

## Systemes de supervision-SCADA-

[Sige.ensam@gmail.com](mailto:Sige.ensam@gmail.com)

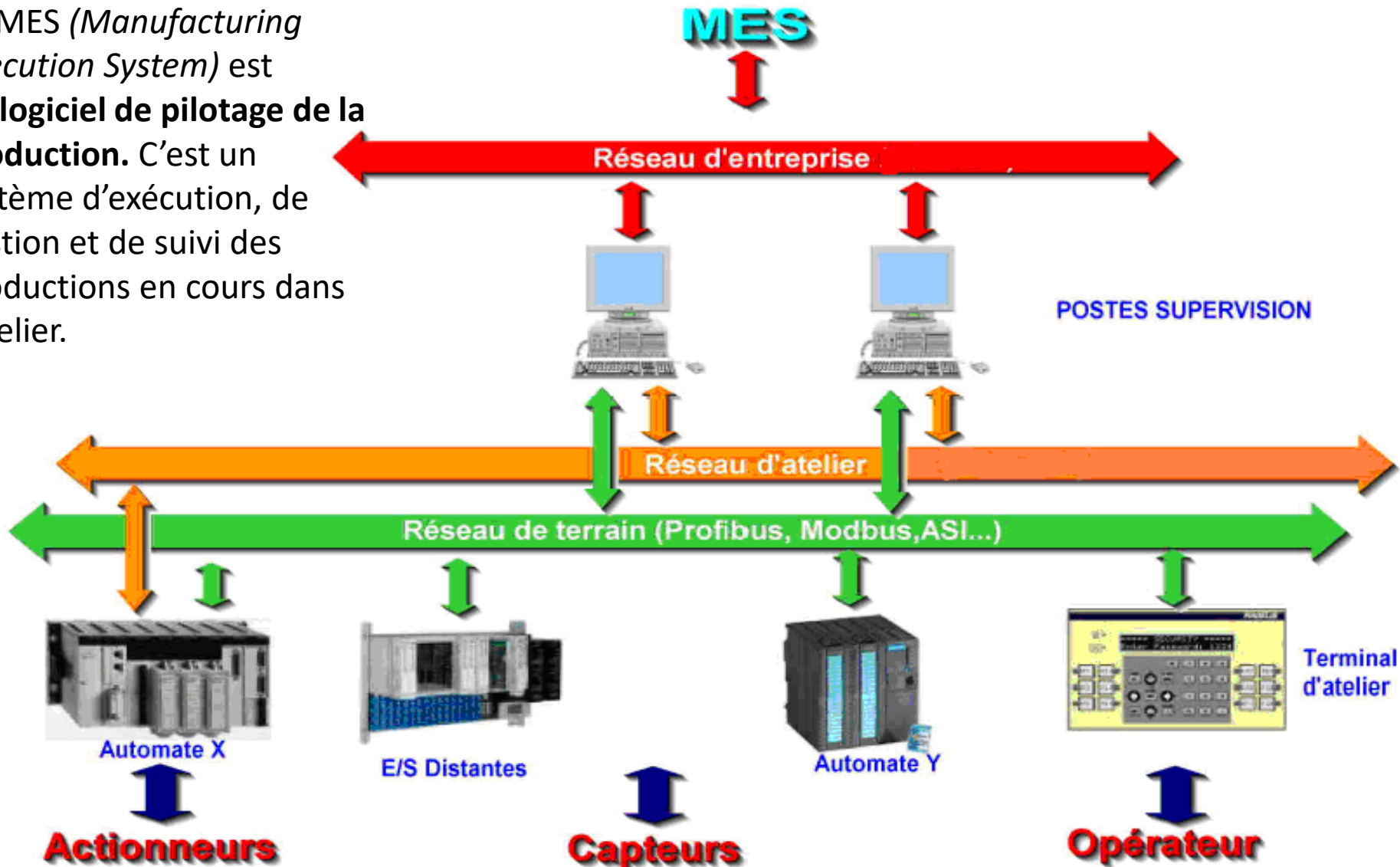
- **Chapitre 1:**
  - 1) Introduction
  - 2) Supervision Industrielle / Principe de Base
  - 3) Logiciels de Supervision / Critères de choix.
- **Chapitre 2: Systèmes industriels communicants**
  - 1) Introduction aux réseaux locaux industriels
    - 11) Définitions et intérêts de mise en réseau
    - 12) Transmission parallèle vs série
    - 13) Transmission asynchrone vs synchrone
    - 14) Réseaux de communication industriels
  - 2) Bus de terrain
    - 21) Bus CAN (Control Area Network)
    - 22) Interface série RS485 MODBUS
    - 23) ProfiBus (Process FieldBus)
- **Chapitre 3: Quelques exemples de supervisions (Node Red...)**

# 1) Introduction aux Systèmes SCADA

- Un système de contrôle et d'acquisition de données en temps réel (**SCADA**) (anglais : Supervisory Control And Data Acquisition, sigle : **SCADA**) est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémessures et de contrôler à distance des installations techniques.
- Les logiciels de supervision sont une classe de programmes applicatifs dédiés au **contrôle de processus** et à la **collecte d'informations en temps réel** depuis des sites distants, en vue de maîtriser un équipement.

# 1) Introduction aux Systèmes SCADA

Le MES (*Manufacturing Execution System*) est un **logiciel de pilotage de la production**. C'est un système d'exécution, de gestion et de suivi des productions en cours dans l'atelier.



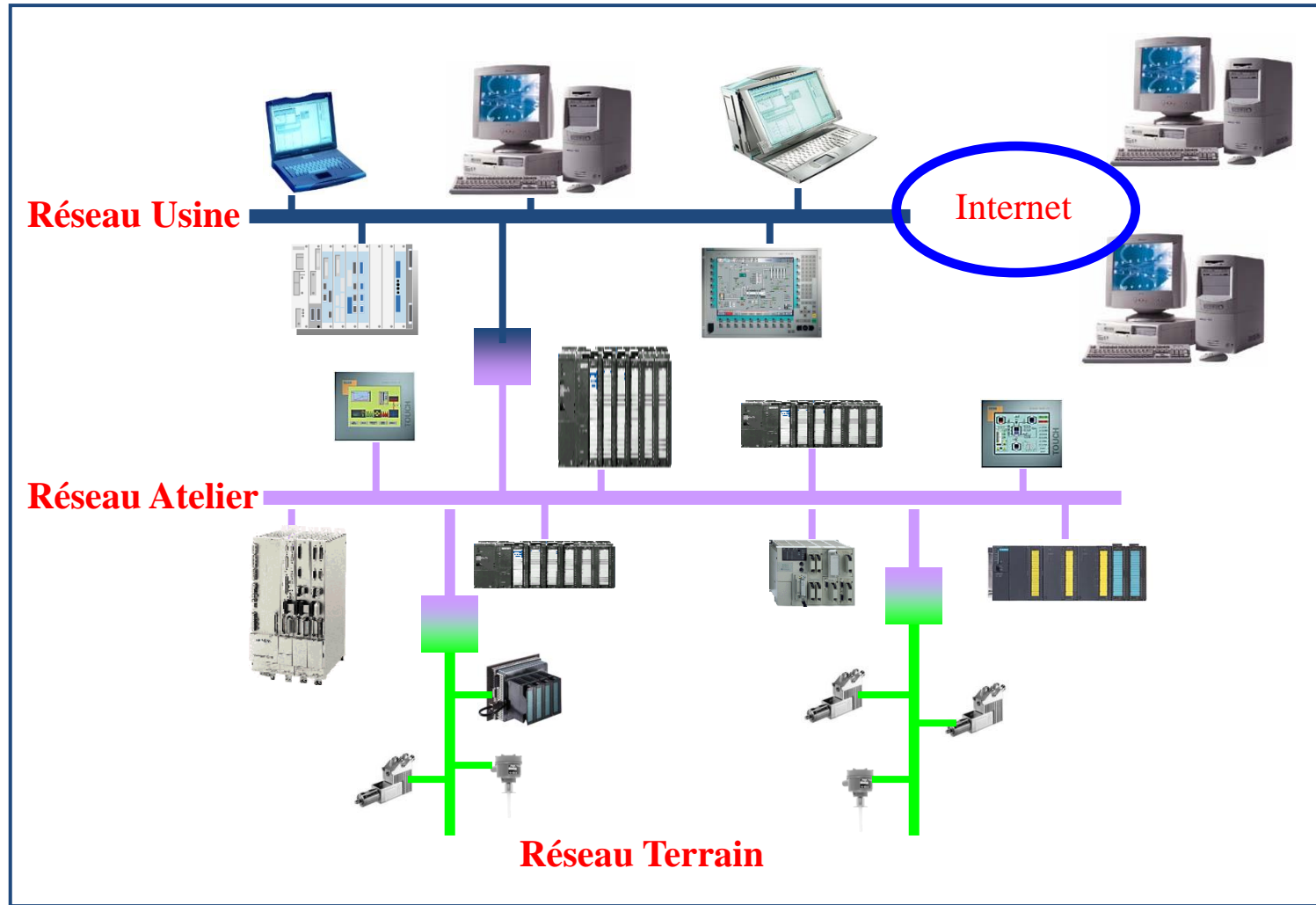
# 1) Introduction aux Systèmes SCADA

Un système SCADA inclut des composants hardware et software:

- Les éléments **hardware** assurent la **collecte** des informations qui sont à disposition du calculateur sur lequel est implanté le logiciel de supervision.
- Le calculateur traite ces données et en donne une **représentation graphique** réactualisée périodiquement.
- Le système SCADA **enregistre** les **événements** dans des fichiers ou les envoie sur une imprimante, par mail...
- Le système **surveille** les conditions de fonctionnement anormal et génère des **alarmes**.

# Introduction : « Évolution des systèmes de contrôle commande »

Le contrôle commande d'aujourd'hui est conçu sous le modèle CIM



**CIM** signifie « modèle de données unifié » (**Common Information Model**). C'est un standard ouvert

# Supervision Industrielle

*1- Définition*

*2- Principe de Base*

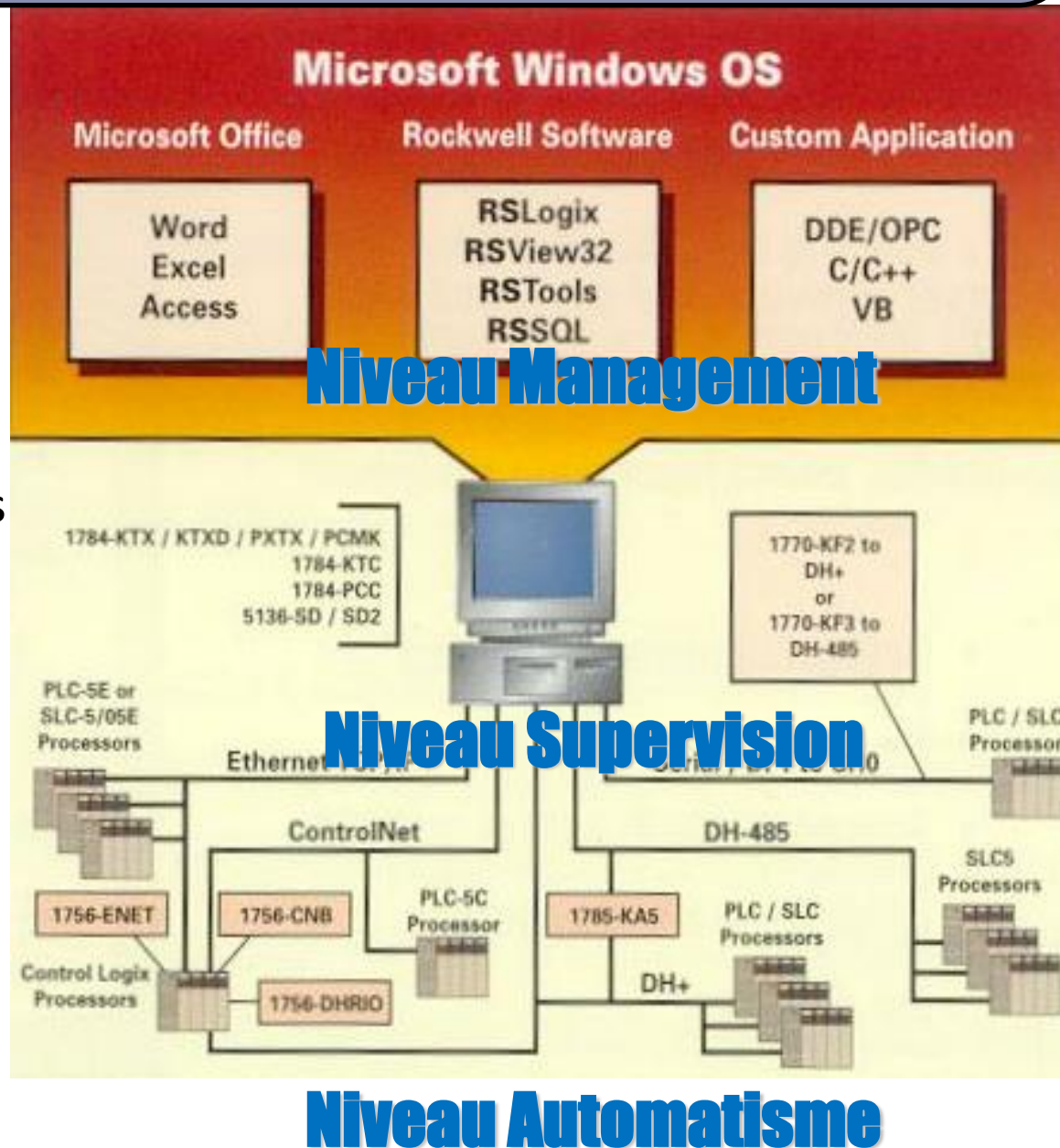
*3- Fonctions de Base*

# Supervision industrielle : Définition

- La supervision est un système informatique interactif qui se situe entre les automatismes d'atelier et la gestion de la production.

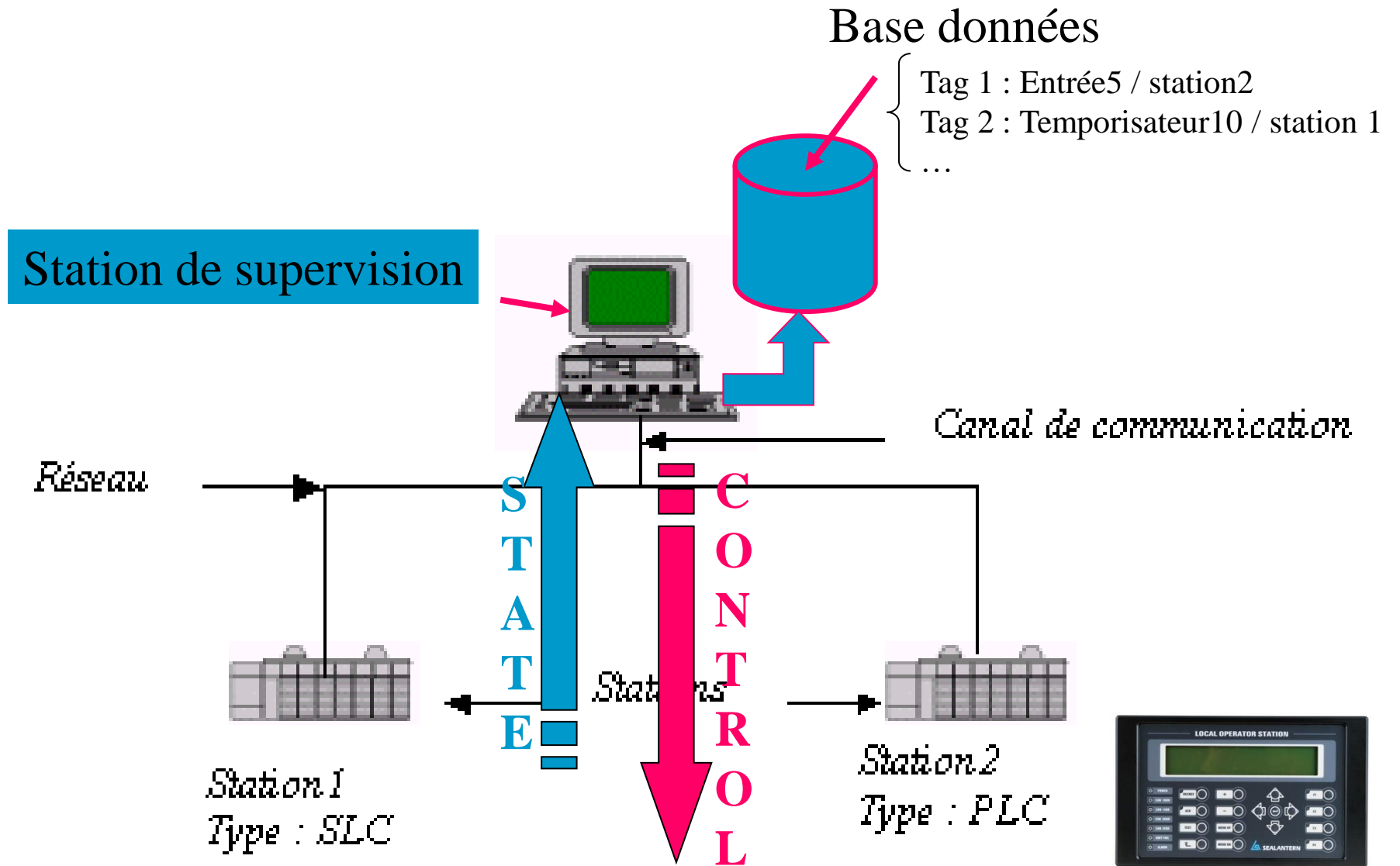
gestion de la production

automatismes d'atelier





# Supervision industrielle : Principe de base



Un SLC, ou circuit de ligne de signalisation

Local Operator Station (PLC)

## 1- Station de Supervision :

- PC bureau
- PC Industriel
- Serveur
- Station

## 2- Réseau :

- Protocole Ouvert ou Propriétaire

## 3- Station :

- API
- DCS ...

