

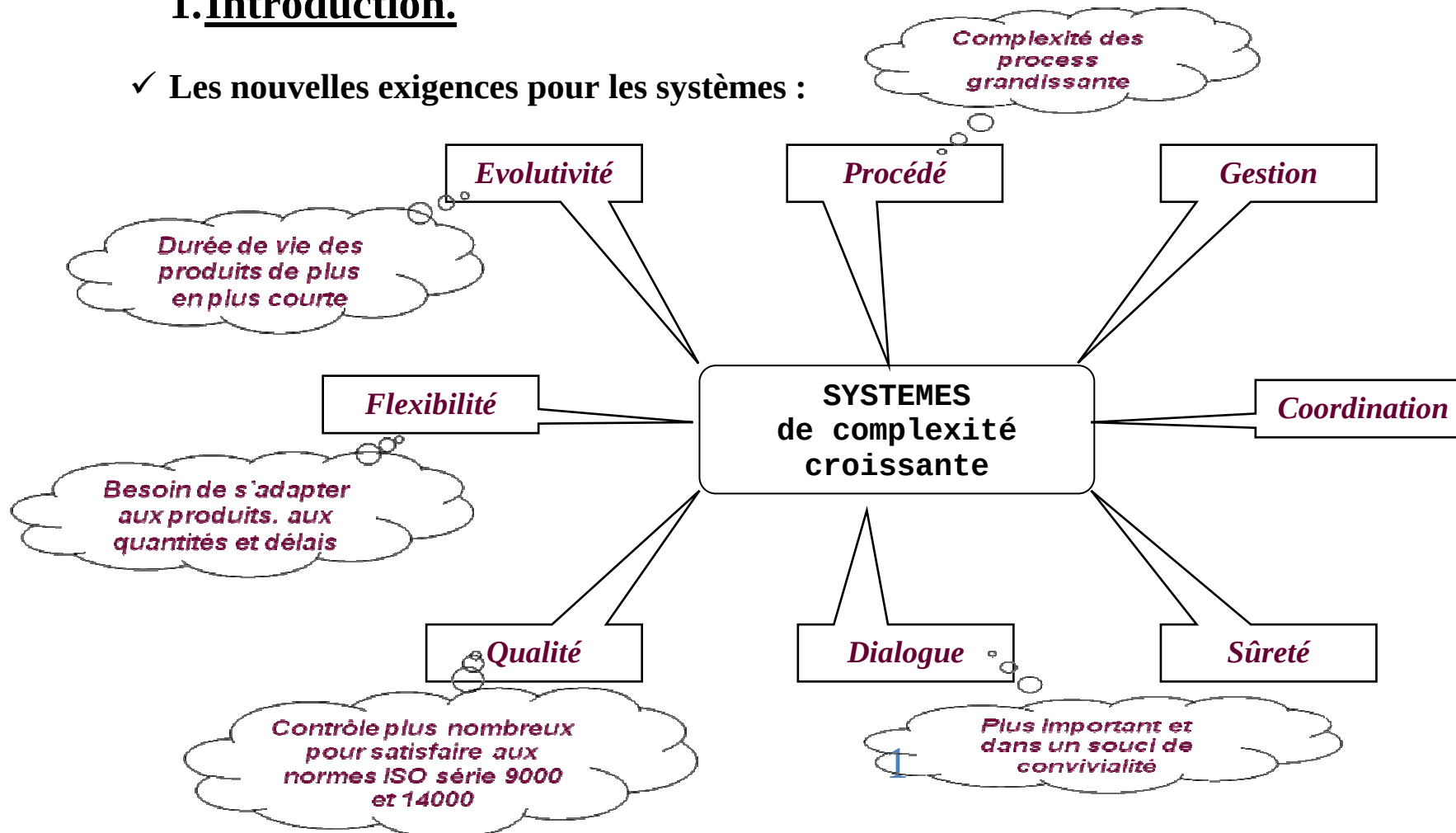
Systèmes numériques Programmables

la possibilité de communiquer

A. Présentation générale

1. Introduction.

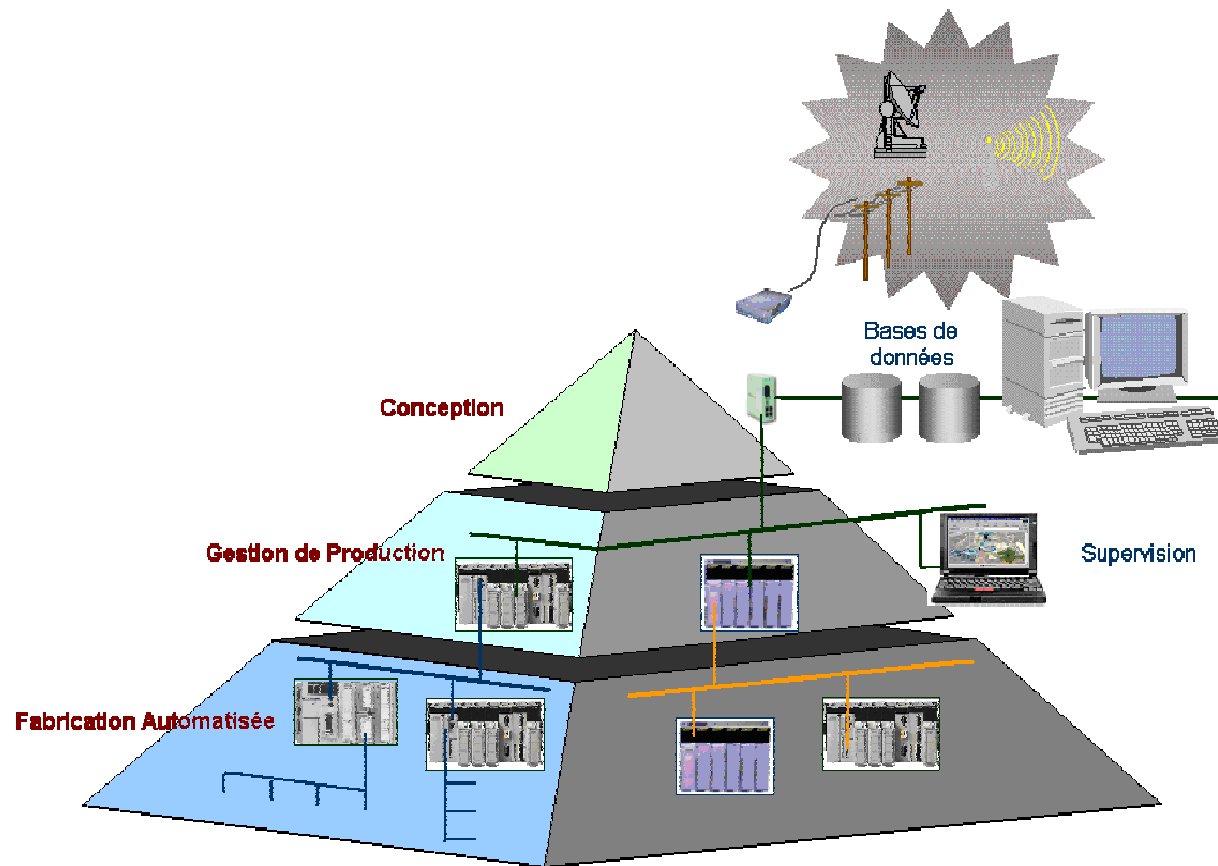
✓ Les nouvelles exigences pour les systèmes :



✓ L 'activité industrielle s'articule autour de **trois pôles majeurs**:

1. La **conception** qui a pour but de générer les données techniques, tels que dossiers d'installations, nomenclatures, gammes de fabrication (CAO, CFAO...).
2. La **Gestion de Production** qui comprend la planification, le suivi de production et des coûts, l'ordonnancement et le traitement des flux, la gestion des données techniques et des stocks.
3. La **Fabrication Automatisée** qui reçoit ses données des deux pôles précédents et qui en retour les nourrit de données réelles tels que constats, bilans, statuts... relatifs aux moyens et aux produits.

