, il doit émettre une trame d'erreur.

Référence utile pour le CAN :

https://www.technologuepro.com/cours-systemes-embarques/cours-systemes-embarques-Bus-CAN.htm

Chapitre IV : PROFIBUS

IV.1. Définition :

Profibus (Process Field Bus) est le nom d'un type de bus de terrain inventé par la société Siemens et devenu peu à peu une norme de communication dans le monde de l'industrie. Il s'appuie sur une liaison RS485.

Spécialement conçus pour une mise en œuvre en environnement industriel (ateliers), les réseaux PROFIBUS se distinguent par une excellente immunité aux perturbations électromagnétiques d'où une grande sécurité des données. Ils ont des passerelles vers Ethernet TCP/IP et utilisent des supports soit en RS485 différentielle soit en Fibre Optique soit en CEI 1158-2.

Le bus de terrain PROFIBUS fait la liaison entre le système d'automatisation, les modules de périphérie et les appareils de terrain.

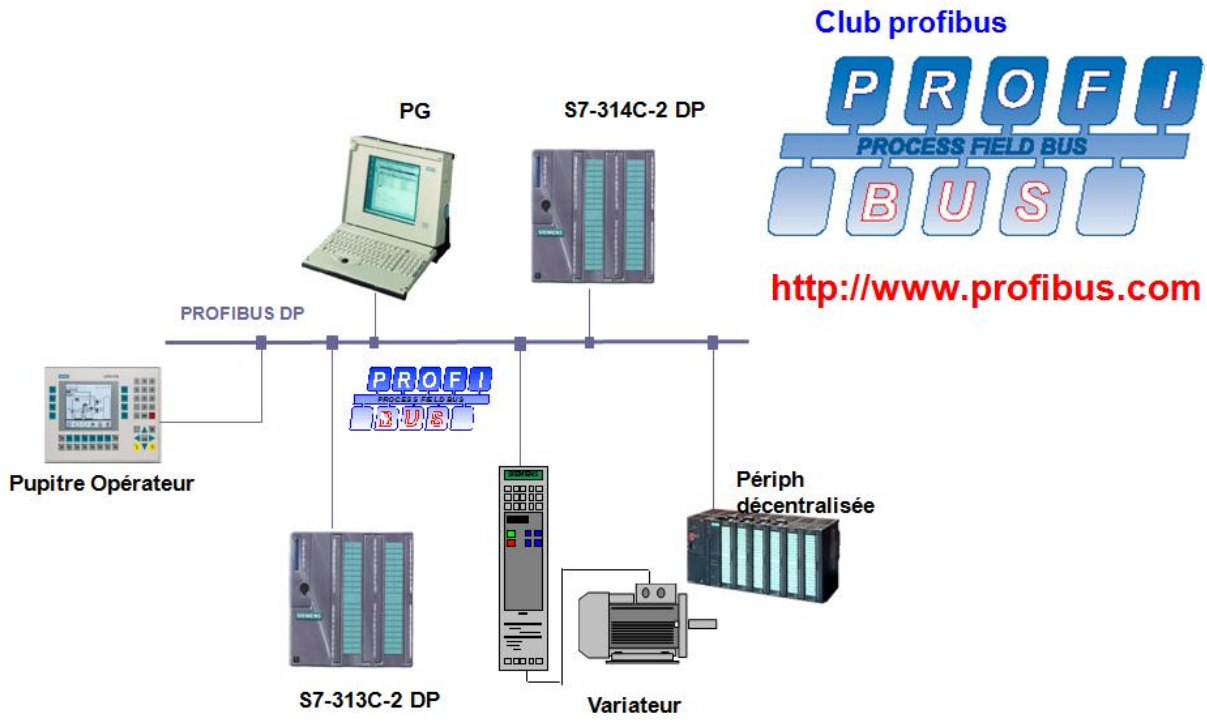


Figure : Domaines d'utilisation de Profibus

PROFIBUS est un système de communication ouvert acceptant les appareils de divers constructeurs sans passer par des interfaces spécialisées (compatible). Il se prête aussi bien à la transmission de données exigeant des actions en des temps de réaction très courts, qu'aux échanges de grandes quantités d'informations complexes. Il est actuellement standardisé dans les normes IEC 61158 et EN 50 170.