## 4- Base de données :

Constituée de variables(tag) dont les propriétés:

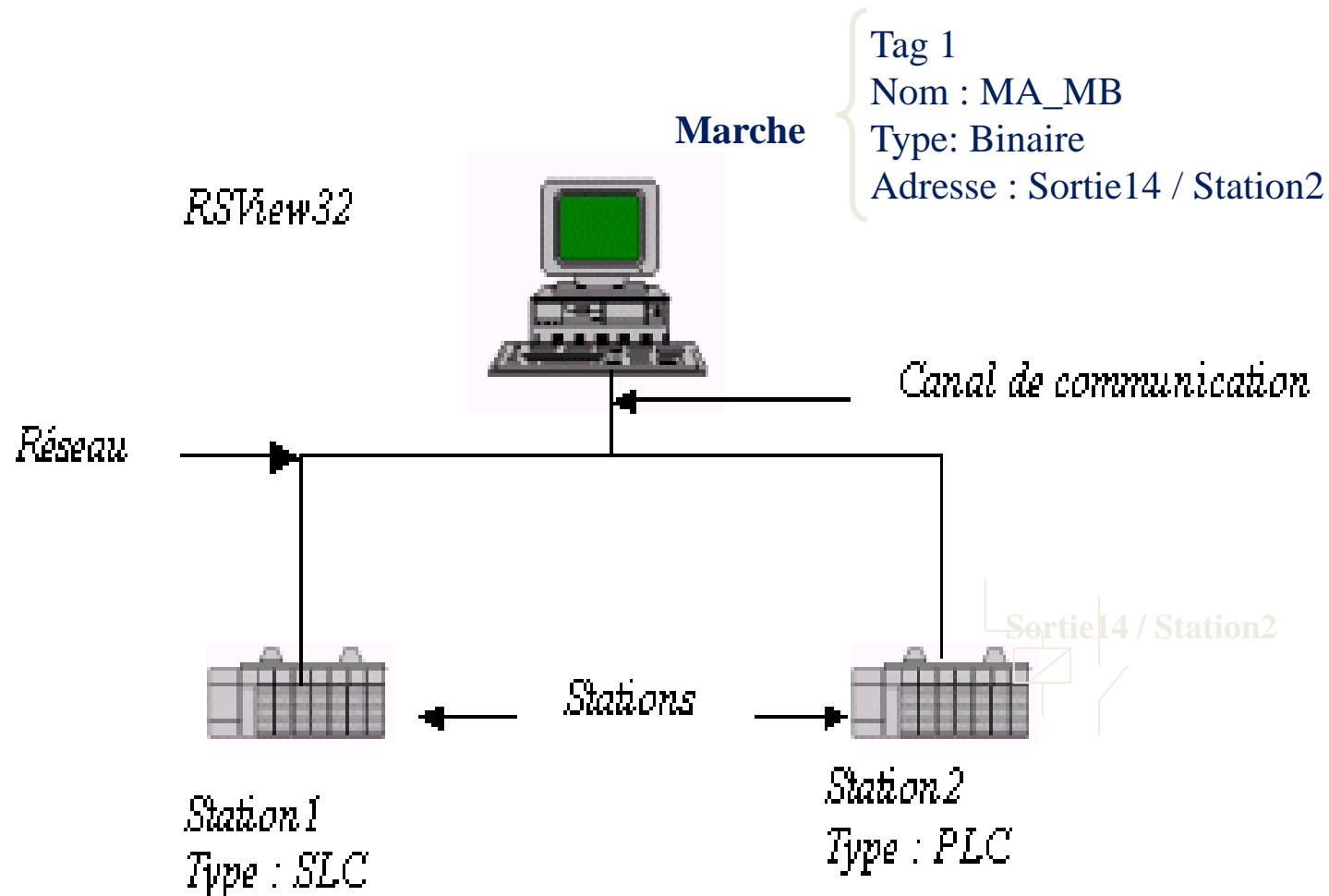
- Nom, Type(binaire, ana,...), adresse(adr. API & adr. Variable – E/S,Interne-...)

**IMPORTANT** : une fois configurée, l'accès à la base de données est transparent pour l'utilisateur

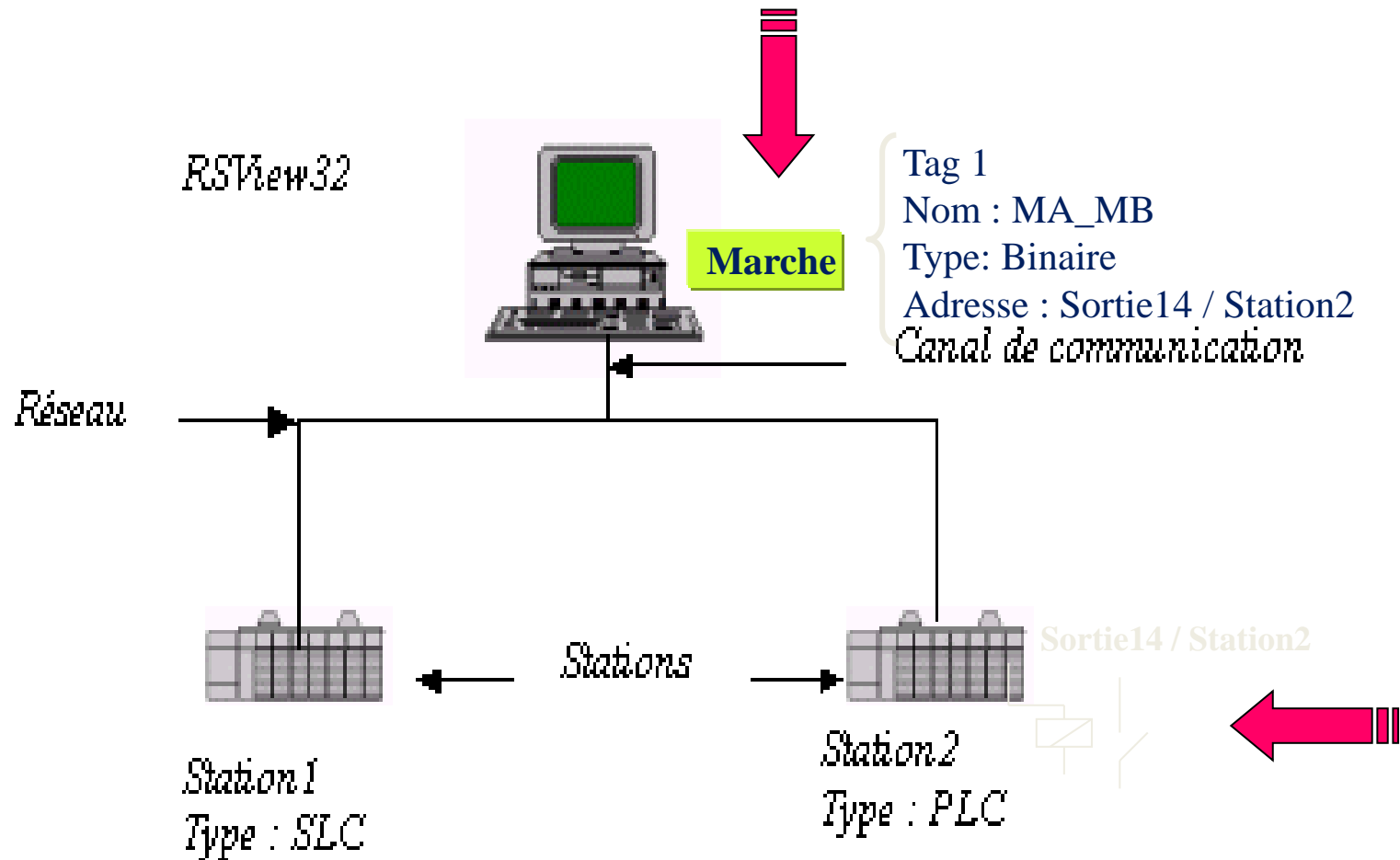
# Supervision industrielle : Fonctions de base

Deux Fonctions de BASE :

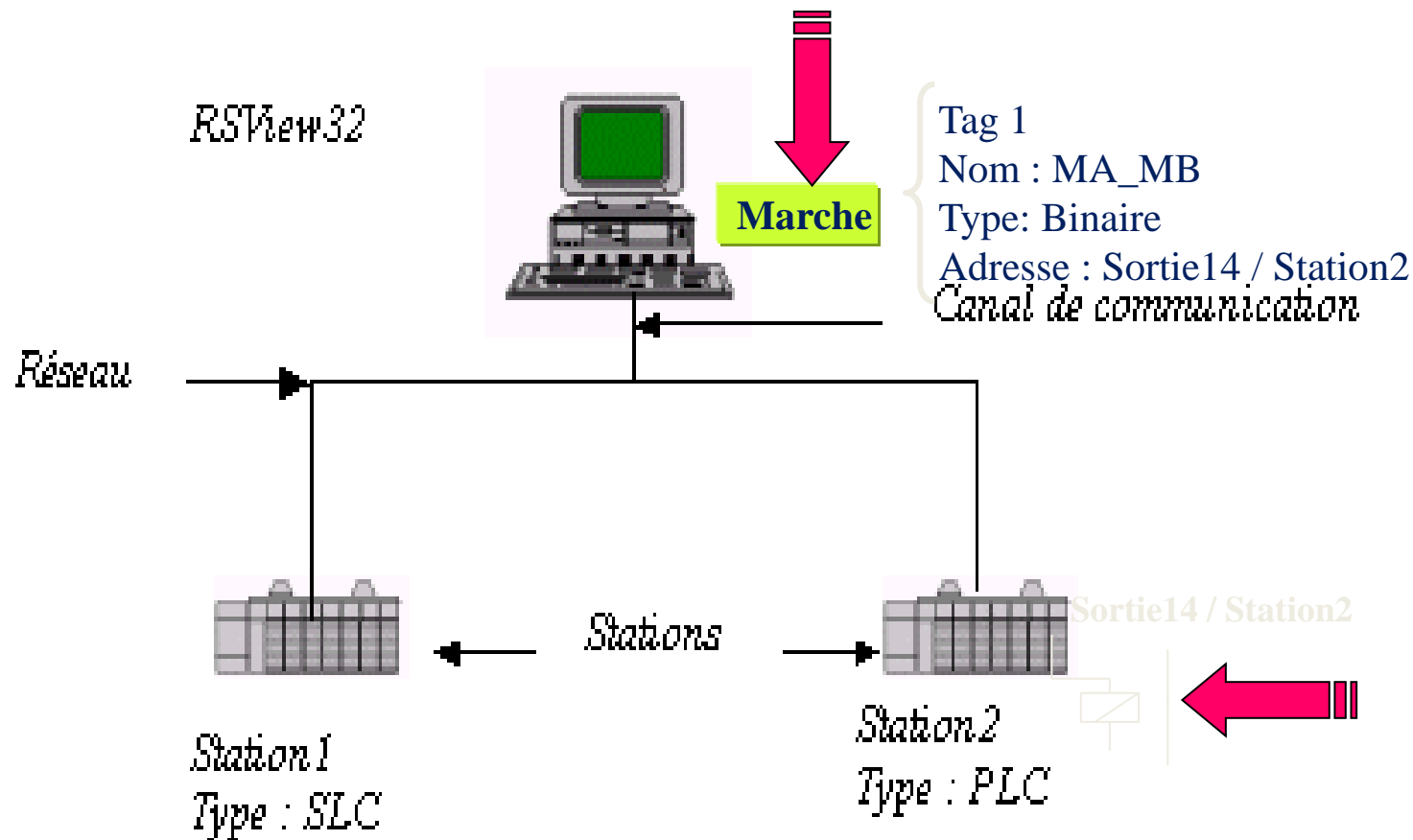
1- Commande : lancer toutes les commandes possibles (set,reset, augmenter) à partir de la station de supervision



## 1- Commande



## 1- Commande

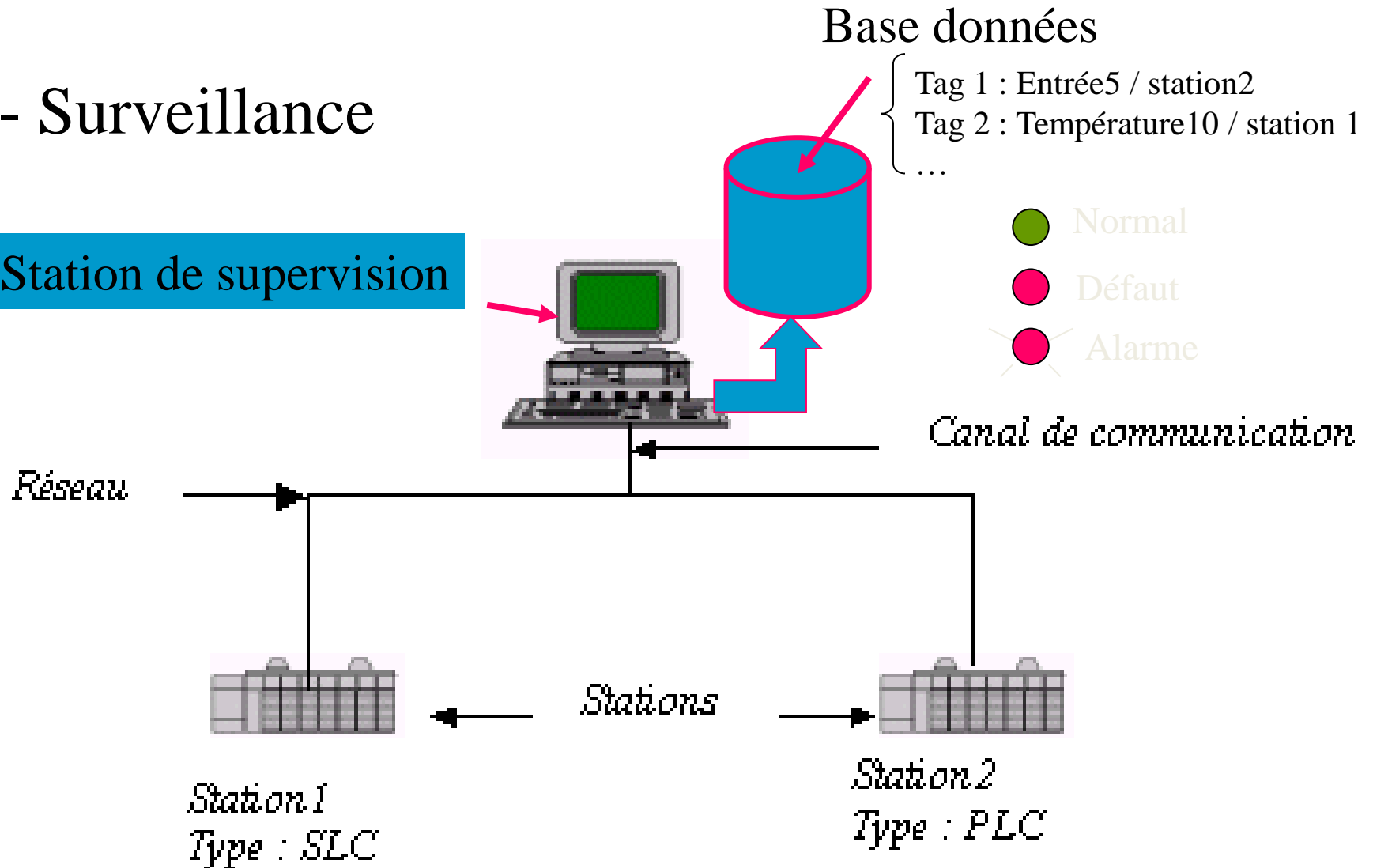


## 2- Surveillance

- Faire le suivi des états de toutes les Tags (variables) déclarées dans la base de données
  - Etat normal
  - Etat défaut
  - Etat alarme

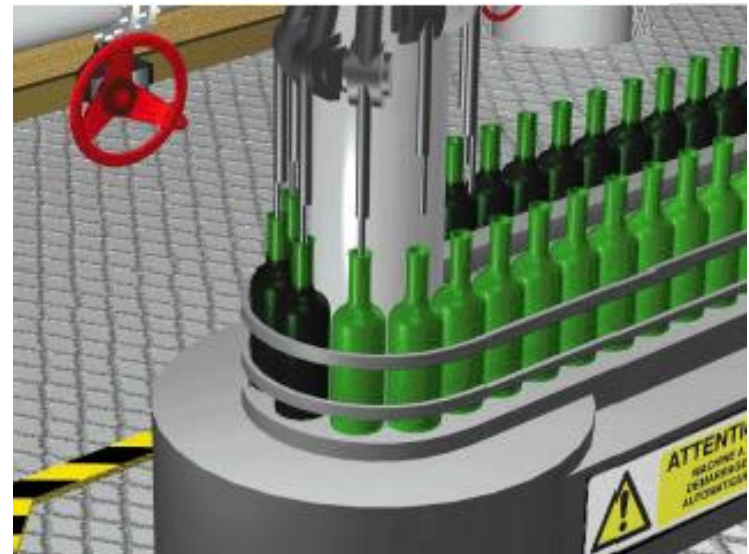
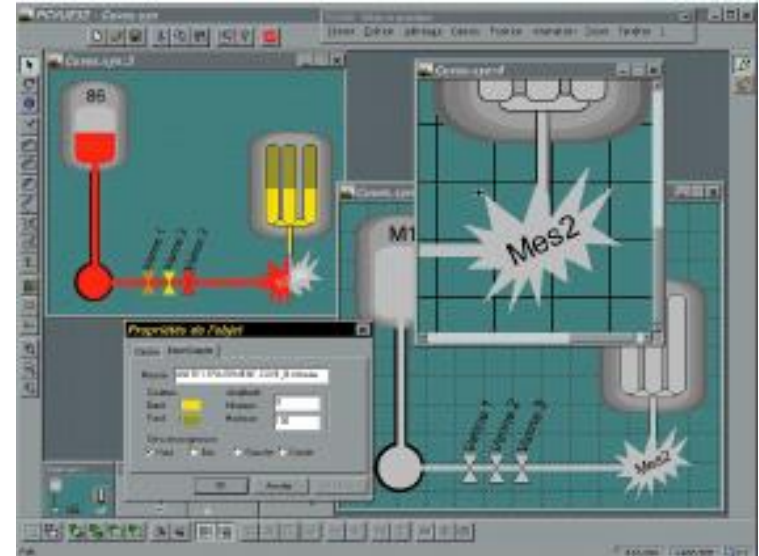
## 2- Surveillance

Station de supervision



# Supervision industrielle : Fonctions de base

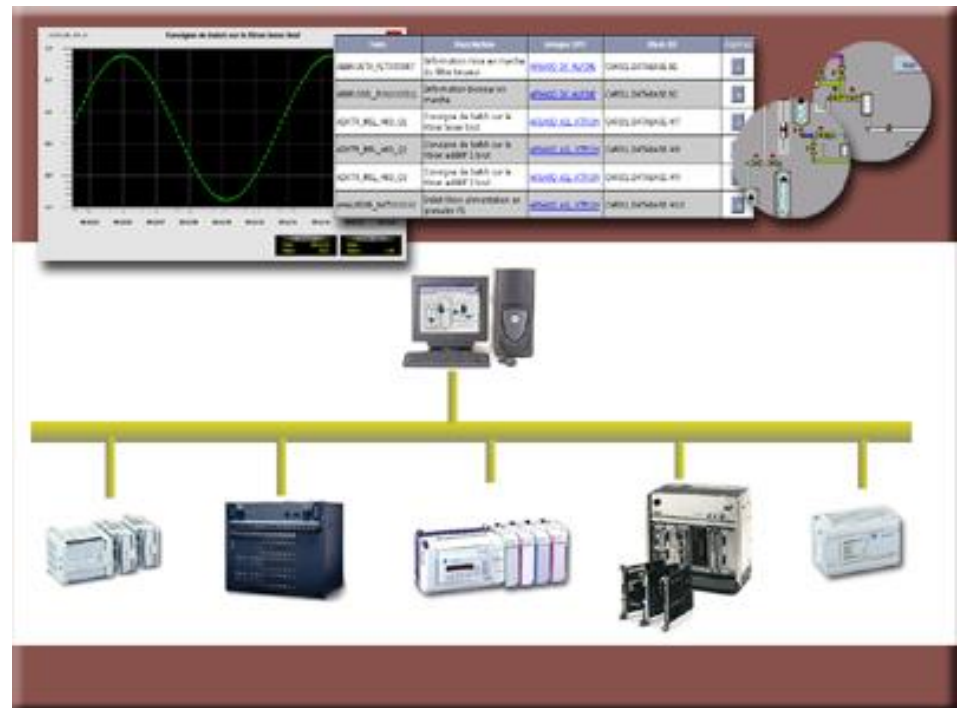
- L'acquisition de données
  - Communiquer avec des équipements différents
  - Communiquer sur des protocoles hétérogènes
- L'interface homme/machine
  - Représenter graphiquement le process et animer en temps réel
  - Communiquer de nouvelles consignes aux équipements





## La Gestion Des Alarmes, Les Courbes De Tendence

- Alarmes
  - Horodatage des événements (déclenchement de l'alarme, acquittement...)
  - Gestion des droits utilisateurs
- Tendances
  - Évolution des indicateurs du process sous forme de courbes en temps réel



## L'archivage des événements du process

- Utilisation de bases de données du marché : SQL Server, Oracle, DB2,...
  - Utilisation de systèmes d'archivage propriétaires
- Favorise la traçabilité du process de fabrication

Tendance...chez les constructeurs

*Vers une intégration plus rapide,*  
interaction forte entre le logiciel et les équipements

- Partage de la base de données temps réel entre le logiciel de supervision et la plate-forme d'automates
- Transfert de données de configuration aisé
- Industrie 4.0

Tendance...chez les éditeurs

### *La solution globale,*

Regroupement de plusieurs logiciels complémentaires

En une offre commerciale, la « suite » comprenant :