Ces différents niveaux dialogue par l'intermédiaire de différents réseaux et bus.



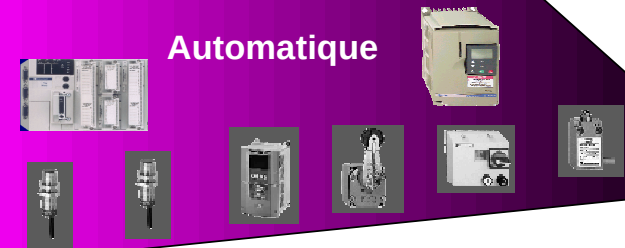
Domaine informatique :

Systèmes de gestion de base de données, fichiers
Échanges à volumes élevés avec des temps de réponse non critique

Segments de données de volumes moyens.
Échanges entre unités de traitement ou de supervision à temps de réponse garantis.
La synchronisation de ces unités exige le traitement sur événement.

Informatique

Automatique



Commande individuelle des processus Automatisés

Traitement des interfaces d'E/S Capteurs - Actionneurs

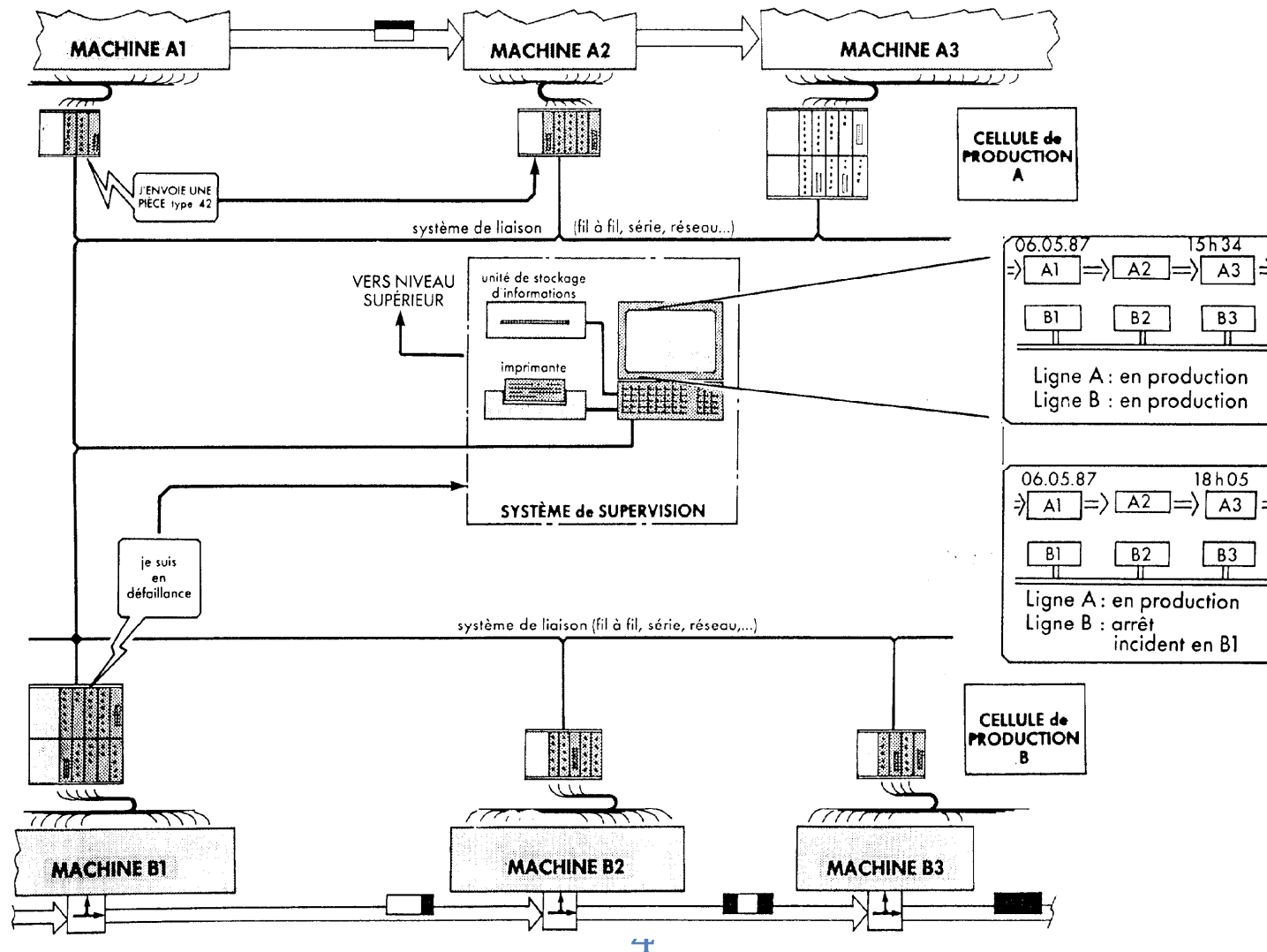
Domaine automatique:

Commande individuelle des processus
Échanges cycliques et événementiels de faible volume

Capteurs et actionneurs
Échanges cycliques de faible volume et à temps de réponse critique.

2. Rôle et intérêt de la supervision.

La supervision industrielle ou supervision d'atelier vous permet de visualiser en temps réel la marche de vos installations, d'avoir une vue globale des différentes consignes et réglages et d'être alerté immédiatement en cas de défaut ou d'alarme.



3. Différents dialogues d'une supervision de production.

1. Assurer la conduite du système en production

lancement de production

le 06.05.87	Cellule production B	
Type 26	Qté	5000
Type 43	Qté	10000
Type 18	Qté	3000

réglage

Type 26 → Type 43
réglages automatiques faits
Poste B2: monter outillage 5347

maintenance préventive

Moteur M4
Cumul de fonctionnement : 3742h
Seuil de révision : 5000h

dialogue de conduite

le 06.05.87 12h38
Marche de préparation cellule B
Préchauffage étuve
Température 85°

2. Faire face aux défaillances des systèmes automatisés

affichage des défauts

le 06.05.87 18 h 27
 arrêt d'urgence B1
 cause : débordement cuve 2
 réaction : fermeture appro. liquide

aide aux diagnostics

défaillance en B1
 arrêt à l'étape 26
 voir fins de course 263 et 266
 voir manostat 370

3. Informer pour faire progresser l'OUTIL et le PRODUIT

journal de marche

○ le 06.05.87 ○
 ○ heure : 9.04 Type 26 Production 5000 ○
 ○ heure : 16.04 Type 43 Production 3422 ○
 ○ arrêt machine B1 18 H 27 ○
 ○ cause sous-ensemble 47E ○

statistiques rebuts

○ Semaine 19.87 Production 7 ○
 ○ Type 1 Qté 43500 rebuts 3% ○
 ○ Type 2 Qté 21100 rebuts 2,1% ○

statistiques arrêts-machines

○ Semaine 19.87		Production 7			○
○ unité de	○ temps	○ défaill.	○ réglage	○ autres	○
○ production	○ fonct./24h				
○ A	○ 89 %	○ —	○ 17 %	○ —	○
○ B	○ 24 %	○ 2 %	○ 4 %	○ —	○

B. Introduction aux Réseaux

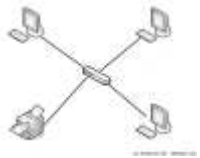
1. Les différentes Topologie physiques des réseaux.

Une topologie physique est en fait la structure physique du réseau. C'est donc la forme, l'apparence du réseau. Il existe plusieurs topologies physiques : le bus, l'étoile (la plus utilisée), l'anneau, le mesh (topologie maillée), l'hybride, etc.