IV.2. Méthode d'accès sur Profibus :

Est une méthode hybride appelée Token-Bus/maître-esclave. La procédure d'accès sur PROFIBUS est conforme aux méthodes "Token Bus" pour les stations actives (Maîtres) et "maître-esclave" pour les stations passives (Esclaves), décrites par la norme CEI 61158-2 / EN 61158-2.

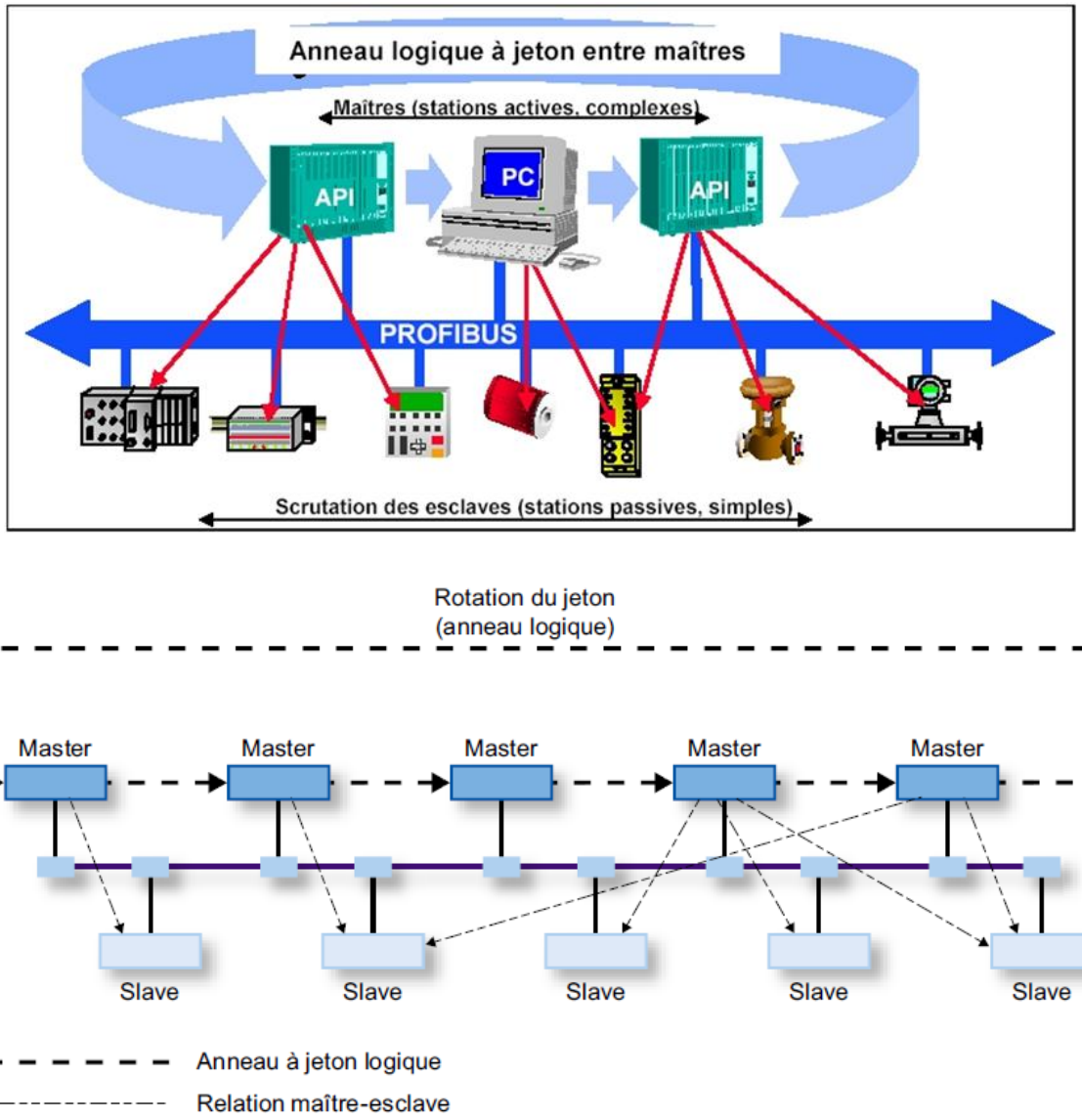


Figure : Méthode d'accès sur Profibus

Cette procédure d'accès permet d'ajouter ou de supprimer des stations du réseau en cours de fonctionnement sans pour autant arrêter le réseau.