- Le logiciel de supervision
- Le logiciel API (Soft Logic)
- La gestion de production

# Les logiciels de Supervision

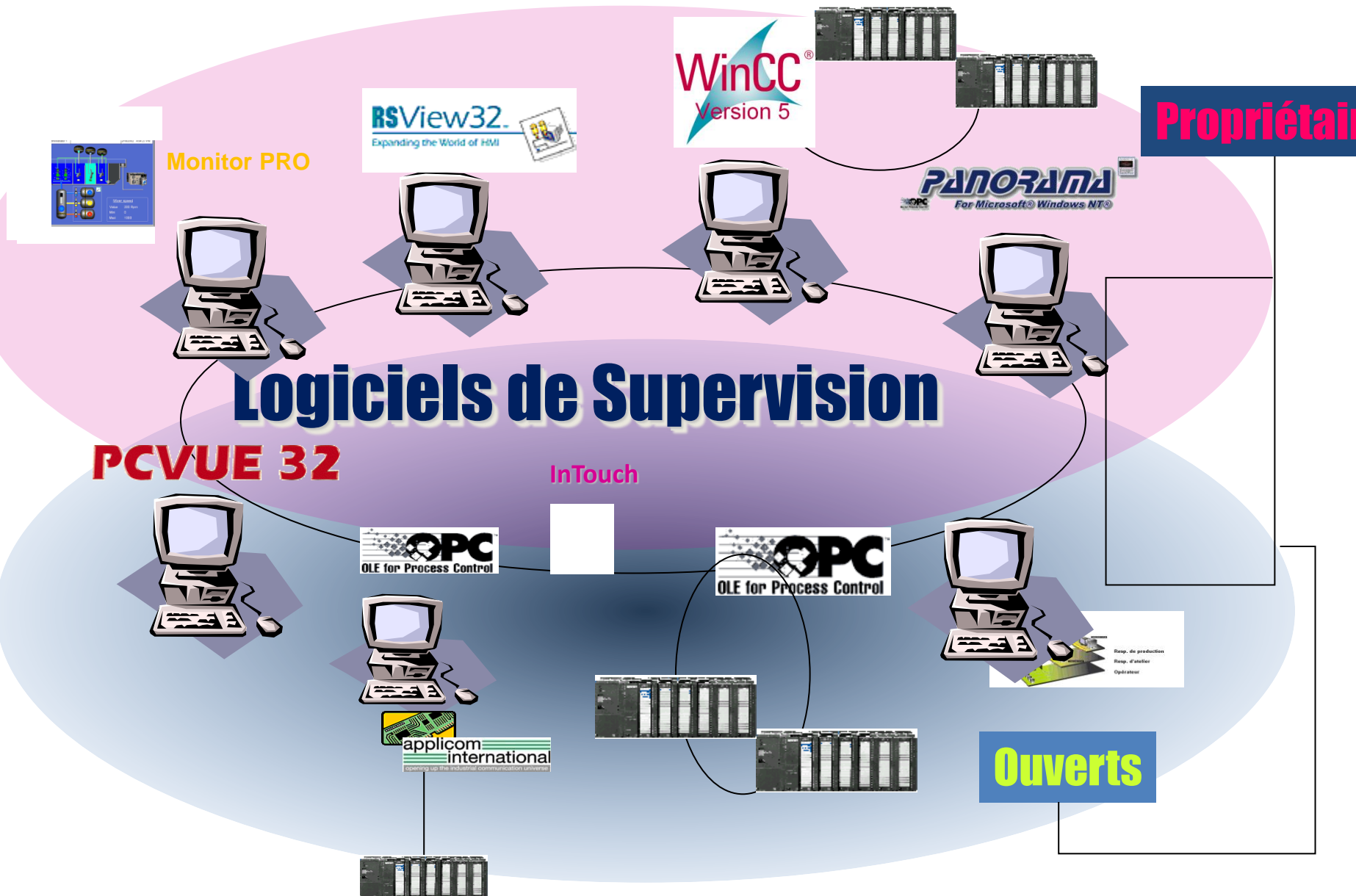
1- Vue Panoramique

2- Editeurs & Constructeurs

3- Critères de Choix

4- Exemple

# Les logiciels de Supervision : **Vue Panoramique**



## 2-Les constructeurs d'automates

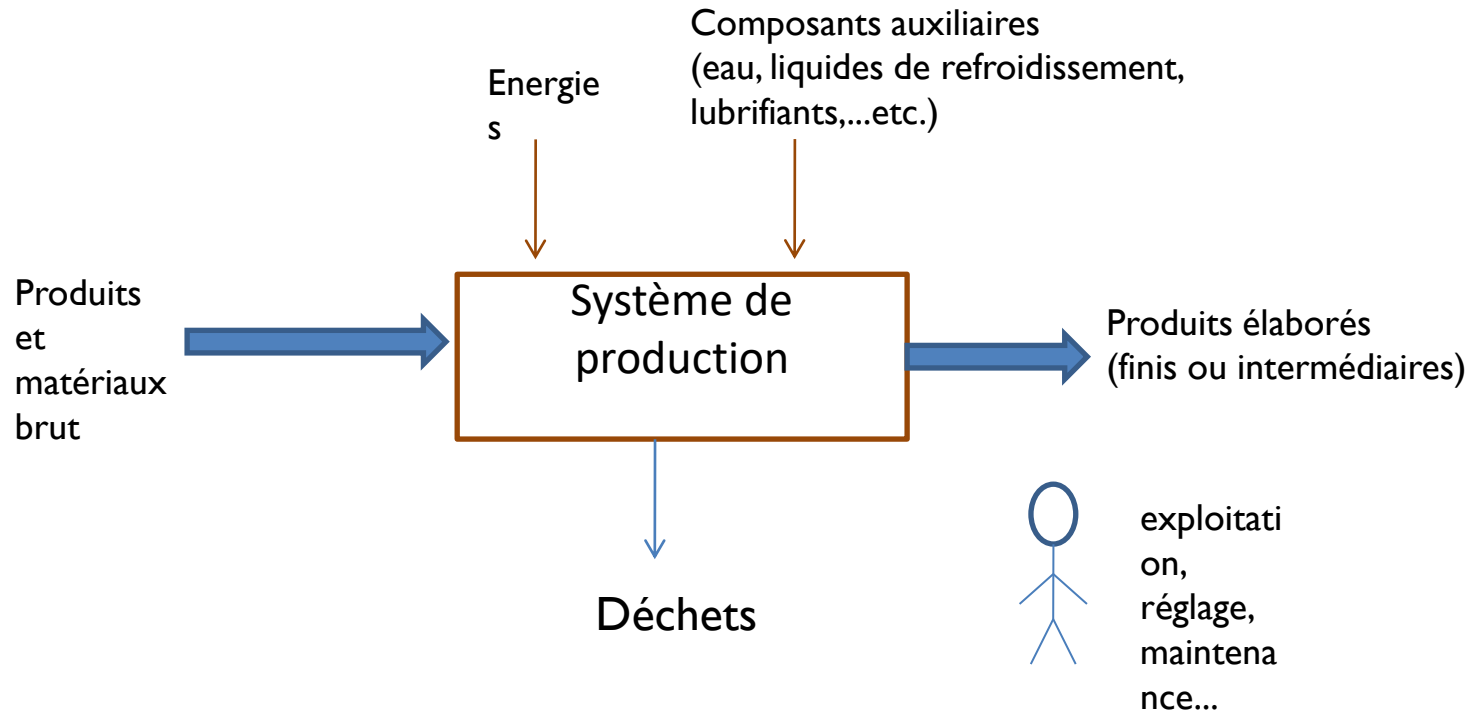
Logiciel	Constructeur
WinCC	Siemens
RS View	Rockwell Software
Cimplicity	GE Fanuc
Monitor-PRO	Schnieder

- Rappels sur les Systèmes Automatisés de production
- Introduction aux réseaux locaux industrie
- Bus de terrain



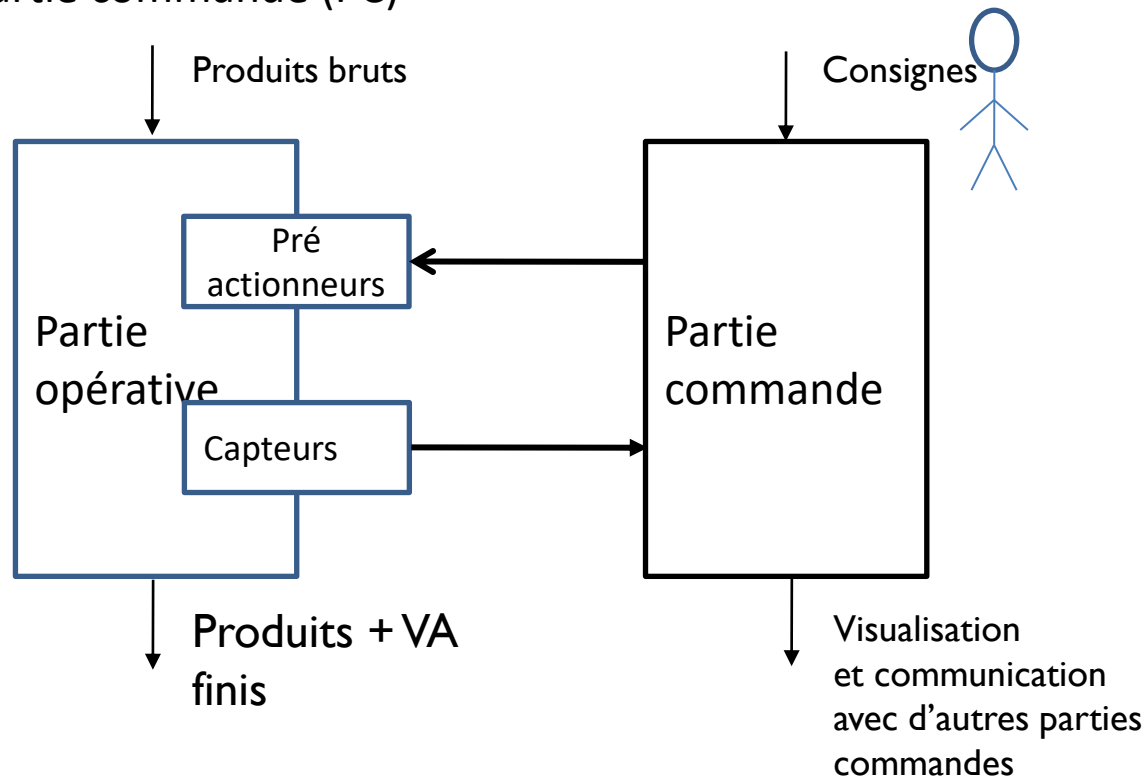
# Les systèmes automatisés de production

- Un système est dit automatisé s'il exécute toujours le même cycle de travail pour lequel il a été programmé.



### Structure d'un SAP

- SAP comporte deux parties :
  - Partie opérative (PO)
  - Partie commande (PC)



### Systèmes industriels communicants

#### Définitions et intérêts de mise en réseau

- Bus : au sens informatique industrielle, conducteur ou ensemble de conducteurs communs à plusieurs circuits permettant l'échange de données entre eux.
- Terrain : indique quelque chose de limité ou délimité géographiquement (usine, atelier, voiture...).

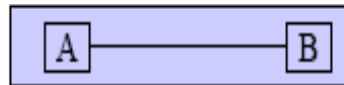
### Définitions et intérêts de mise en réseau

#### Intérêts :

- Réduction des couts initiaux
- Réduction massive du câblage : 1 seul câble en général pour tous les équipements au lieu d'un par équipement.
- Possibilité de réutiliser le câblage analogique existant dans certains cas.
- Réduction du temps d'installation.
- Réduction du matériel nécessaire à l'installation.
- Réduction des couts de maintenance
- Complexité moindre donc moins de maintenance (fiabilité accrue)
- Maintenance plus aisée : temps de dépannage réduit, localisation des pannes possibles grâce à des diagnostics en ligne («on line») donc à distance.
- Outils de test dédiés (analyseur...)
- Flexibilité pour l'extension du bus de terrain et pour les nouveaux raccordements.

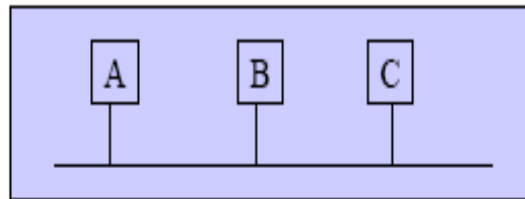
### Définitions et intérêts de mise en réseau

- Point-à-point



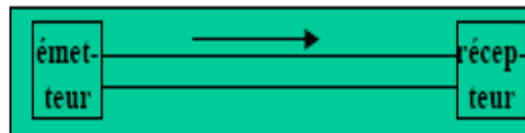
Liaison physique entre 2 points du réseau

- multi-points  
(multidrops)



Liaison physique partagée  
par plus de 2 noeuds

- 
- simplex



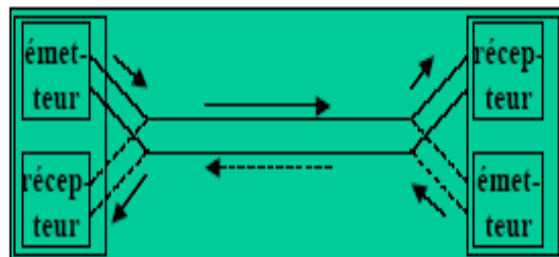
Echange à sens unique  
sur canal binaire

- full duplex



Echange dans les 2 sens  
simultanément (2 lignes binaires  
ou 2 canaux à fréq. différentes  
sur ligne unique)

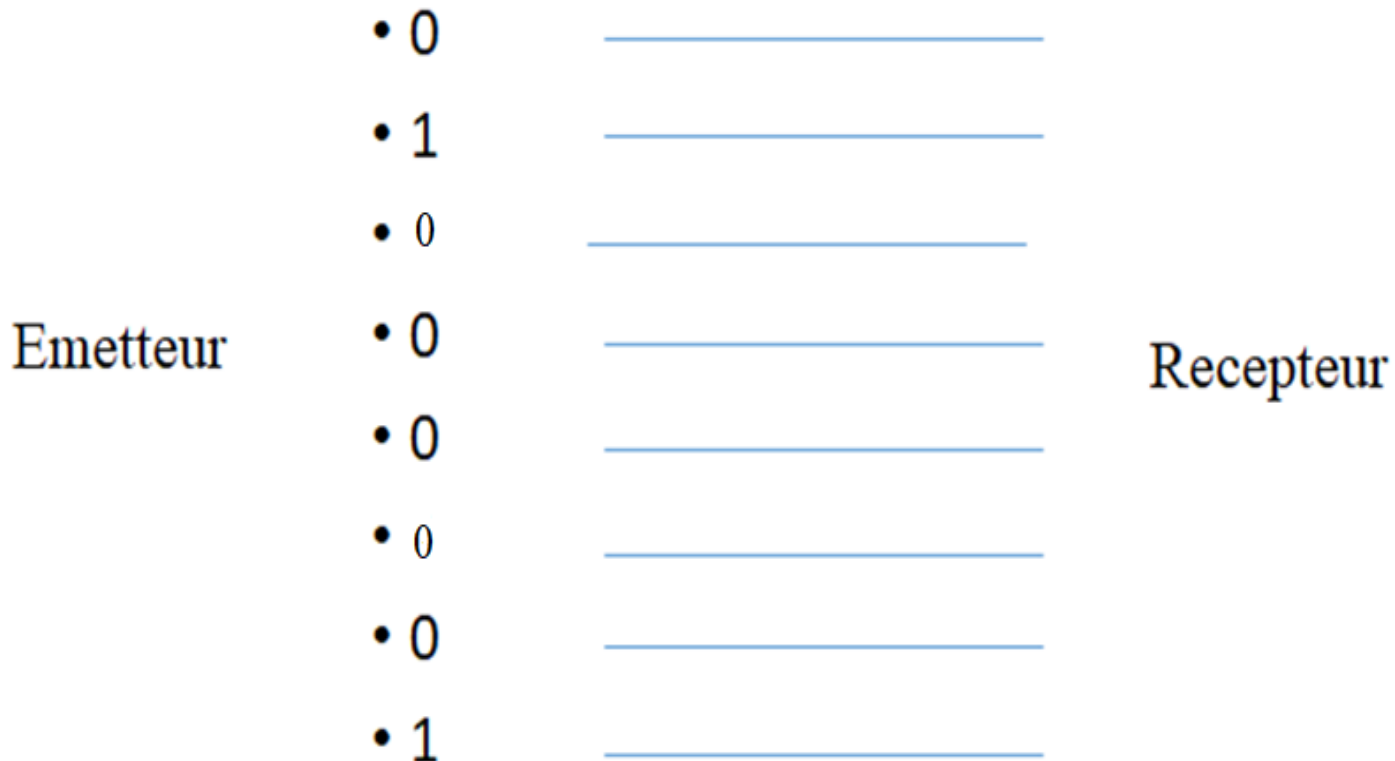
- half duplex



Echange dans les 2 sens  
alternativement  
sur le même canal

### Transmission parallèle vs série

- Exemple de transmission parallèle: soit à transmettre le caractère A en mode parallèle:  $ASC(A) = (65)_{10} = (41)_{16} = (01000001)_2$



### Transmission parallèle vs série

- Exemple de transmission série: soit à transmettre le caractère A en mode série:



- Avantages: Economie de fils et d'énergie d'où l'utilisation de la transmission série.
- Exemple: USB, SATA, RJ45.....
- La transmission parallèle commence à disparaître (DB25)

### Transmission synchrone et transmission asynchrone

#### Transmission asynchrone

- Dans une transmission asynchrone, les caractères sont émis de façon *irrégulière*, l'intervalle de temps entre deux caractères est aléatoire, le début d'un caractère peut survenir à n'importe quel moment.
- Il faut indiquer au destinataire où commence et se termine un caractère particulier, La réponse est donnée par les *bits de départ et d'arrêt* souvent désignés par leur appellation anglo-saxonne de START (élément de départ) et de STOP (élément d'arrêt).
- Un octet transmis d'une façon asynchrone est illustré sur la page suivante :

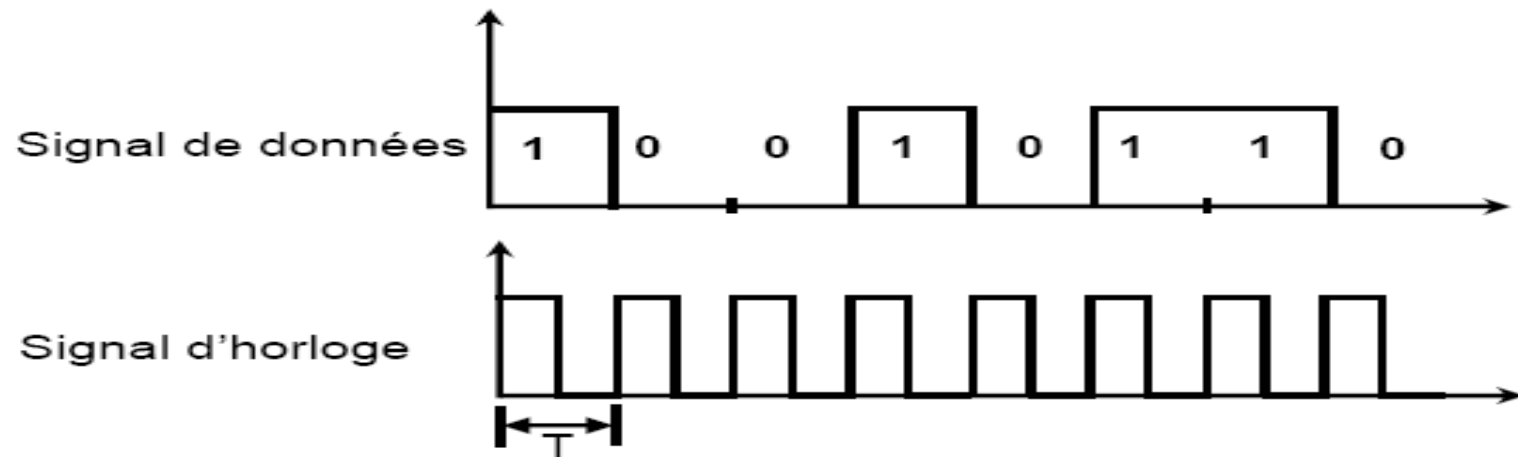
Remarque : Un bit de parité peut être utilisé pour détecter les erreurs susceptibles d'apparaître pendant la transmission.