Je vais vous présenter ici que les 3 topologies que nous serons amenées à utiliser.

Classification globale la plus courante à ce jour

a. le réseau local : LAN

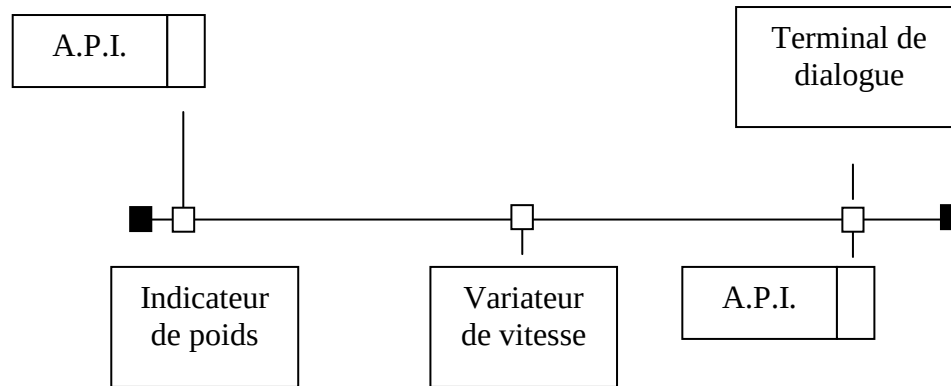


Un LAN, Local Area Network (en français réseau local) est un réseau limité à un espace géographique.

Exemple : l'ensemble des ordinateurs du labo A2I ou d'une habitation ou de machines industrielles forme un LAN.

- **Topologie BUS** ;

Exemple industriel: liaison entre automates et plusieurs outils de traitements



Dans cette topologie, tous les matériels sont connectés entre eux par le biais d'un seul câble appelé **(BUS)** débuté et terminé par des **terminateurs (■)**. Les terminateurs ont pour but de maintenir les signaux électriques de données dans le câble.

Dans cette topologie, étant donné que le câble de transmission est commun, il ne faut pas que 2 machines communiquent simultanément. On utilise alors un protocole particulier d'accès au bus sur chaque machines ou, dans le cas du protocole Télémécanique Uni-Telway, c'est un équipement dédié qui gère les échanges sur un même bus.

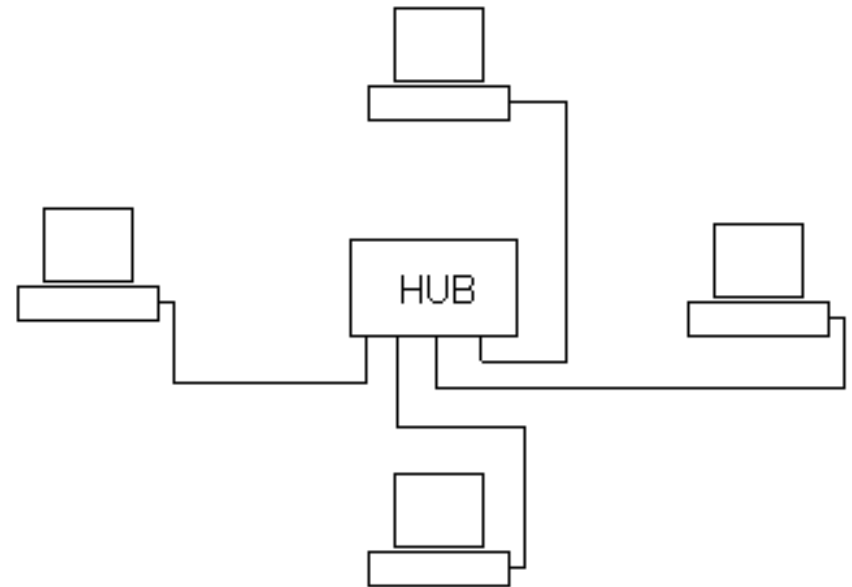
Le principal défaut de cette topologie est que toutes les machines utilisent le même câble, s'il vient à ne plus fonctionner, alors le réseau n'existe plus (panne de mode commun).