Il existe deux variantes de Profibus en cours d'utilisation, le plus couramment utilisé est Profibus DP, tandis que celui le moins utilisé c'est Profibus PA, et aussi FMS qui est remplacée par TCP/IP.

IV.3. Le protocole PROFIBUS PA (Process Automation)

Le bus PROFIBUS-PA (Process Automation) est utilisé en technique des processus et génie chimique pour le contrôle des instruments de mesure par un système de conduite de processus. Les câbles bus ne véhiculent qu'un faible courant qui, même en cas d'incident, ne produit pas d'étincelle susceptible de provoquer une explosion. (Son utilisation est en général dans des milieux qui présentent des dangers d'explosion). Le même câble porte de l'alimentation et du signal d'information et supporte jusqu'à 31,25 kbit/s comme débit maximum de transmission de données.

IV.4. Le protocole PROFIBUS DP (périphérie décentralisée)

Le bus PROFIBUS-DP (Decentralised Peripheral) (périphérie décentralisée) est utilisé pour la commande de capteurs, d'actionneurs ou d'automates programmables par une commande centrale dans une usine de production où les applications sont automatisées.

La majorité des automates Siemens disposent d'une ou deux interfaces Profibus-DP pour le dialogue avec le PC de programmation. Mise à part sa fonction servant à lier le PC de programmation à la CPU, le Profibus-DP peut servir de liaison entre un maître (par exemple la CPU) et ses esclaves.

On reconnaît facilement un câble Profibus-DP par la couleur : violet. En l'ouvrant, on distingue 2 fils : un vert et un rouge, nommés "A" et "B". Les deux fils sont en paire-torsadée blindée, soigneusement isolés par une feuille conductrice et une tresse.

Figure : Câble Profibus-DP

En général, les connecteurs Profibus sont des connecteurs DB9 plus ou moins standards. Le fil "A" est relié à la pin n°3 du connecteur DB9, tandis que le fil "B" est relié à la pin n°8.

IV.5. Terminaison de lignes :

Ce sont des résistances de terminaison équivalentes à l'impédance du câble pour polariser la ligne en l'absence de signal. En général, elles sont intégrées dans le connecteur et activables par un interrupteur.

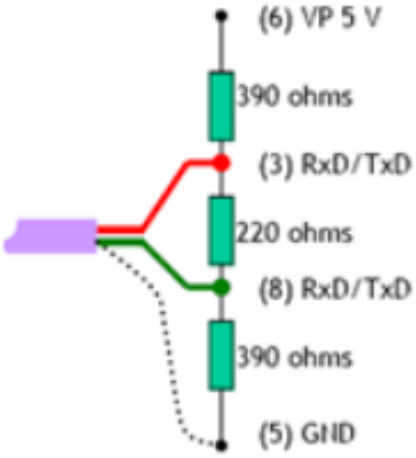


Figure : Terminaison de ligne

IV.6. Débit et distance de Profibus

Le principe de la communication Profibus-DP est basé sur la méthode maître-esclave. Le maître interroge cycliquement un ou plusieurs esclaves.

On distingue deux types de maîtres DP :

- le maître de classe 1 : il pilote cycliquement le processus
- le maître de classe 2 : il assure le paramétrage des appareils et le diagnostic

Avantages :

- protocole de communication très rapide car très proche du matériel
- utilisable avec des systèmes d'autres marques.

Chapitre V : Aperçu sur les réseaux industriels sans fils

V.1. le standard IEEE 802.11

IEEE 802.11 est un ensemble de normes concernant les réseaux sans fil locaux (le Wi-Fi) qui ont été mises au point par le groupe de travail 11 du comité de normalisation LAN/MAN de l'IEEE (IEEE 802). Le terme « 802.11x » est également utilisé pour désigner cet ensemble de normes.