### Transmission synchrone :

- Dans une transmission synchrone, les bits sont émis d'une façon *régulière*, sans séparation entre les caractères, pour cela un signal d'horloge périodique de période  $T$  fonctionne pendant toute la durée de l'émission.



### Les réseaux de communication industriels

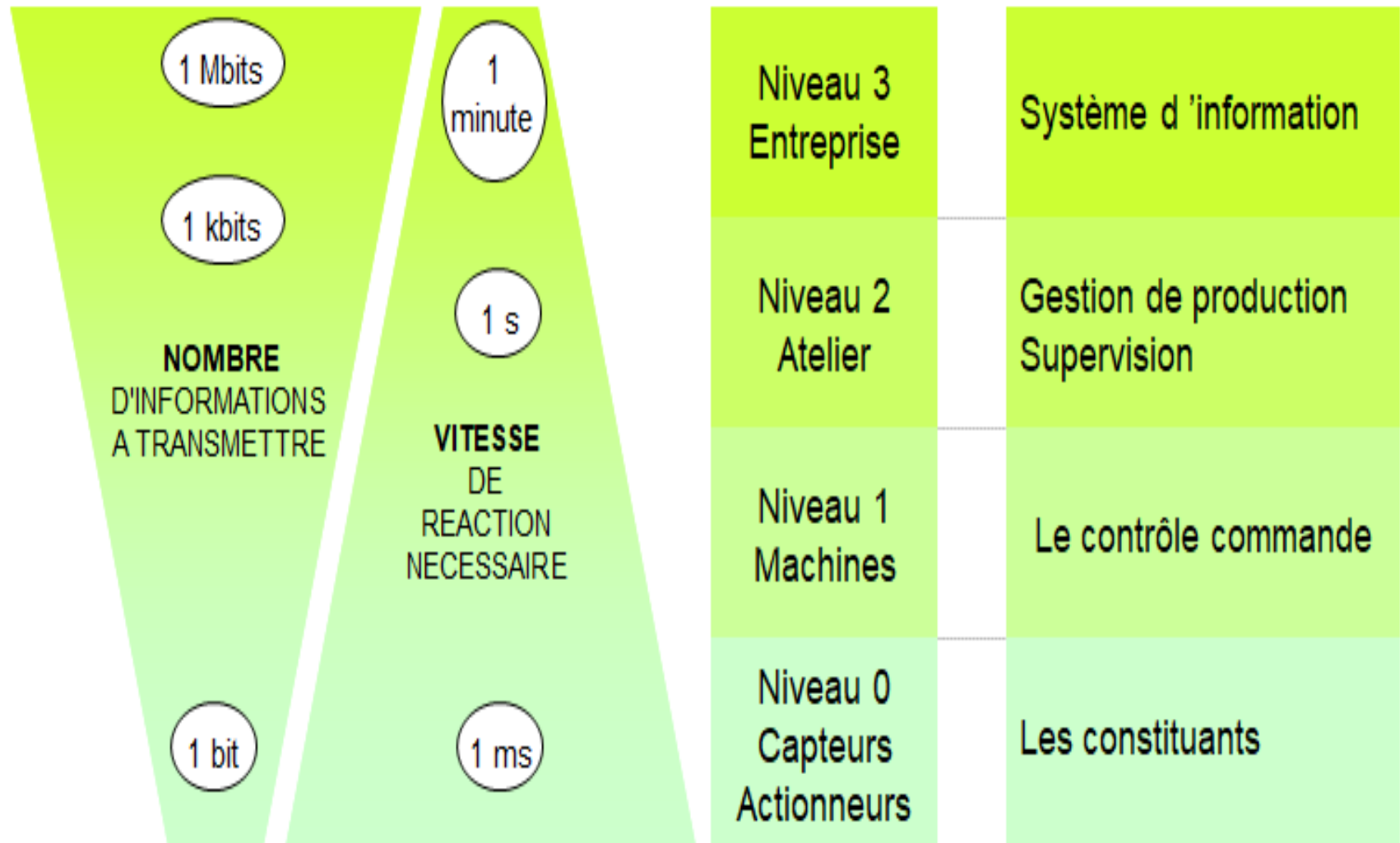
- Pour des raisons liées au coût et à la robustesse, la plupart des réseaux de communication industriels utilisent :
- **une transmission numérique série asynchrone half-duplex.**

#### ■ Connectivity Networks

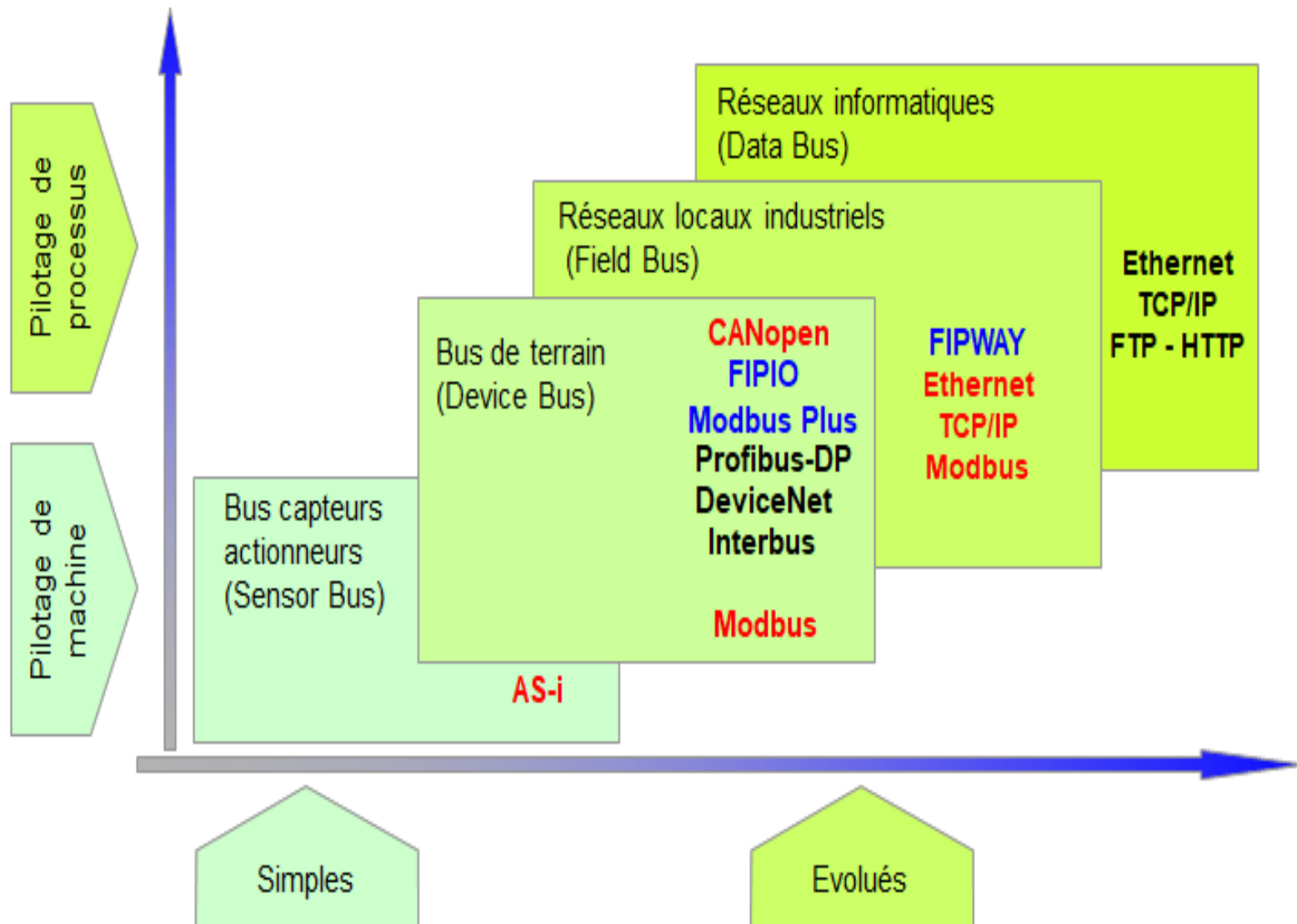
Approche pragmatique quand le marché impose sa solution

**DeviceNet** (Allen-Bradley) - **Profibus** (Siemens) - **Interbus** (Phoenix) ...

### Les besoins en communication industrielle

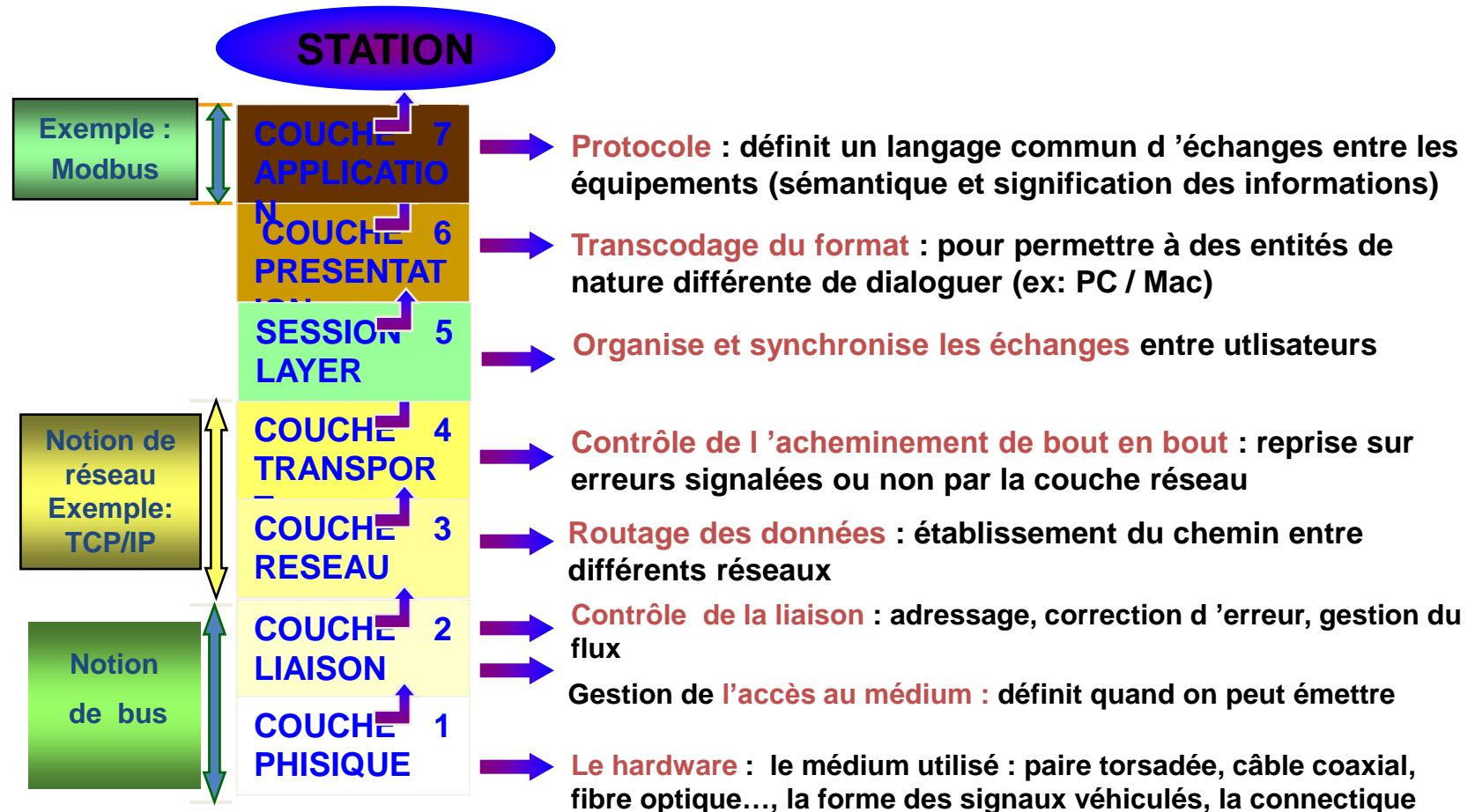


### Positionnement des principaux réseaux et bus



## Chapitre 2: Systèmes communicants : Description du modèle OSI

Le modèle OSI (Open Systems Interconnection) est un modèle de référence en ce qui concerne les réseaux, il est proposé par l'ISO (International Standards Organisation), il décrit les concepts et les démarches à suivre pour interconnecter des systèmes, il est composé de 7 couches :



TCP : Transmission Control Protocol  
(Couche 4)

IP : Internet Protocol (Couche 3)

# Chapitre 2: Systèmes communicants : Description du modèle OSI

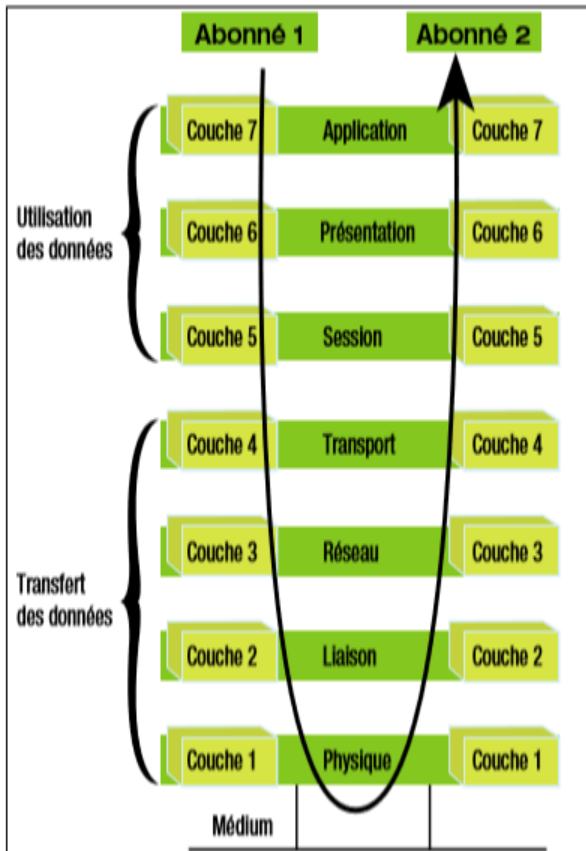


Figure . Le modèle OSI.

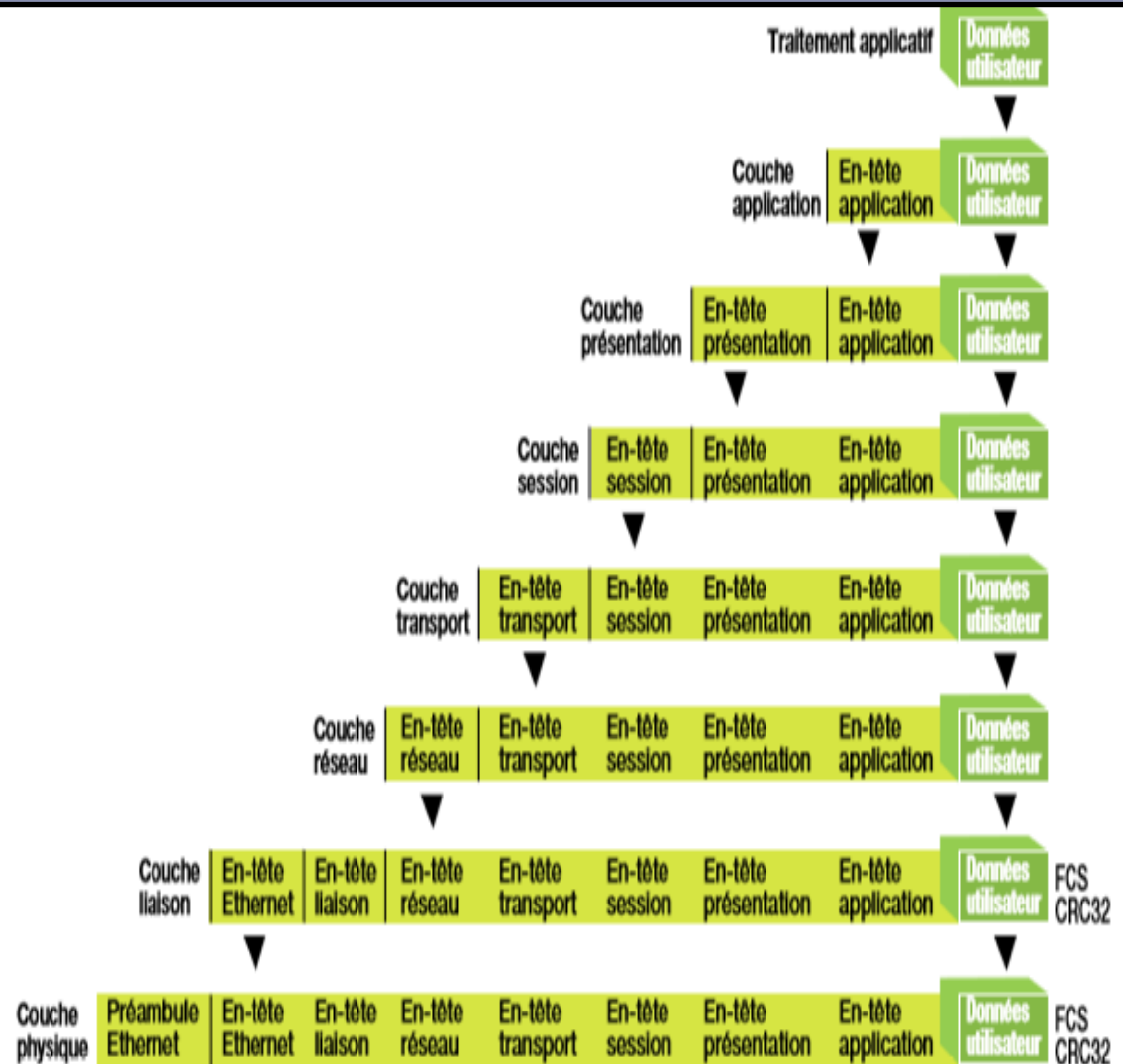


Figure . Mécanisme d'encapsulation.

### Les principaux supports utilisés



Les supports de transmission ou **MEDIUMS** influent sur :

- vitesse
- distance
- immunité électro-magnétique

Mediums les plus utilisés :

#### La paire de fils torsadés

Le plus **simple** à mettre en œuvre, et le **moins cher**.

#### Le câble coaxial

Il se compose d'un conducteur en cuivre, entouré d'un écran mis à la terre. Entre les deux, une couche isolante de matériau plastique. Le câble coaxial a **d'excellentes propriétés électriques** et se prête aux transmissions à **grande vitesse**.

#### La fibre optique

Ce n'est plus un câble en cuivre qui porte les signaux électriques mais une fibre optique qui transmet des signaux lumineux. Convient pour les **environnements industriels agressifs**, les transmissions sont sûres, et les **longues distances**.