V.1.1. L'architecture en couches

La norme IEEE 802.11 définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Cette dernière est elle-même subdivisée en deux sous-couches, la sous-couche LLC (Logical Link Control) et la couche MAC (Medium Access Control). La figure suivante illustre l'architecture du modèle proposé par le groupe de travail 802.11 comparée à celle du modèle OSI.

<table>
<tr><td rowspan="2">OSI Layer 2
Data Link Layer</td><td colspan="6">802.11 Logical Link Control (LLC)</td></tr>
<tr><td colspan="6">802.11 Medium Access Control (MAC)</td></tr>
<tr><td>OSI Layer 1
Physical Layer (PHY)</td><td>FHSS</td><td>DSSS</td><td>IR</td><td>Wi-Fi
802.11b</td><td>Wi-Fi
802.11g</td><td>Wi-Fi5
802.11a</td></tr>
</table>

Chaque couche physique 802.11/a/b/g est divisée en deux sous-couches :

- la sous-couche PMD (Physical Medium Dependent) qui gère l'encodage des données et effectue la modulation
- la sous-couche PLCP (Physical Layer Convergence Protocol) qui s'occupe de l'écoute du support et fournit un CCA (Clear Channel Assessment) à la couche MAC pour lui signaler que le canal est libre.

Les cinq couches radio du standard IEEE 802.11/a/b/g utilisent des fréquences situées dans des bandes dites sans licence. Il s'agit de bandes libres, qui ne nécessitent pas d'autorisation de la part d'un organisme de réglementation. Les deux bandes sans licence utilisées dans 802.11/a/b/g sont :

- la bande ISM (Industrial, Scientific and Medical)
- la bande U-NII (Unlicenced-National Information Infrastructure).

V.1.2. La bande ISM

La bande ISM utilisée dans 802.11/b/g correspond à une bande de fréquence située autour de 2.4 GHz, avec une largeur de bande de 83.5 MHz (2.4 GHz – 2.483 5 GHz). Cette bande ISM est reconnue par les principaux organismes de normalisation, tels que la FCC au Etats-Unis, l'ETSI en Europe, l'ART en France. La largeur de bande libérée pour les RLAN varie cependant suivant les pays (voir tableau suivant).

Pays	*Bande de fréquences*
Etats-Unis (FCC)	2.400-2.485 GHz
Europe (ETSI)	2.400-2.4835 GHz
Japon (MKK)	2.471-2.497 GHz
France (ART)	2.4465-2.4835 GHz

V.1.3. La bande U-NII

La bande sans licence U-NII est située autour de 5 GHz. Elle offre une largeur de bande de 300 MHz (plus importante que celle de la bande ISM qui est égale à 83.5 MHz). Cette bande n'est pas continue mais elle est divisée en trois sous-bandes distinctes de 100 MHz. Dans chaque sous bande la puissance d'émission autorisée est différente. La première et la deuxième sous bande concernent des transmissions en intérieur. La troisième sous-bande concerne des transmissions en extérieur. Comme pour la bande ISM, la disponibilité de ces trois bandes dépend de la zone géographique. Les Etats-Unis utilisent la totalité des sousbandes, l'Europe n'utilise que les deux premières et le

Japon la première. Les organismes chargés de réguler l'utilisation des fréquences radio sont : l'ETSI (European Telecommunications Standards Institute) en Europe, la FCC (Federal Communications Commission) aux Etats-Unis, le MKK (Kensa-kentei Kyokai) au Japon.

V.2. ZigBee

Est un protocole de haut niveau permettant la communication de petites radios, ***à consommation réduite***, basée sur la norme IEEE 802.15.4 pour les réseaux à dimension personnelle (Wireless Personal Area Networks : WPAN).

La technologie **ZigBee** permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, jouets, ...). La technologie ZigBee, opérant sur la bande de fréquences des 2,4 GHz et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ.

Agréées le 14 décembre 2004, les spécifications de ZigBee 1.0 sont disponibles auprès des membres de la communauté industrielle ZigBee Alliance.

Cette technologie a pour but la communication de courte distance telle que le propose déjà la technologie Bluetooth, tout en étant moins chère et plus simple.

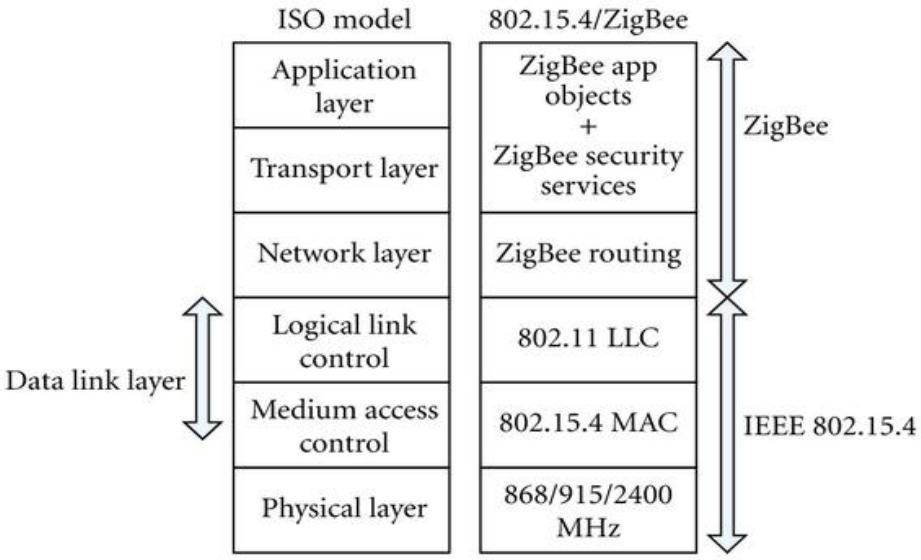
Comparaison des protocoles Zigbee, Bluetooth et Wi-Fi

Caractéristique	Zigbee	Bluetooth Low Energy	Bluetooth	Wi-Fi
IEEE	802.15.4	802.15.1	802.15.1	802.11a/b/g/n/ac
Besoins mémoire	4-32 ko		250 ko +	1 Mo +
Autonomie avec pile	Années	Années	Mois	Jours
Nombre de nœuds	65 000+	illimité	255	256+
Vitesse de transfert	20-250 kb/s	1 Mb/s	1-3 Mb/s	11-54-108-320-1000 Mb/s
Portée (environ)	10 m [1]	10 m	10 m	100 m

On retrouve ZigBee dans les contrôles industriels, les applications médicales, les détecteurs de fumée et dans la télécommande de la freebox v6.

V.2.1. ZigBee et Modèle OSI

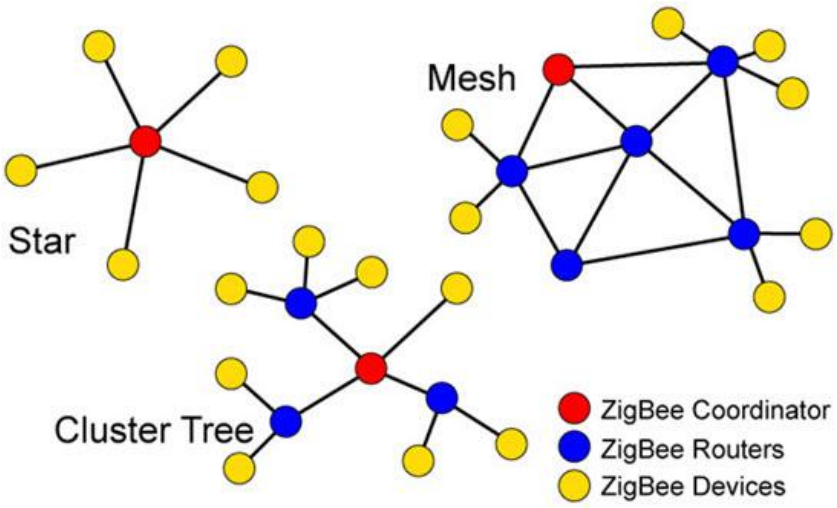
ZigBee est conforme avec le modèle OSI dans sa structure en couches comme le montre la figure ci-dessous :



Dans cette structure on remarque que le standard ZigBee contient les 5 couches du modèle OSI à savoir : application, transport qui est intégrée dans la couche application, et constitue avec la couche réseau (routing) les spécifications ZigBee, liaison et physique.