Coût du  
médium

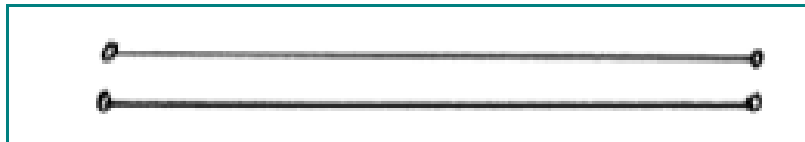
Faible



Important

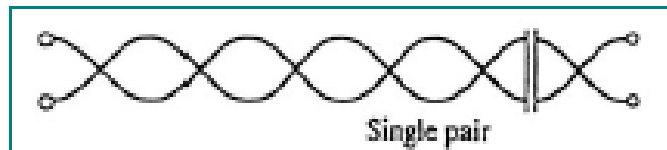
### Liaisons métalliques

Paires ouvertes : 2 fils isolés côte à côte (signal + commun)



- pour « multidrops »
- bon marché
- sensibles aux perturbations électromagnétiques
- Vitesses limitées

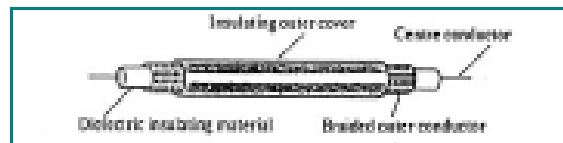
Paires torsadées (twisted pair)



Le plus courant !

- Signal par mesure différentielle
- peu sensible aux perturbations électromagnétiques (ressenties identiquement par les 2 fils)
- améliorable par blindage
- Vitesse.: 100 ... 1000 Mbits

Coaxes



- Transmission large bande (télédistribution)
- Très bonne immunité aux parasites
- Installation sur grandes longueurs
- améliorable par blindage
- Vitesse.: 100 Mbits max. pour 100 m (ex. Ethernet)



### Quelques standards paire torsadée

#### •RS232 :

Liaison point à point par connecteur SUB-D 25 broches.  
Distance < 15 mètres, débit < 20 kbits/sec.

#### •RS422A :

Bus multipoint **full duplex** (bi directionnel simultané) sur 4 fils.  
Bonne immunité aux parasites, distance maxi 1200 mètres à 100 kbits/sec.  
2 fils en émission, 2 fils en réception.

#### •RS485 :

Bus multipoint **half duplex** (bi directionnel alterné) sur 2 fils.  
Mêmes caractéristiques que RS422A mais sur 2 fils.

# LE BUS CAN

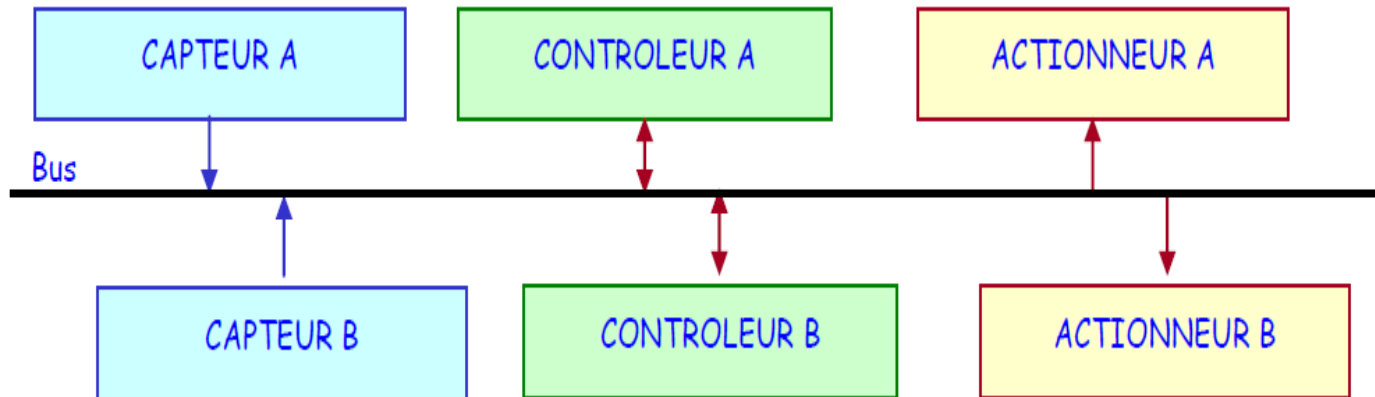
- **1- Présentation**
- Pour satisfaire les exigences de confort, de sécurité, de réduction de la pollution et de la consommation, de performances, ..., l'automobile se dote de systèmes électroniques de plus en plus nombreux : système de contrôle moteur, systèmes de navigation, systèmes d'anti-blocage, d'anti-patinage, de suspension active, d'anti-collisions, ... Et pilote automatique !

# LE BUS CAN

- Tous ces systèmes ont besoin pour fonctionner d'échanger des informations. Dès que leur nombre devient important, il n'est plus possible de les relier par des lignes indépendantes. En effet, avec cette solution, il faudrait 1 à 2,5 km de lignes pour un véhicule moderne, ce qui représente une masse comprise entre 30 et 50kg ! et en conséquence, de graves problèmes de coûts et de maintenance.

# LE BUS CAN

- L'industrie automobile a donc développé une architecture de communication à base de bus de terrain. Renault et Sagem ont développé le bus VAN (vehicle area network) et l'équipementier Bosch a développé le bus CAN (controller area network).





## 2- Historique du Bus CAN

- ☐ 1983 : début développement par l'entreprise BOSCH
- ☐ 1985 : spécification protocole "CAN 1.0"
- ☐ 1987 : premier échantillon de circuits intégrés CAN
- ☐ 1991 : spécifications protocole "CAN 2.0A et CAN2.0B" aux normes ISO 111898 . Première voiture équipée (Mercedes classe S)
- ☐ 1997 : Tous les grands fondeurs de silicium (Motorola , Philips , Intel) proposent des circuits CAN.
- ☐ 2000 : explosion des équipements reliés par le CAN

# 3- Les noeuds CAN

- Tout élément branché sur le bus CAN est appelé noeud. Chaque noeud peut émettre et recevoir des informations. Un message émis sur le bus est diffusé à l'ensemble des noeuds récepteurs. Des noeuds peuvent être branchés ou débranchés sans ajout, ni modifications du soft ou du hardware.

# 4- Le message CAN

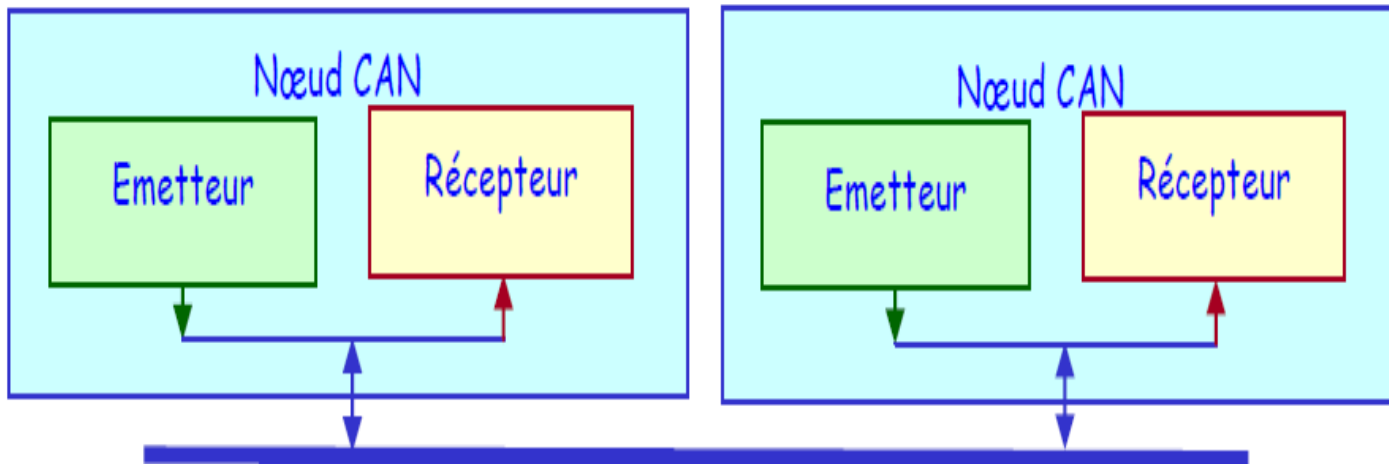
- ☐ Le message CAN est constitué de deux parties :
- ☐ **☐ L'identificateur (ID): définit le type du message.**
- ☐ **☐ Les données (DATA): représente la valeur du message.**
  
- ☐ Exemple :
- ☐ ID = Pression pneu avant gauche
- ☐ DATA= valeur de la pression
- ☐ Un noeud émetteur diffuse un message à l'ensemble des noeuds récepteurs. Les noeuds récepteurs n'utilisent ce message que s'il les intéresse. Ils possèdent pour cela un **filtre d'acceptance qui ne laisse passer que les messages dont les identificateurs sont acceptés.**



## 5- Règle de priorité

- Comme chaque noeud peut émettre simultanément sur le bus, il peut y avoir des conflits d'accès. Pour pallier à ce problème, il existe **une règle de priorité. Le message le plus prioritaire est celui qui possède l'identificateur le plus faible. Chaque noeud émetteur doit donc en même temps "écouter" le bus. Il est donc émetteur et récepteur.**

**Si un autre noeud envoie un message plus prioritaire, il doit se "taire".**

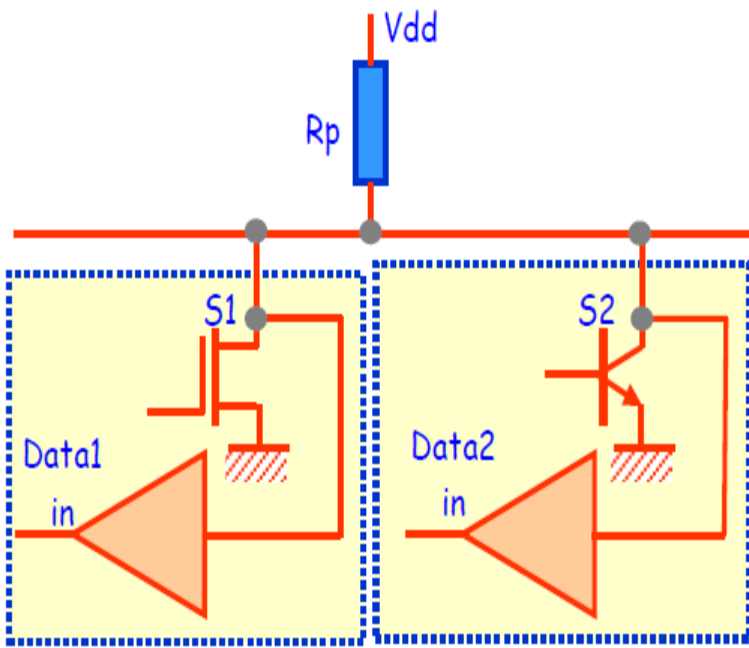


Exemple : Le message A d'identificateur 647(hexa) est plus prioritaire que le message B d'identificateur 663(hexa).

## 6- Gestion de la priorité des messages grâce à un arbitrage bit à bit.

- ☐ L'arbitrage entre les deux identificateurs est réalisé bit après bit lors de leur émission grâce à la notion de bit dominant et de bit récessif. Lorsque deux bits sont en concurrence, le bus CAN se comporte comme une fonction ET. En conséquence, le bit „0“ est le bit dominant.
- ☐ **Exemple de réalisation matérielle : médium filaire**
- ☐ La réalisation matérielle utilise des circuits émetteurs à collecteur ouvert.
- ☐ ☐ Transistor saturé : bit '0'
- ☐ ☐ Transistor bloqué : bit '1'

- Il suffit qu'un seul transistor soit saturé pour imposer un '0' sur le bus. Il faut que tous les transistors soient bloqués pour imposer un '1' sur le bus. On crée bien une fonction ET.

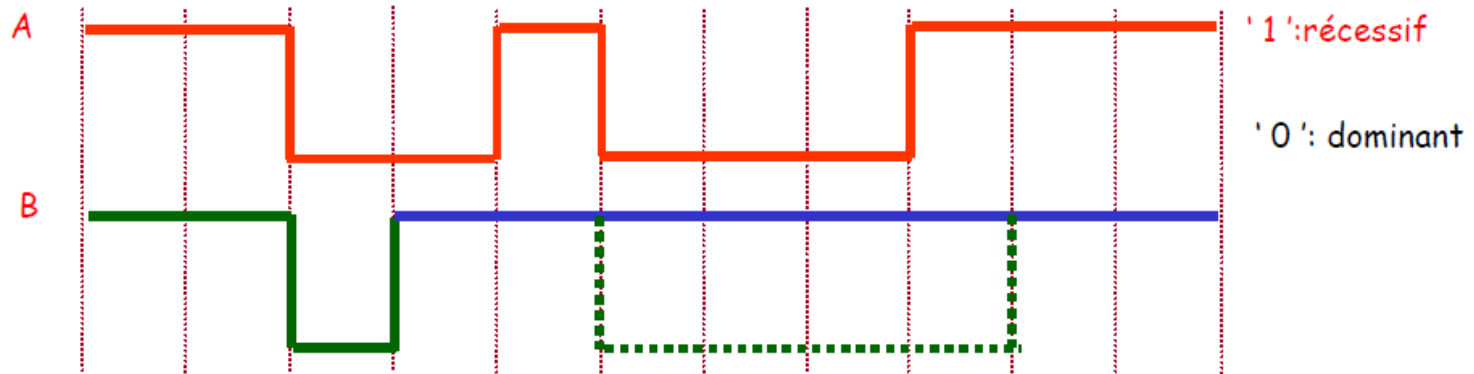


# Exemple d'arbitrage :

Reprenons l'exemple précédent et représentons la suite des éléments binaires qui codent les identificateurs des messages A et B.

Message A : ID = h647 = 11001000111

Message B : ID = h663 = 11011000011



Les identificateurs A et B ont les mêmes valeurs binaires pendant les 3 premiers coups d'horloge. On émet donc pour l'instant 110 sur le bus. Au 4eme coup d'horloge, l'émetteur A émet un bit dominant '0' et l'émetteur B émet un bit récessif '1'. L'identificateur A devient alors prioritaire sur l'identificateur B. L'émetteur B se "tait" et met sa ligne à '1' bit récessif pour ne pas gêner l'émission de l'émetteur A.

# 8- Débit et longueur du bus

- Pour que l'arbitrage de la priorité fonctionne correctement, il faut que le temps de propagation  $t_p$  d'un bit entre les noeuds soit négligeable devant la durée  $T_b$  du bit :  $t_p \ll T_b$ .
- Exemple : medium filaire
- $v = 200000 \text{ km/s}$  soit  $5 \text{ ns/m}$
- Débit =  $1 \text{ Mbits/s}$  d'où  $t_p = L \cdot 5 \text{ ns} \ll T_b = 1 \mu\text{s}$  soit  $L \ll 200 \text{ m}$
- Débit =  $100 \text{ kbits/s}$  d'où  $t_p = L \cdot 5 \text{ ns} \ll T_b = 10 \mu\text{s}$  soit  $L \ll 2000 \text{ m}$
- **Configurations recommandées :**

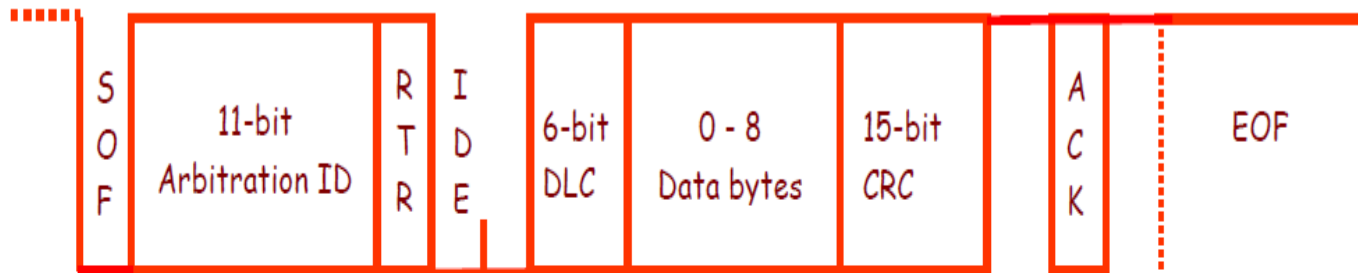
Débit	Longueur
1 Mbits/s	40 m
500 kbits/s	100 m
100 kbits/s	500 m
20 kbits/s	1000 m

La longueur du réseau CAN est d'autant plus faible que le débit est élevé.

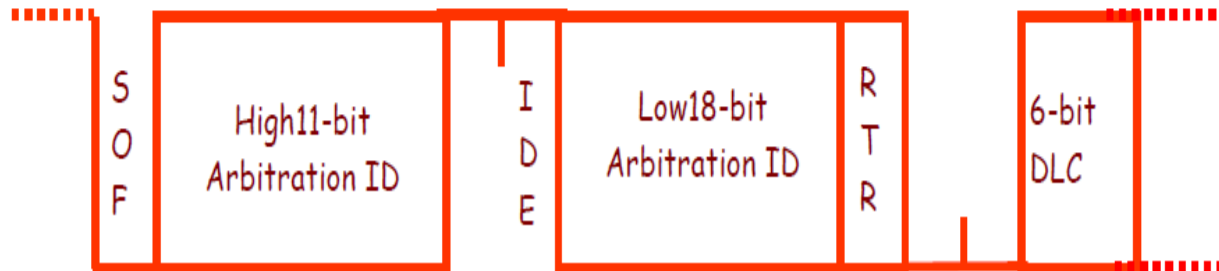
# 9- Les trames CAN

Il existe deux types de trames : la trame standard 2.0A qui comporte un identificateur sur 11 bits et la trame standard 2.0B qui comporte un identificateur sur 29 bits.

Trame standard 2.0a : identificateur sur 11 bits



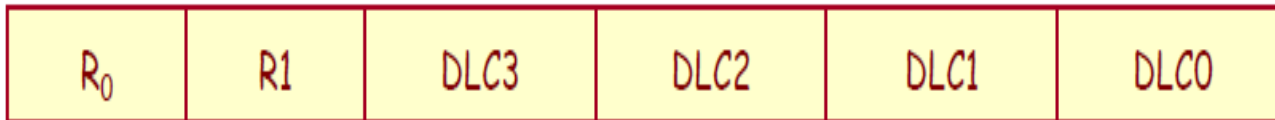
Trame standard 2.0b : identificateur sur 29 bits



- ☐ Les bits successifs ont les significations suivantes :
- ☐ **Bit SOF (Start of Frame) : Bit dominant '0' qui indique le début de la trame.**
- ☐ **Bits d'identification :**
- ☐ Trame standard : 11 bits du MSB au LSB.
- ☐ Trame étendue : 11 bits de poids forts, suivis de 18 bits de poids faibles après le bit IDE.
- ☐ **Bit RTR (Remote transmit request)**
- ☐ ☐ bit dominant (0) pour les trames de données. Les trames de données permettent le transfert des données.
- ☐ ☐ bit récessif (1) pour les trames de requête. Une trame de requête est émise pour demander la transmission d'une trame de données associée à un identificateur (au lieu d'attendre que la source des données transmette ces données de sa propre initiative).



- **Bit IDE (Identifier Extension)**
- 0 bit dominant (0) pour les trames standard,
- 1 bit récessif (1) pour les trames étendues.
- Les trames standard sont prioritaires sur les trames étendues.
- **Bits DLC (Data Length Code)**
- Dans une trame de données, indique le nombre d'octets de données. Dans une trame de requête, indique le nombre d'octets de données souhaités dans la trame de données demandée. Le nombre d'octets de données est compris entre 0 et 8.



On code sur 6 bits mais on en n'utilise que quatre, les deux bits de poids forts ne servant à rien.

- ☐ **Data bytes**
- ☐ Dans les trames de données, ce champ contient entre 0 et 8 octets. Dans les trames de requête, ce champ est vide.
- ☐ **Bits CRC (Cyclic Redundancy Check)**
- ☐ Ces 15 bits permettent de détecter des bits en erreur. Le CRC est calculé dans l'émetteur à partir des bits qui le précèdent. Tous les récepteurs le recalculent à partir des bits reçus. Si le CRC recalculé par un récepteur est différent du CRC émis dans la trame, le récepteur détecte une erreur.
- ☐ **Bit ACK (ACKNOWLEDGE)**
- ☐ L'émetteur émet 1 bit récessif. Les récepteurs intéressés par le message qui ont reçu la trame avec succès émettent un bit ACK dominant.
- ☐ Si aucun récepteur n'a émis un bit ACK, l'émetteur lit un état récessif. Il retransmet alors automatiquement la trame.
- ☐ **Bits EOF (End Of Frame)**
- ☐ Chaque trame se termine par une séquence de 7 bits récessifs. Après cette séquence, le bus se retrouve au repos (idle). Une nouvelle trame peut être émise après une durée supérieure ou égale à 3 bits (silence intertrame).