V.2.2. Topologies de ZigBee

Dans le standard ZigBee on peut réaliser des réseaux de différentes topologies : étoile, arbre et maillée comme le montre cette figure.



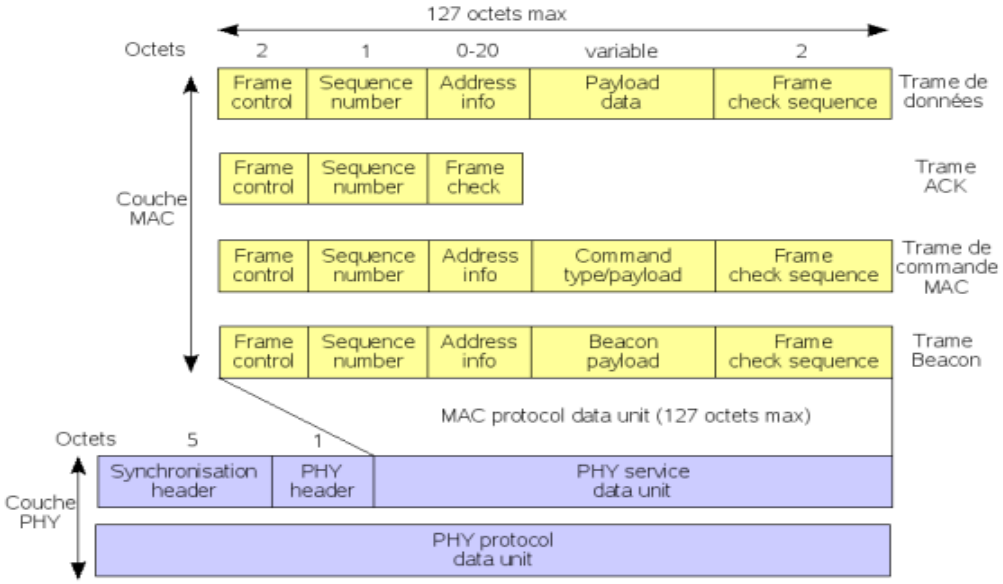
V.2.3. Fréquences utilisées

Le protocole 802.15.4 utilisé par ZigBee définit 3 bandes de fréquences utilisables :

Bande	Disponibilité	Nombre de canaux	Vitesse maxi théorique
868 MHz	Europe	1	20 kbit/s
915 MHz	Amériques et Australie	10	40 kbit/s
2.4 GHz	Disponible partout	16	250 kbit/s

V.2.4. Structure de trames (couche liaison)

Le standard 802.15.4 définit 4 types de trame de base : Données, ACK, commande MAC et beacon.



Le champ Frame Control indique type de trame MAC et spécifie le format du champ adresse

Le champ Sequence Number assure l'ordre à la réception et permet l'acquittement des trames MAC

Le champ adresse est variable de 0 à 20 octets en fonction du type trame :

- data : adresse source et adresse destination
- acquittement : pas d'adresse

Le champ de données permet une charge utile jusqu'à 104 octets.

Le FCS (Frame Check Sequence) assure que la trame est transmise sans erreur.

La trame de commande MAC permet le contrôle et la configuration à distance des nœuds par le coordinateur PAN.

Les trames de balisage (Beacon) réveillent les modules clients qui attendent leur adresse et se rendorment s'ils ne la reçoivent pas. Les trames beacon sont importantes dans les réseaux maillés et les clusters d'étoile pour que les nœuds soient synchronisés avec une consommation d'énergie minimum.

V.2.5. Méthode d'accès au support

Deux méthodes d'accès au canal :

- Réseau sans trames "Beacon" : CSMA-CA (carrier-sense medium-access with collision avoidance) avec acquittement des paquets reçus correctement.
- Réseau avec trames "Beacon" : utilisation d'une structure de "super-trame" pour contrôler l'accès au canal.