# 10- Débit net et débit brut

- Le débit maximal brut est de 1Mbits/s mais le vrai débit est forcément moindre à cause de tous les bits qui accompagnent les bits de Data.
- Une trame standard comporte 49 bits en plus des Bits de Data (0...64).
- Une trame étendue comporte 69 bits en plus des Bits de Data (0...64)

# 11- La détection d'erreurs

- Le protocole CAN est très sécurisé grâce à de nombreux mécanismes de détection d'erreur dans une trame.
- Exemple : Soit une ligne bruitée de probabilité d'erreur (Bit Error Rate) égale à  $10^{-4}$ . Avec un débit de 10kbits/s, il y a en moyenne 1 bit faux par seconde. L'utilisation du protocole CAN, sur cette même ligne, permet d'obtenir une probabilité de non détection d'un bit faux de  $10^{-12}$ , ce qui correspond à laisser passer un bit faux en moyenne tous les 3 ans ! Avec une utilisation moyenne de 1 heure par jour, 1 bit faux n'est pas détecté en moyenne tous les 72 ans!

Un noeud CAN peut détecter les types d'erreurs suivantes :

- **Bit Error (bus monitor)**

Pendant la transmission, l'émetteur émet et lit le bus. Si le niveau lu est différent du niveau émis, un bit error est détecté. Ce contrôle ne s'applique que pour les champs Data Length Code, Data Bytes, et Cyclic Redundancy Check de la trame émise.

- **Form Error**

Une erreur Form apparaît quand une violation du format de la trame est détectée.

- **CRC Error**

Une erreur CRC est détectée par un noeud récepteur lorsque le CRC calculé à la réception est différent de celui qui se trouve dans la trame.

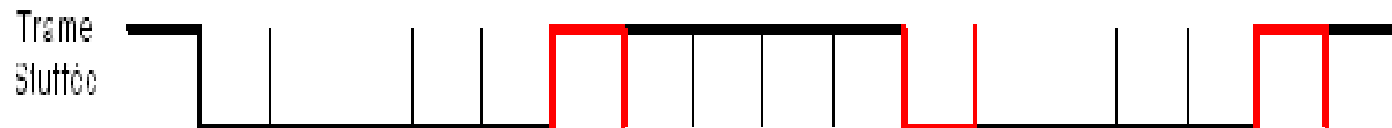
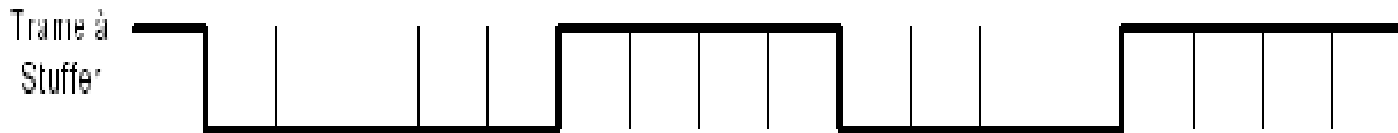
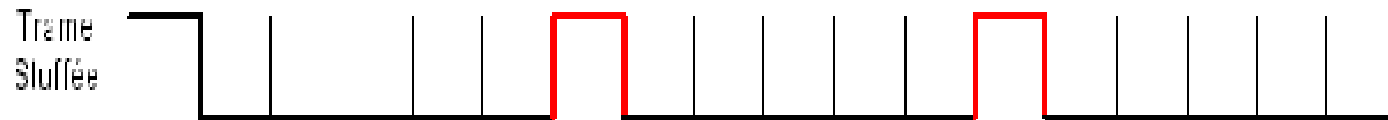
- **Acknowledgement Error**

Une erreur acknowledgment est détectée par un noeud émetteur quand il ne lit pas un bit ACK dominant.

- **Stuff Error**

- Quand un noeud émetteur émet 5 bits identiques, il insère automatiquement un bit complémenté dans la trame. Ce bit, appelé stuff bit, est automatiquement supprimé par les noeuds récepteurs. Une stuff error apparaît donc lorsque 6 bits consécutifs sont égaux.
- Le stuff bit permet aussi de garantir qu'il y aura suffisamment de fronts dans la trame de manière à ce que les horloges des récepteurs puissent être synchronisées sur celle de l'émetteur

# Stuff Error



## 12- La gestion des noeuds défectueux

Le CAN fournit aussi un mécanisme de gestion d'erreur qui élimine du réseau un nœud défectueux lorsqu'un pourcentage important des trames qu'il émet entraîne une erreur. Pour cela, un nœud contient un compteur d'erreurs en réception (REC) et un compteur d'erreurs en émission (TEC). Ces compteurs sont :

- incrémentés de 8 à chaque erreur détectée en émission/réception.
- décrémentés de 1 à chaque trame émise/reçue avec succès.

Selon l'état de ses compteurs, un nœud peut se trouver :

- en état erreur active (fonctionnement normal)
- en état erreur passive (fonctionnement anormal)
- en état bus off (déconnecté)



# Erreur active:

- En fonctionnement normal, tous les noeuds sont en état erreur active. Dans cet état, un noeud participe aux communications sur le bus et émet des trames d'erreur dites actives quand une erreur est détectée. Il envoie sur le bus la



Conséquences :

1- arrêt de la transmission en cours

2- retransmission

Lorsque les compteurs TEC et REC sont supérieurs à la valeur 127 alors le noeud passe en erreur passive.

# Erreur passive :

- Dans cet état, un noeud participe aux communications sur le bus et émet des trames d'erreur dites passives quand une erreur est détectée.

6 bits récessifs (Error flag)	8 bits récessifs (délimiteur)
-------------------------------	-------------------------------

- Conséquences :
  - 1- continuation de la transmission en cours
  - 2- pas de retransmission si la trame est reçue avec succès par les autres noeuds
- Lorsque le compteur TEC dépasse la valeur 255, le noeud rentre dans l'état Bus off.
- **Bus off**
- Dans cet état, un noeud ne participe plus aux communications sur le bus. Il ne peut être remis en état erreur active que par une opération manuelle.

# Les principaux moyens d'accès au médium

**Maître - Esclave**

**Anneau à jeton**

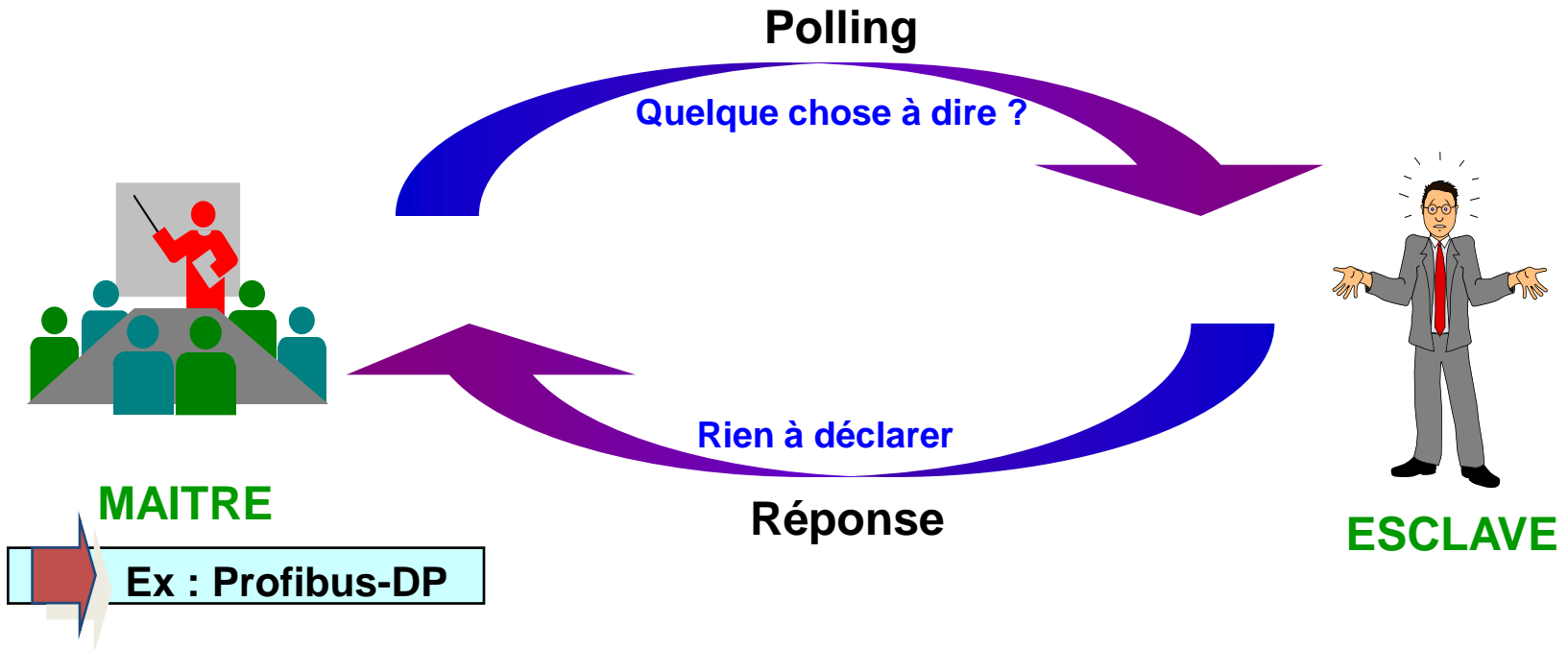
**Accès aléatoire**

# Maître - Esclave

Se situe au niveau de l'accès au médium

Le **MAITRE** est l'entité qui accorde l'accès au médium.

L'**ESCLAVE** est l'entité qui accède au médium après sollicitation du maître.

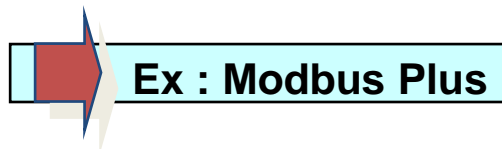


# Anneau à jeton = Token ring

Se situe au niveau de l'accès au médium

Les membres d'un **ANNEAU** logique ont l'autorisation d'émettre lors de la réception du jeton.

Le **JETON** est un groupe de bits qui est passé d'un nœud au suivant dans l'ordre croissant des adresses.



# Accès aléatoire

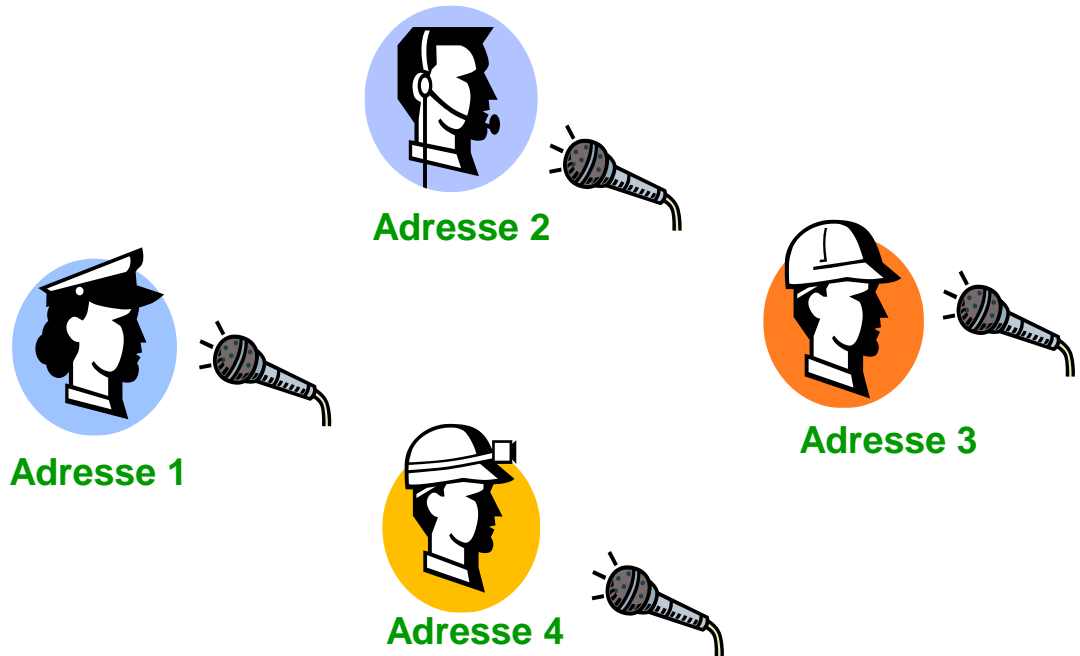
Se situe au niveau de l'accès au médium

## Carrier Sense Multiple Access

Un ensemble de règles détermine comment les produits sur le réseau réagissent lorsque deux équipements tentent d'accéder au médium en même temps (*collision*).

Discussion informelle entre individus indisciplinés :

Dès qu'un silence est détecté, celui qui désire parler prend la parole.



## CSMA/CD CSMA/CA

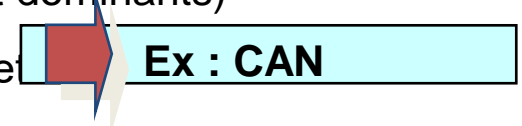
**CSMA/CD** = *Carrier Sense Multiple Access Collision Detect* : Collision destructive

- 1 - Détection de la collision
- 2 - Arrêt de transmission de la trame
- 3 - Emission d'une trame de brouillage
- 4 - Attente d'un temps aléatoire
- 5 - Ré-émission de la trame



**CSMA/CA** = *Carrier Sense Multiple Access Collision Avoidance* : Collision non destructive collision

- 1 - Détection de la collision non destructive (bits récessifs et dominants)
- 2 - L'équipement avec la priorité la plus basse cesse d'émettre
- 3 - Fin de transmission de l'équipement le plus prioritaire
- 4 - L'équipement avec la priorité la plus basse peut émettre sa trame





## INTRODUCTION

- Le Modbus est un protocole de communication industriel introduit par Modicon en 1979.
- Il est généralement utilisé avec les automates programmables ou les équipements de types industriels.
- Il est maintenant devenu une norme "open protocol" dans le domaine de l'automatisme et de la communication industrielle, et est le moyen le plus couramment utilisé pour faire communiquer des équipements industriels.
- IL existe des versions avec des modifications mineures ou adaptées à d'autres environnements (comme par exemple JBUS ou MODBUS II).



# INTRODUCTION

- Un des avantages du protocole Modbus est sa flexibilité, mais aussi sa facilité de mise en œuvre.
- La plupart des appareils et dispositifs embarqués comme les microcontrôleurs, les automates, les capteurs intelligents etc...sont équipés d'interface Modbus et sont capables de communiquer en Modbus.
- Au début,le Modbus a été initialement conçu pour fonctionner avec les lignes de communication filaires série mais il existe aujourd'hui des extensions à la norme pour les communications sans fil et les réseaux TCP / IP.
- Le protocole Modbus permet la communication entre plusieurs équipements connectés sur un même réseau, par exemple un système qui mesure la température et l'humidité d'un four peut communiquer ses résultats à un ordinateur de traitement via Modbus.

# LES SUPPORTS PHYSIQUES DE TRANSMISSION DU PROTOCOLE MODBUS

Les communications Modbus peuvent s'effectuer via les supports physiques suivants :

- RS-232
- RS-485
- RS-422
- Ethernet TCP/IP (Modbus Ethernet)

## LES VARIATIONS DU PROTOCOLE MODBUS

Il existe 3 variations du protocole Modbus:

- Le Modbus RTU (8bits)
- Le Modbus ASCII (7 bits)
- Le Modbus TCP/IP (ethernet)

Les communications de type modbus sont caractérisées par leur vitesse de transmission ou baudrate qui s'exprime en bits/s. Typiquement, cette vitesse de transmission est souvent comprise entre 9600 et 19 200 bits/s, mais on peut avoir des vitesses supérieures.

# **LE MODBUS VIA LIAISON RS-232/RS-422/RS-485**

- **La communication modbus via RS-232,RS-422 et RS-485 fonctionne en mode maitre/esclave. Cela signifie qu'un dispositif fonctionnant comme maître va interroger un ou plusieurs dispositifs fonctionnant comme esclave.**
- **Un dispositif esclave ne peut donc pas fournir volontairement des informations au maître, il doit attendre une sollicitation.**
- **Le maître peut écrire des données dans les registres d'un périphérique esclave ou lire les données à partir des registres de celui-ci.**

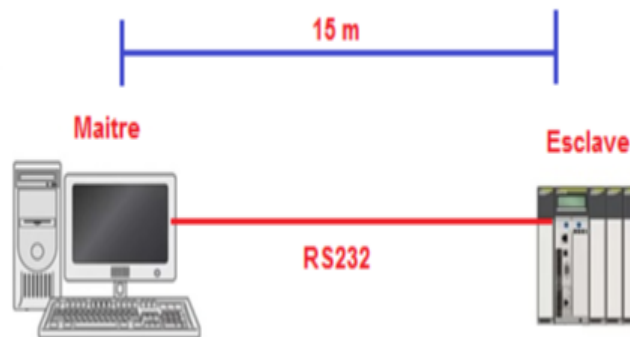
**Le RS232,RS422 et RS485 sont des supports physiques de transmission de données en série. Chacune de ces interfaces a des avantages et des inconvénients.**

# Le RS232

- C'est le plus connu des standards de communication série. Les ports série RS232 sont présents sur la plupart des PCs standards. Il est de type point to point et est composé des lignes Rx,Tx et GND.
- Le RS232 permet de faire communiquer uniquement un maitre et un esclave sur chaque ligne. Il fonctionne en full duplex et sa vitesse de communication peut aller jusqu'à 115 kbits/s.
- 
- En RS232, la distance séparant les deux équipements ne dépasse pas généralement 15 m. Si on n'a besoin d'ajouter plusieurs esclaves sur la même ligne, il faudra utiliser les liaisons RS422 ou RS485 qui sont plus adéquates.
- Le RS232 a comme inconvénients d'être inadapté dans les environnements où il y'a beaucoup de bruits ou parasites (risque perturbation transmission).

# Le RS232

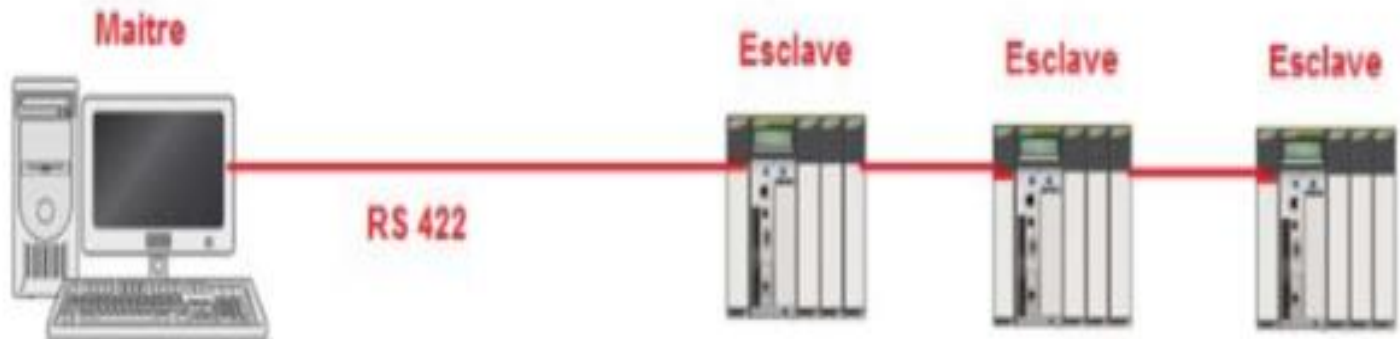
- C'est le plus connu des standards de communication série. Les ports série RS232 sont présents sur la plupart des PCs standards. Il est de type point to point et est composé des lignes Rx,Tx et GND.
- Le RS232 permet de faire communiquer uniquement un maitre et un esclave sur chaque ligne. Il fonctionne en full duplex et sa vitesse de communication peut aller jusqu'à 115 kbits/s.
- En RS232, la distance séparant les deux équipements ne dépasse pas généralement 15 m. Si on n'a besoin d'ajouter plusieurs esclaves sur la même ligne, il faudra utiliser les liaisons RS422 ou RS485 qui sont plus adéquates.
- Le RS232 a comme environnements où perturbation trans



oté dans les  
u parasites (risque

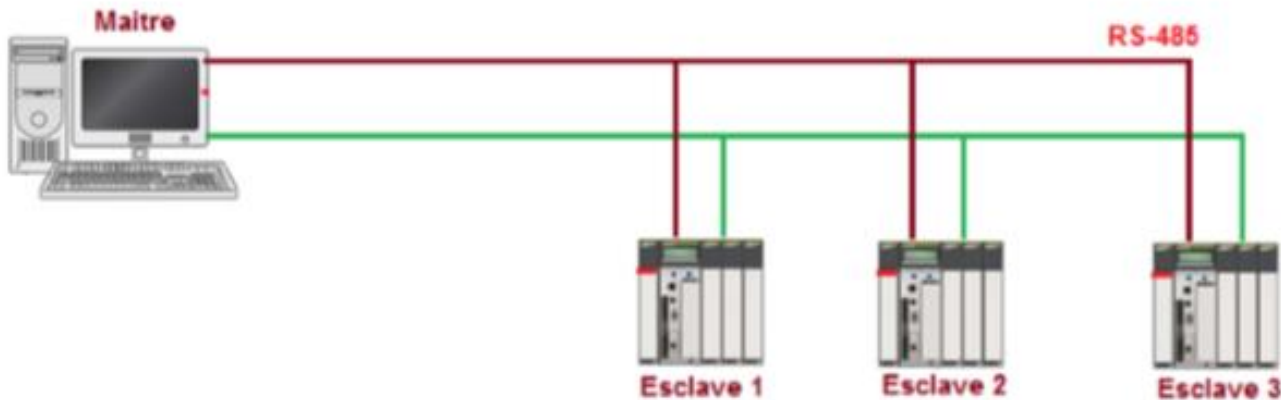
# Le RS422

- Il est full duplex et est utilisé sur les ordinateurs Apple, sa vitesse de transmission peut aller jusqu'à 10 Mbits/s.
- Les signaux sont envoyés sur 2 fils afin d'augmenter la fréquence de transmission.
- Il peut supporter jusqu'à 10 récepteurs par ligne (on dit alors qu'il est multidrop ou multi-points).



# Le RS485

- Les médias de type RS485 sont souvent en half duplex c'est-à-dire la transmission s'effectue via 2 fils.



- Ils permettent de faire communiquer jusqu'à 32 périphériques sur la même ligne de données et sur une distance pouvant aller jusqu'à 1200 m sans répéteurs.
- A noter que l'on peut obtenir du full duplex en utilisant 4 fils de transmission au lieu de 2. Cela permet d'avoir un débit de transmission plus rapide.
- Chaque périphérique esclave peut aussi communiquer avec les 32 autres périphériques.
- Les protocoles de communication RS422 et RS485 sont multidrop c'est à dire plusieurs périphériques peuvent communiquer sur la même ligne de données.
- Le RS485 a comme avantages d'être immunisé contre les bruits ou parasites.

# LES SPECIFICITES DU MODBUS via interface série RS-xxx

- En modbus série, seul le maître est actif, les esclaves sont complètement passifs. C'est le maître qui doit lire et écrire dans chaque esclave.
- Le maître peut communiquer avec un nombre d'esclaves allant jusqu'à 247 (cas du modbus via RS-485 avec l'utilisation de répéteurs) sur le même réseau.
- Les adresses allant de 248 à 255 sont des adresses réservées



Le RS485 ne peut pas comporter plus de 32 périphériques sur le même nœud, on utilise alors des répéteurs afin de pouvoir ajouter d'autres périphériques sur la ligne





# TOPOLOGIE D'EQUIPEMENTS CONNECTES VIA LE MODBUS SERIE RS-xxx

- Dans l'image ci-dessous le système Scada/HMI agit en tant que maître alors que les automates agissent en tant que esclaves.

**Scada / HMI**

**Maitre**



**Equipements esclaves**



## LES MESSAGES DE BROADCAST

- Aussi appelé message de diffusion est une communication unidirectionnelle initiée par le maitre et envoyé à tous les esclaves.
- Ce type de message n'obtient pas de réponse de la part des esclaves, il est utilisé pour envoyer des commandes communes à tous les esclaves par exemple les commandes de configuration ou de réinitialisation.

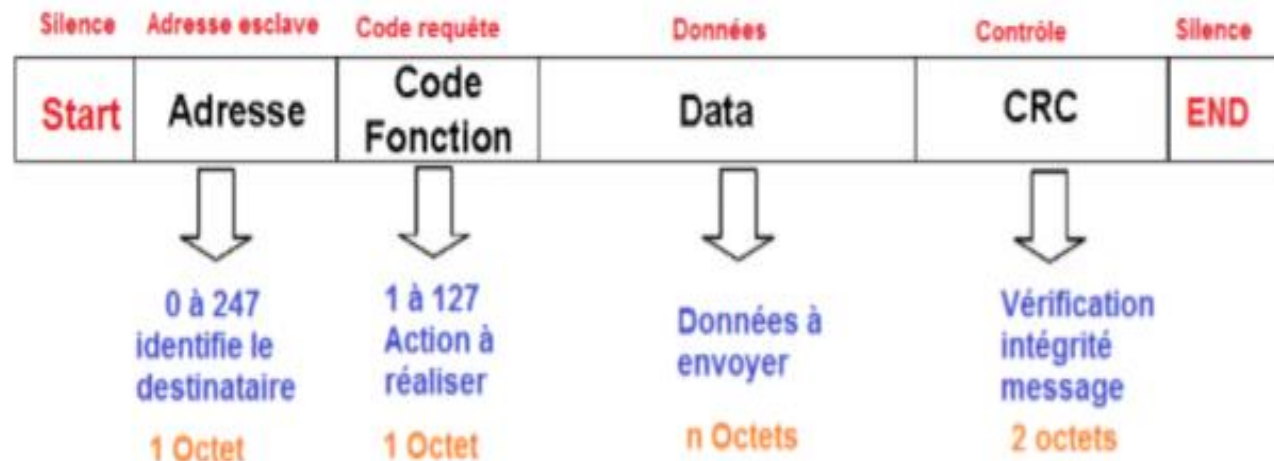
## LE MODBUS RTU (Remote Terminal Unit)

- La communication Modbus RTU est de type série et se fait via les interfaces série RS232, RS485 ou RS422. Le codage des informations s'effectue en binaire.
- Le modbus RTU fait partie des protocoles industriels les plus utilisés.
- Si la communication s'effectue via le RS232, il ne peut y avoir dans ce cas qu'un seul maitre et qu'un seul esclave. Par contre si la communication s'effectue via le RS485 ou le RS422, on peut avoir plusieurs esclaves.

NB : En modbus RTU on peut pas avoir plusieurs maitres. Le mode de fonctionnement multi-maitre n'est possible qu'avec le modus TCP/IP

# LE MODBUS RTU (Remote Terminal Unit)

- L'avantage du mode RTU est que les données à transmettre prennent moins de place donc moins de temps pendant les transmissions. En effet, on adresse plus de données en 8 qu'en 7 bits.
- La trame du MODBUS RTU est constituée d'une suite de caractères hexadécimaux et contient les informations suivantes :
  - Numéro d'esclave (1 octet) (le numéro 00 est réservé aux messages de diffusion)
  - Code fonction (1 octet)
  - Données (n octets)
  - CRC (2 octets)



# LE MODBUS RTU (Remote Terminal Unit)

- Chaque octet composant une trame RTU est codé sur 2 caractères hexadécimaux (2 fois 4 bits)
- La taille maximale des données est de 256 octets. L'ensemble des informations contenues dans le message est exprimé en hexadécimal.
- Chaque octet composant un message est transmis en mode RTU de la manière

**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).

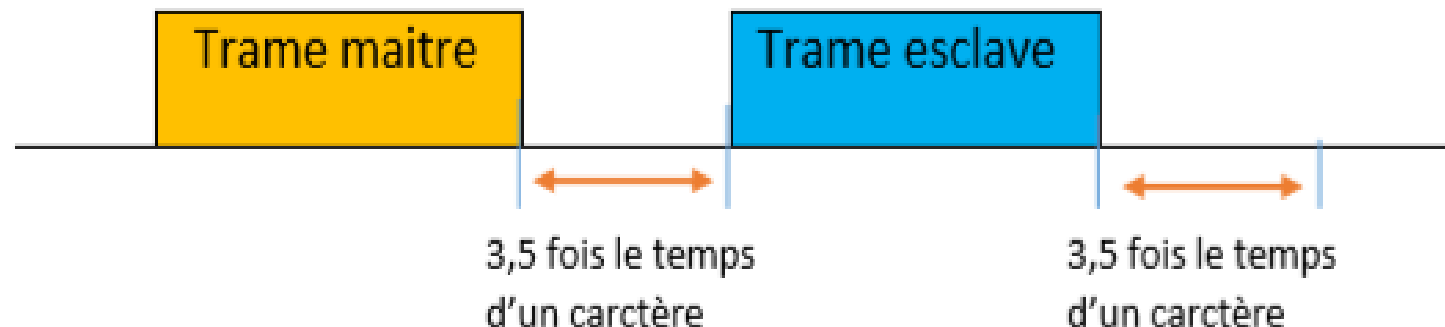
Avant et après chaque message(trame), il doit y avoir un silence minimum de 3,5 fois le temps de transmission d'un caractère. L'ensemble du message doit être transmis de manière continue.

Ainsi,l'équipement détecte le début d'un message quand il reçoit un caractère valide (contenant son adresse ou l'adresse 00) dans un intervalle de temps d'au moins 3,5 fois la longueur d'un caractère.

Si le débit de transmission est 9600 bits/s, on aura : 3,5 caractère (  $3,5 * 11 * (1/9600)$  )

Le temps maximum entre 2 caractères doit être inférieur à 1,5 fois le temps de transmission d'un caractère. Dans le cas contraire, il y a une erreur de transmission.

NB : 1 caractère est un format de 11 bits constitué de : 1 bit de start, 8 bits de données et 2 bit de stop (**ou 1 bit parité + 1 bit stop**)



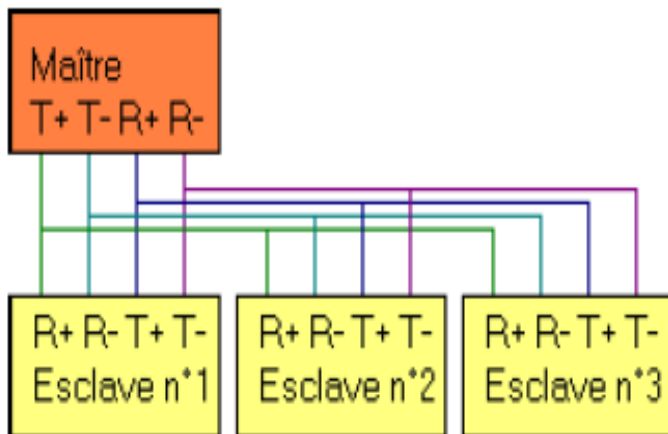
La nature des informations de la trame peut varier selon que l'on fera de la lecture/écriture, de mots, de bits ....

# Le protocole MODBUS

## Interface série RS485 MODBUS

### 1. Principe

- Le protocole **Modbus** (marque déposée par **MODICON**) est un protocole de dialogue basé sur une structure hiérarchisée entre un maître et plusieurs esclaves.
- Une **liaison multipoints** (RS-485) relie maître et esclaves.

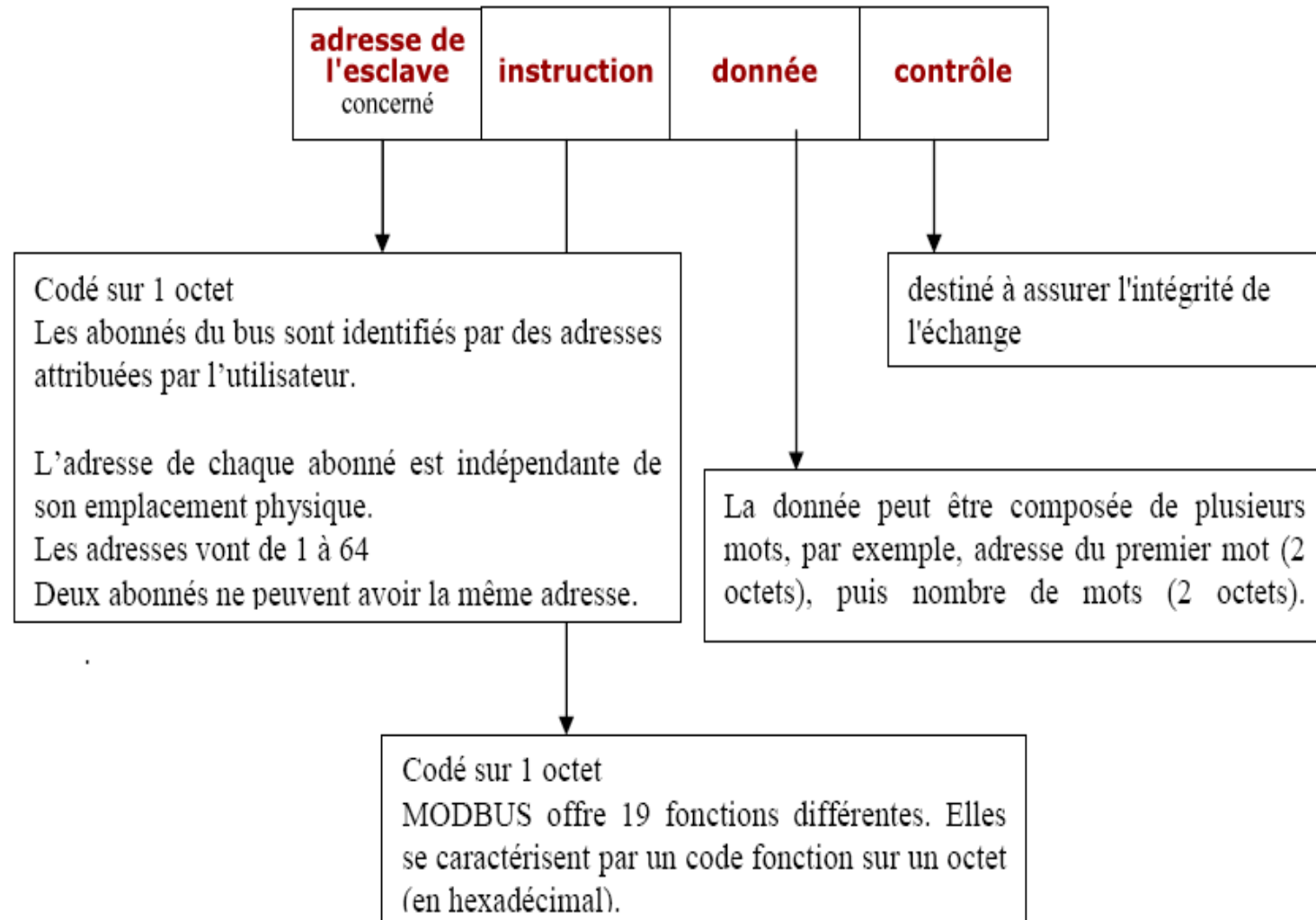


## 2.Données :

- Vitesse de transmission : 9600 ou 19200 bits/seconde
- Trame : 8 bits sans parité
- Parité : NO, sans parité ; EVEN, parité paire; ODD, parité impaire
- 1 bit ou 2 bits stop
- Mode de communication : **half-duplex**. (2 fils)
  - le maître parle à un esclave et attend sa réponse,
  - le maître parle à l'ensemble des esclaves, sans attente de réponse (diffusion générale).
- Il ne peut y avoir sur la ligne qu'un seul équipement en train d'émettre.  
Aucun esclave ne peut envoyer un message sans une demande préalable du maître. Le dialogue entre les esclaves est impossible.

# Structure du message :

Le maître envoie un message constitué de la façon suivante:



La détection de fin de message est réalisée sur un **silence** de plus de 2 caractères.



# Exemple :

Lecture par le maître des mots W450 à W456 sur un ATV-28 (esclave n°2). Cette requête comporte 8 octets:

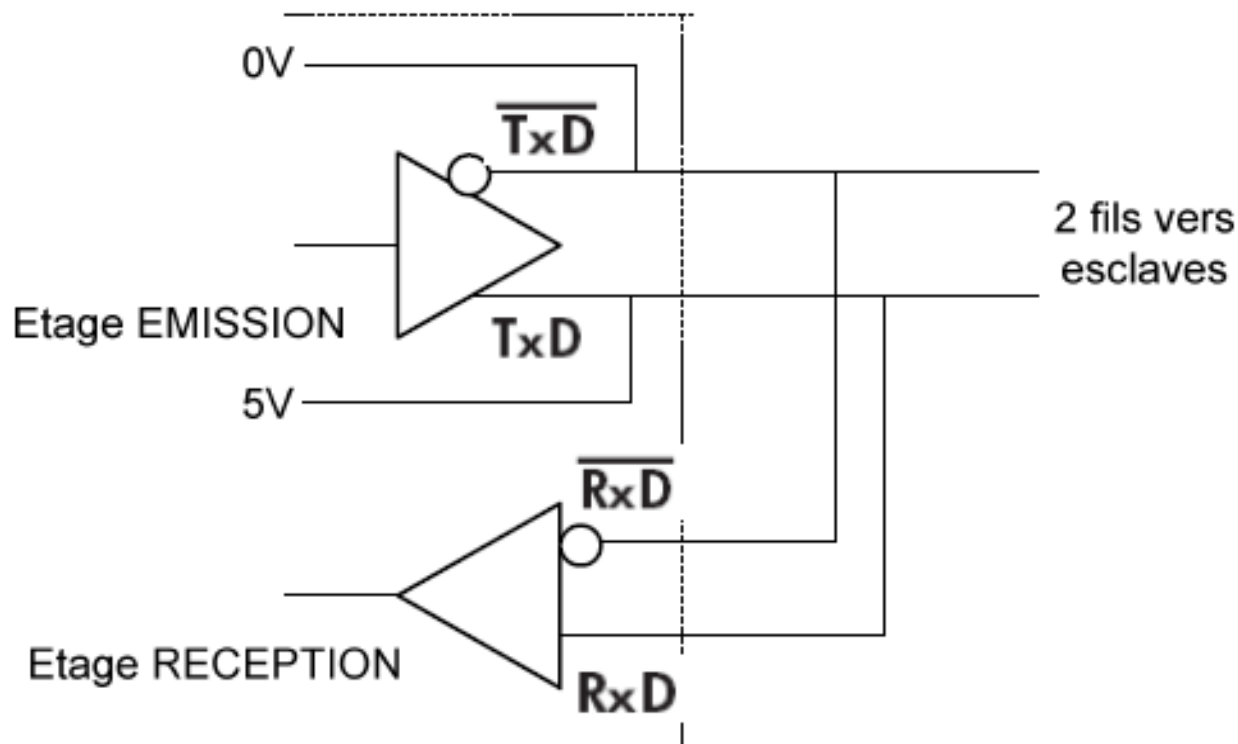
02	03	01 C2	00 07	XX XX
n° de l'esclave	instruction de lecture de N mots	450 est converti en code hexadécimal	7 mots	Valeur du CRC

Le protocole Modbus est très utilisé pour les communications des automates programmables industriels et des variateurs de vitesse des moteurs électriques.