La structure de super-trame est mise en place par le coordinateur en transmettant des trames Beacon à des intervalles réguliers (multiples de 15.38ms, jusqu'à 252s).

V.3. Protocoles de communication HART et WirelessHART

Highway Addressable Remote Transducer (HART) est un protocole de communication utilisé en contrôle industriel pour communiquer numériquement avec des capteurs ou actionneurs dits intelligents.

Il consiste à enrichir une boucle de courant 4-20 mA, classiquement utilisée de manière analogique, en y superposant un courant alternatif de valeur moyenne nulle, dont la modulation de fréquence véhicule des informations de manière numérique1.

Le WirelessHART est une version sans fil de ce protocole. Elle est une norme industrielle ouverte, développée pour les besoins particuliers de la communication sans fil au niveau terrain dans le génie des procédés. Elle remplit l'ensemble des exigences spécifiques en termes de fiabilité, de sécurité, de rentabilité et de convivialité.

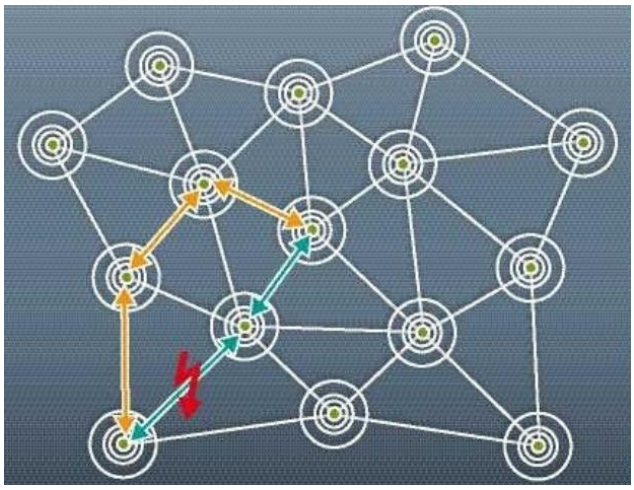
La technologie WirelessHART utilise une bande de 2,4 GHz, utilisée sans licence dans le monde entier, comme mode de transfert pour plusieurs technologies radio, comme WLAN, Bluetooth et ZigBee.

WirelessHART utilise un réseau maillé non étoilé où toutes les stations radio (appareils de terrain) forment un réseau. Chaque station participante sert simultanément de source de signal et de répétiteur. Le transmetteur d'origine envoie un message à son voisin le plus proche, qui transmet le message jusqu'à atteindre la station de base et le récepteur proprement dit. De plus, des itinéraires alternatifs sont configurés pendant la phase d'initialisation. Si le message ne peut pas être transmis via un chemin particulier, à cause d'un obstacle ou d'un récepteur défectueux, le message est transféré automatiquement vers un itinéraire alternatif. En plus d'étendre la portée du réseau, le réseau maillé non étoilé fournit donc des voies de communication redondantes pour plus de fiabilité.

La communication dans le réseau sans fil est coordonnée avec TDMA (Time Division Multiple Access), qui synchronise les composants du réseau par blocs de temps de 10 ms. On obtient ainsi un réseau très fiable (sans collision) et on réduit les délais d'exécution et les temps morts pendant lesquels une station doit rester active.

Pour éviter tout brouillage, WirelessHART utilise aussi FHSS (Frequency Hopping Spread Spectrum). Les 15 canaux tels que définis dans IEEE802.15.4 sont utilisés en parallèle ; WirelessHART utilise FHSS pour « sauter » d'un canal à l'autre. Les canaux déjà utilisés sont désactivés pour éviter les collisions avec d'autres systèmes de communication sans fil.

La combinaison de la synchronisation 10ms et des 15 canaux permet 1 50 communications par seconde.



Réseaux WirelessHART pour l'automatisation des procédés

La communication sans fil s'impose rapidement pour les applications d'automatisation. Pour l'automatisation des procédés, ce n'est pas la quantité de données qui pose problème, mais les distances à couvrir. Chaque fois que l'architecture de l'usine ne permet pas de recourir à un câblage conventionnel, l'accès aux données n'est possible qu'en se rendant fréquemment sur le terrain.

WirelessHART propose une solution économique. Les valeurs mesurées sont disponibles régulièrement, ce qui se traduit par une qualité accrue et des opérations moins coûteuses pour les usines de transformation.

Les équipements WirelessHART :

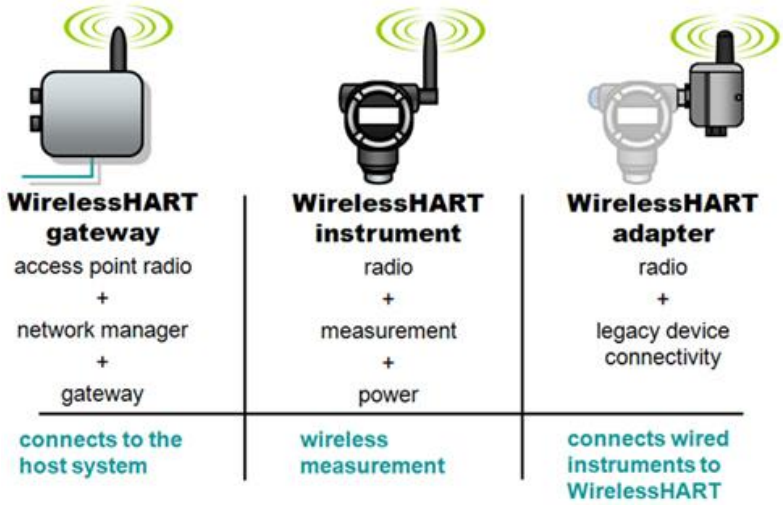
Les appareils WirelessHART permettent l'installation d'appareils de terrain de différents fabricants sans efforts de câblage – et donc sans coûts - supplémentaires. Une communication fiable et sans interférence est établie entre les composants suivants :

Passerelles :

La passerelle WirelessHART, qui établit la connexion sans fil avec le réseau, est à la fois l'élément central et l'équipement le plus évolué d'un réseau WirelessHART. Elle est équipée d'une ou de plusieurs interfaces pour des systèmes hôtes (RS 485, Ethernet, PROFIBUS) et elle est équipée d'un « gestionnaire de réseau » et d'un « gestionnaire de sécurité ».

Adaptateurs :

Les adaptateurs WirelessHART peuvent être connectés à tous les appareils de terrain HART conventionnels ou 4 … 20 mA, directement ou à l'aide d'un câble court. Ces adaptateurs lisent les données de l'appareil de terrain via HART ou traduisent le signal 4 … 20 mA en valeur numérique, avant de transmettre les données au réseau WirelessHART. Ces solutions ultra flexibles transforment n'importe quel appareil de terrain en appareil de terrain WirelessHART.



Convertisseur de température :

Le convertisseur de température WirelessHART est un appareil de terrain déjà équipé d'une interface WirelessHART. Pour cet appareil, on peut dire que l'interface 4 … 20 mA est remplacée par une antenne.

Sécurité des réseaux de communication industriels sans fil :

Les réseaux de communication sans fil s'immiscent de plus en plus dans les applications d'automatisation industrielle. Nous les rencontrons pour faire communiquer des terminaux entre eux, pour communiquer avec des capteurs ou avec des machines, pour enregistrer des données saisies par des opérateurs mobiles, ou encore pour qu'un automaticien connecte sa console de programmation à un équipement de contrôle.

Les principaux avantages sont une architecture souple avec peu de câbles, bien adaptée pour communiquer avec des équipements mobiles et des utilisateurs mobiles (les opérateurs de maintenance par exemple), ou pour installer des ateliers automatisés flexibles.

Quelques uns des désavantages relatifs aux technologies de communication sans fils sont leur haute sensibilité aux interactions avec l'environnement (les réflexions des ondes électromagnétiques dans un contexte industriel sont susceptibles de perturber fortement les transmissions hertziennes par exemple, voire de les bloquer carrément).

Sans barrière physique entourant les transmissions sans fil d'un réseau d'usine sans fil; il devient absolument nécessaire d'avoir une stratégie de défense en profondeur sans fil pour protéger le réseau contre les accès non autorisés.