# Câblage d'une liaison RS485 :

**RS-485** : c'est une liaison série, de type asynchrone, différentielle qui permet un débit élevé (jusqu'à 10 Méga-bits/seconde) sur une distance importante (jusqu'à 1200m).

Elle dispose de 2 bornes d'émission polarisées notées Tx(+), Tx(-) ou  $\overline{\text{TxD}}$  et de 2 bornes de réception polarisées notées Rx(+), Rx(-) ou  $\overline{\text{RxD}}$ .



# Mode RTU (Remote Terminal Unit) :

## Mode RTU :

Le mode de transmission utilisé est le mode RTU. La trame ne comporte ni octet d'en-tête de message, ni octets de fin de message.

Sa définition est la suivante :



Les données sont transmises en binaire.

CRC16 : paramètre de contrôle polynomial (cyclical redundancy check).

La détection de fin de trame est réalisée sur un silence supérieur ou égal à 3 caractères.

**Type RTU** (Unité terminale distante) : chaque octet composant une trame est codé sur 2 caractères hexadécimaux (2 fois 4 bits).

START	Adresse	Fonction	Données	CRC	END
Silence	1 octet	1 octet	n octets	2 octets	Silence

La taille maximale des données est de 256 octets.

# Format général d'une trame

- Deux types de codage peuvent être utilisés pour communiquer sur un réseau Modbus.
- Tous les équipements présents sur le réseau doivent être configurés selon le même type.

Type ASCII : chaque octet composant une trame est codé avec 2 caractères ASCII (2 fois 8 bits).

START	Adresse	Fonction	Données	LRC	END
1 caractère	2 caractères	2 caractères	n caractères	2 caractères	2 caractères « CR LF »

LRC : C'est la somme en hexadécimal modulo 256 du contenu de la trame hors délimiteurs, complémentée à 2 et transmise en ASCII.

Type RTU (Unité terminale distante) : chaque octet composant une trame est codé sur 2 caractères hexadécimaux (2 fois 4 bits).

START	Adresse	Fonction	Données	CRC	END
Silence	1 octet	1 octet	n octets	2 octets	Silence

## **Exemple d'échange entre un maître et un esclave**

**Trame émise par le maître** : 04 03 00 02 0001 25 CA

- Adresse esclave : 04
- Code fonction 03 = lecture registre
- N° du registre de début de lecture : MSB : 00 et LSB : 02
- Nombre de registre de lecture : MSB : 00 et LSB : 01
- CRC : 25 CA

**Réponse de l'esclave avec erreur** : 04 83 02 01 31

- Adresse esclave : 04
- Code fonction : lecture avec MSB = 1 : 83
- Code erreur (n° registre) : 02
- CRC : 01 31

**Réponse de l'esclave sans erreur** : 04 03 02 02 58 B8 DE

- Adresse esclave : 04
- Code fonction : lecture registre : 03
- Nombre d'octets données : 02
- Données du registre 0002 : MSB 02 et LSB : 58
- CRC : B8 DE

## Services supportés par MODBUS

MODBUS offre 19 fonctions différentes. Elles se caractérisent par un code fonction sur un octet (en hexadécimal). Tous les équipements ne supportent pas tous les codes fonction.

Code	Nature des fonctions MODBUS	TSX 37
H'01'	Lecture de n bits de sortie consécutifs	*
H'02'	Lecture de n bits de sortie consécutifs	*
H'03'	Lecture de n mots de sortie consécutifs	*
H'04'	Lecture de n mots consécutifs d'entrée	*
H'05'	Ecriture de 1 bit de sortie	*
H'06'	Ecriture de 1 mot de sortie	*
H'07'	Lecture du statut d'exception	
H'08'	Accès aux compteurs de diagnostic	
H'09'	Téléchargement, télé déchargement et mode de marche	
H'0A'	Demande de CR de fonctionnement	
H'0B'	Lecture du compteur d'événements	*
H'0C'	Lecture des événements de connexion	*
H'0D'	Téléchargement, télé déchargement et mode de marche	
H'0E'	Demande de CR de fonctionnement	
H'0F'	Ecriture de n bits de sortie	*
H'10'	Ecriture de n mots de sortie	*
H'11'	Lecture d'identification	*
H'12'	Téléchargement, télé déchargement et mode de marche	
H'13'	Reset de l'esclave après erreur non recouverte	

## Différence des trames ASCII ou RTU

- Certains équipements permettent le choix entre ces deux formats :
- Le format RTU permet pour une même vitesse de transmission un plus fort débit de données.
- Le format ASCII offre une "souplesse" plus importante sur les timing inter-octet (jusqu'à 1 seconde) et constitue une véritable transmission asynchrone.
- Définition : RTU, Remote Terminal Unit. Ces deux formats de trames peuvent être utilisés dans le protocole MODBUS, mais sont incompatibles entre eux. Environ 95% des modules communicants sur MODBUS utilisent des trames "RTU".

# PROFIBUS

- PROFIBUS est un réseau de communication selon la norme RS-485.
- Les stations actives accèdent au réseau selon la méthode du "Token Bus" (bus à jeton).
- Les stations passives selon la méthode "maître-esclave".
- La vitesse max de transmission est au maximum de 12 Mbits/s (cette vitesse est fonction du matériel utilisé et de la distance)
- 32 stations max par segment, 127 stations max sur un réseau
- Les supports de transmission sont:
  - liaison bifilaire
  - fibre optique
  - Liaison sans fil (IR et Radio)



# Spécifications techniques de PROFIBUS

Standard	PROFIBUS EN 50 170 / IEC 61158
Méthode d'accès	Passage de jeton et maître/esclave (déterministe)
Vitesse	9.6 Kbit/sec. - 12 Mbit/sec.
Médiums	Cuivre : une paire blindée Optique: câble fibre optique (verre et plastique)
Nbre de participants	127
Taille	Cuivre: max. 9.6 km (dépend de la vitesse) Optique: plus de 100 km (dépend de la vitesse)
Topologie	Ligne, arbre, étoile, anneau, anneau redondant
Applications	Niveau cellule et terrain

# PROFIBUS DP (Decentralized Periphery)

## Norme EN 50170/IEC 61158

Dialogue de type maitre-esclave, indépendant du temps de cycle automate

- DP offre la possibilité de communiquer de manière transparente avec la périphérie décentralisée ou avec un esclave intelligent par exemple du type API.  
Volume d'échange max 244 octets entrée/244 octets sortie
- Tous les esclaves normalisés PROFIBUS DP peuvent être raccordés, leur description se fait par un fichier \*.GSD.

Plus de 1700 produits, en provenance de plus de 280 offreurs.

# PROFIBUS PA

Ce terme désigne les exigences et caractéristiques d'un réseau PROFIBUS utilisé dans le process, PA -> **Process Automation**.

PROFIBUS PA utilise le même protocole que [PROFIBUS DP](#), il s'agit simplement d'un profil qui permet de standardiser des caractéristiques et comportement d'appareils standard.

Tout ce qui a été décrit sur le fonctionnement de [PROFIBUS DP](#) reste vrai pour PROFIBUS PA.

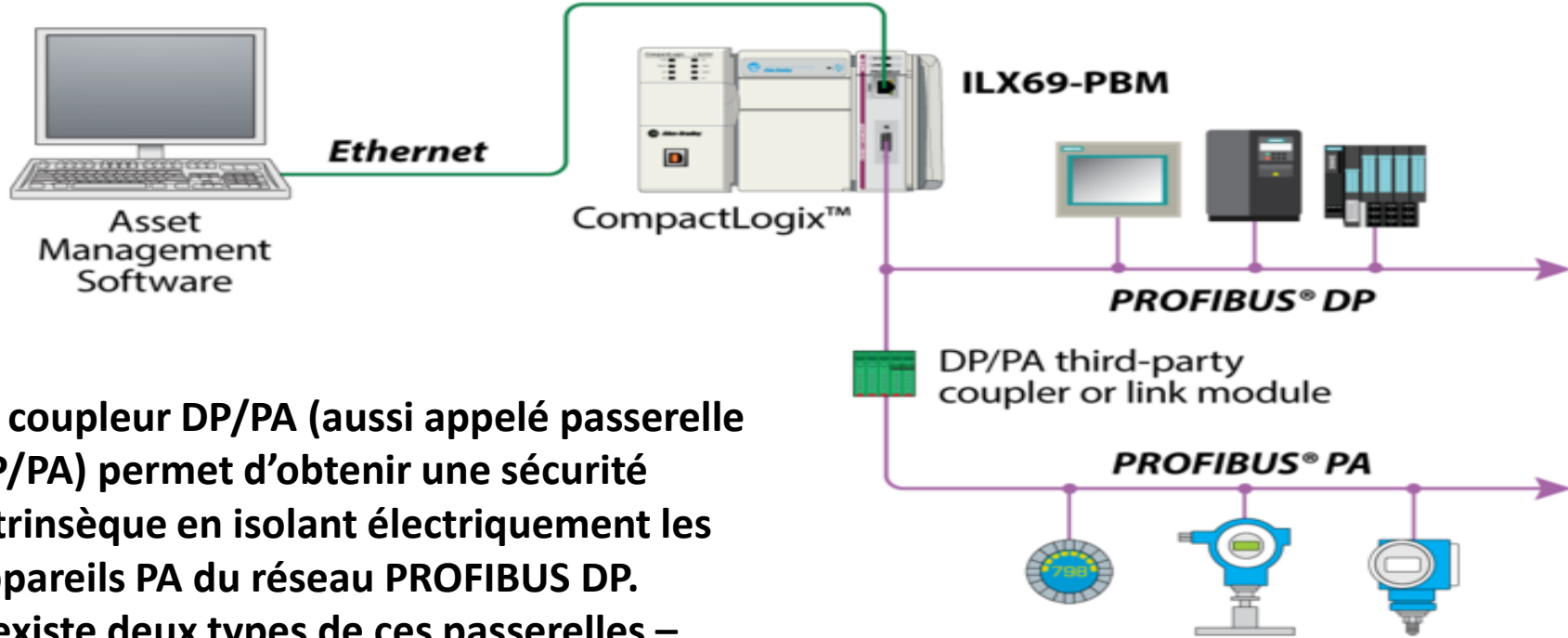
## Quelles sont les différences avec DP ?

- Les contraintes dans le process sont différentes de celles que l'on connaît dans les procédés dits manufacturiers.
- La proportion de valeurs analogiques est beaucoup plus importante.
- Les exigences de rapidité sont moindres.
- Les appareils sont principalement des capteurs et des actionneurs process.
- Ces derniers sont télé alimentés.
- Beaucoup d'installations en process sont en zone explosible ATEX (chimie, pharmacie, Oil & Gas ...).

## Différence entre profibus PA et Profibus DP

-----Profibus-DP (Decentralized Peripherals) est utilisé pour connecter des équipements actifs et des détecteurs à un contrôleur central dans des applications de production industrielle. Le bus propose en standard un certain nombre de moyens de diagnostic.

-----Moins répandu, Profibus-PA (Process Automation) est utilisé pour des équipements de mesure et de surveillance ; il est particulièrement conçu pour les zones à risques (d'explosion notamment). La couche physique est conforme à IEC 61158-2, permettant d'alimenter les instruments connectés via le bus tout en limitant les courants qui permettraient un risque d'explosion, même en cas de défaut ; cependant cette fonctionnalité limite le nombre d'équipements pouvant être connectés à un même segment de bus PA. Le débit y est limité à 31,25 kbit/s



Le coupleur DP/PA (aussi appelé passerelle DP/PA) permet d'obtenir une sécurité intrinsèque en isolant électriquement les appareils PA du réseau PROFIBUS DP. Il existe deux types de ces passerelles – transparente et non-transparente. Les principales différences sont:

- Le coupleur transparent n'est pas détecté par le maître PROFIBUS. Il requiert la limitation de la bande passante à 45.45kbps, il est donc particulièrement adapté à l'industrie de process où la vitesse n'est pas un impératif.
- Le coupleur non-transparent est vu par le maître PROFIBUS comme un noeud additionnel, il requiert généralement l'utilisation d'un outil de configuration spécifique afin d'intégrer les fichiers GSD des appareils PA.

Les appareils PA ne sont pas directement accessibles par le maître PROFIBUS qui peut communiquer jusqu'à 12Mbps avec les appareils PROFIBUS DP, permettant l'utilisation simultanée d'appareils DP et PA sur un seul réseau physique.

# PROFIBUS FDL

FDL (Fieldbus Data Link) offre des services de **communication de type SEND/RECEIVE** pour la transmission de données sur le sous-réseau PROFIBUS entre stations actives.

PA est conçu spécialement pour l'**instrumentation de process**.

Le support de transmission est ici une paire torsadée blindée. Le signal est transmis sous forme de données synchrone à **45,45 kbit/s**.

La **ligne de données** est en général également **utilisée** pour **l'alimentation des appareils** de terrain.

Possibilité de **fonctionnement à sécurité intrinsèque** (en atmosphère explosible)

# QCM

1/ Parmi, les termes suivants, lequel n'est pas une variante du protocole Modbus

- Modbus ASCII
- Modbus PLC
- Modbus RTU

2/ Choisissez la bonne réponse

- Un périphérique esclave ne pas fournir volontairement des informations au périphérique maître sans sollicitation
- Un périphérique esclave peut fournir volontairement des informations au périphérique maître

3/ Répondre par Vrai ou Faux : En modbus RTU, seuls les esclaves sont actifs, le maître est complètement passif

- Faux
- Vrai

4/ Choisissez la bonne réponse

- Une message de broadcast est un message envoyé par le maître à tous ses esclaves
- Un message de broadcast est un message envoyé par l'esclave au maître

5/ Répondre par Vrai ou Faux : Pour vérifier l'intégrité des données d'une trame modbus RTU, on utilise le LRC

- Vrai
- Faux

# Exercices MODBUS

## Question du maître

**Remarque :** le "mot" représente ici 2 octets soit 16 bits.

### Lecture de n mots : fonction 3 ou 4

■ Demande.

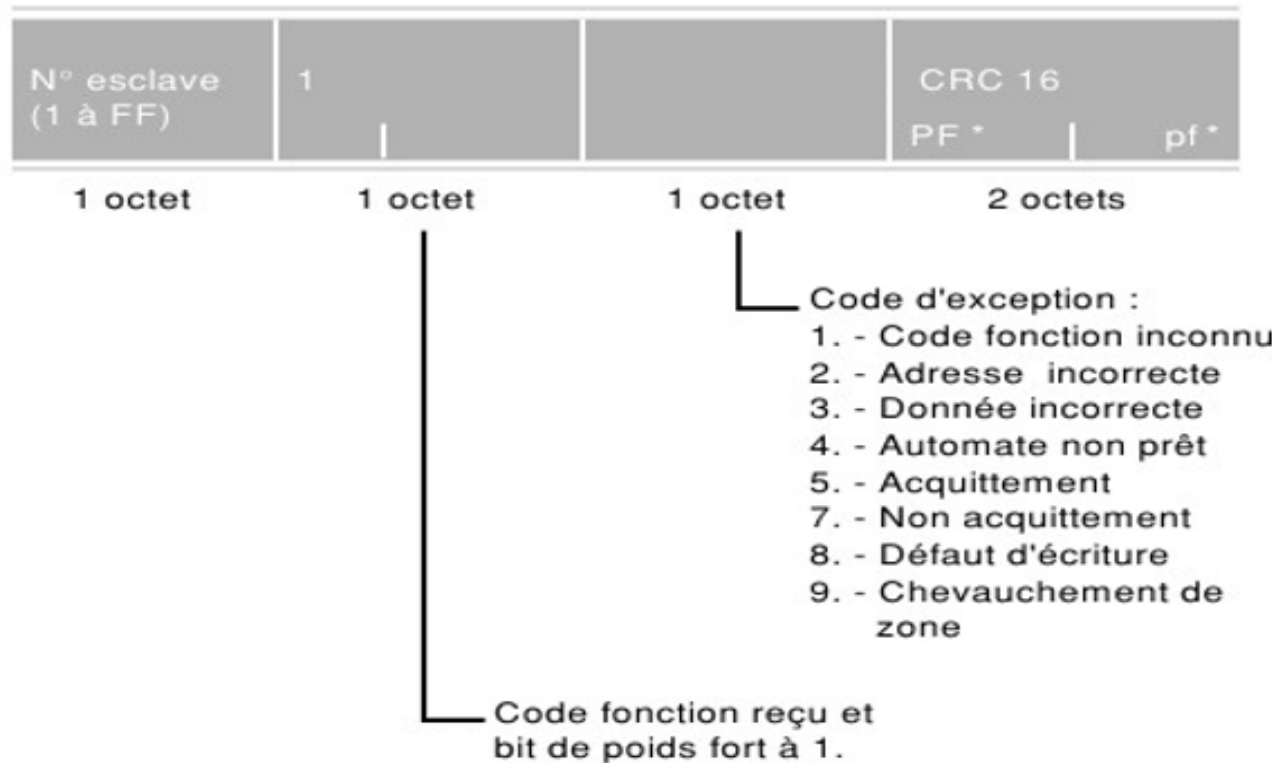
N° esclave	3 ou 4	Adresse du 1 <sup>er</sup> mot à lire : PF *   pf *	Nombre de mots à lire n ≤ 125 : PF *   pf *	CRC 16 pf *   PF *
1 octet	1 octet	2 octets	2 octets	2 octets

■ Réponse.

N° esclave	3 ou 4	Nombre d'octets lus	Valeur 1 <sup>er</sup> mot PF *   pf *	Valeur du dernier mot PF *   pf *	CRC 16 pf *   PF *
1 octet	1 octet	1 octet	2 octets	2 octets	2 octets



Contenu d'une réponse exception.



Le message émis par le maître est le suivant :

04	03	00	02	00	01	25	9F
----	----	----	----	----	----	----	----

Exercice n°1: Décoder le message émis par le maître en complétant le tableau suivant.

Réponse :

Champs	Valeur	Signification/Décodage
Adresse de l'esclave		
Code fonction		
Mot de contrôle (CRC)		

## ***Réponse(s) de l'esclave***

L'esclave peut émettre deux types de réponse :

Réponse n°1 :

04	03	02	02	58	74	DE
----	----	----	----	----	----	----

Réponse n°2 :

04	83	02	D0	F0
----	----	----	----	----

### **Exercice n°2**

Décoder le message « réponse n°1 » émis par l'esclave en complétant le tableau suivant.

*Réponse :*

<b>Champs</b>	<b>Valeur</b>	<b>Signification/Décodage</b>
Adresse de l'esclave		
Code fonction		
Mot de contrôle (CRC)		

### **Exercice n°3**

Décoder le message « réponse n°2 » émis par l'esclave en complétant le tableau suivant.

*Réponse :*

<b>Champs</b>	<b>Valeur</b>	<b>Signification/Décodage</b>
Adresse de l'esclave		
Code fonction		
Mot de contrôle (CRC)		

D'après les messages transférés entre le maître et l'esclave, en déduire le type de trame (RTU ou ASCII) utilisé ici.

Réponse :

# Exercice

Etude des trames échangées entre un contrôleur et son esclave par le réseau **MODBUS**. On relève sur l'analyseur les trames suivantes :

Question contrôleur : **03 10 05 EF 01 02 06 00 00 00 00 32 33 65 CA**

Réponse de l'esclave : **03 10 05 EF 01 02 30 3B**

1- Compte tenu de la configuration de la liaison (vitesse 9600 bauds, bit Start, données sur 8bits, 1 bit de stop),

a- Calculer la durée de transmission d'une trame constituée de N caractères ?

( un caractère=bit start, 8 bits données, 1 bit de stop) .....

b- En déduire les temps de transmission des trames du contrôleur et de l'esclave,

On suppose que le délai d'attente est l'équivalent de 3 octets :.....

2- Quelles sont les raisons du choix du réseau d'API MODBUS ?

.....

3- Comparer Le réseau MODBUS RTU et MODBUS ASCII.

.....