- **Topologie étoile** ;

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un matériel appelé **hub** ou **switch**. Il s'agit d'une boîte comprenant un certain nombre de jonctions **RJ-45** auxquelles on peut connecter les câbles en provenance des ordinateurs.

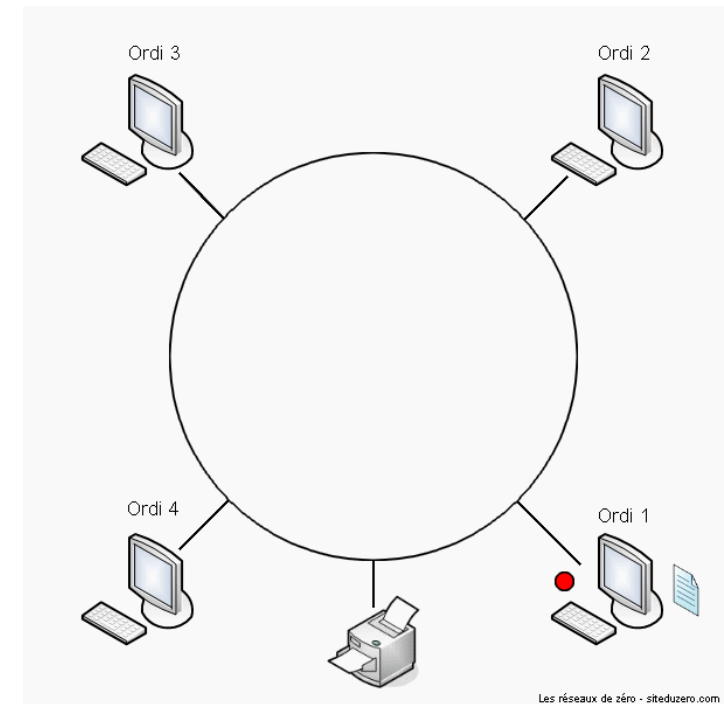
Exemple d'ordinateurs reliés entre eux dans une même salle :

Le principal défaut de cette topologie, c'est que si l'élément central (hub ou switch) ne fonctionne plus, plus rien ne fonctionne : toute communication est impossible (panne de mode commun).

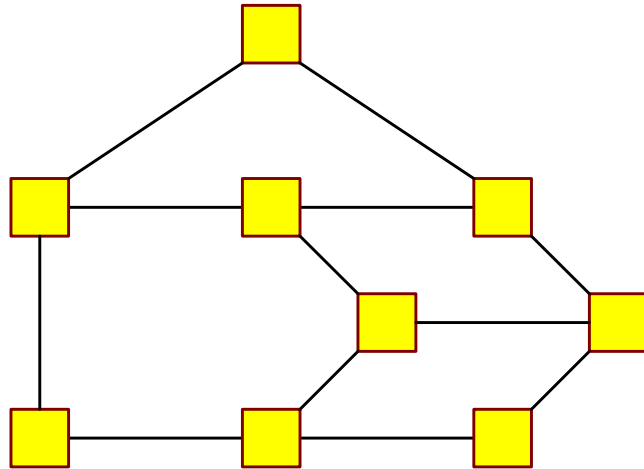


- **Topologie anneau** ;

un réseau en anneau c'est comme un réseau en bus avec les machines disposées en cercle. la topologie de type bus possédait un problème de collision de données (voir ce qui avait été dit au dessus). Ce principe est repris dans le réseau en anneau. Sauf que là, la méthode anticollision différente. Le principe est assez simple : une machine connectée au réseau possède un jeton virtuel. Ce jeton, c'est une **autorisation de communiquer**. Une fois que la machine a transmis ce qu'elle voulait, elle passe le jeton à la machine suivante, et ainsi de suite. Si le détenteur du jeton n'a rien à dire, il le passe au suivant.



b. le réseau étendu : WAN



WAN signifie Wide Area Network, en français, on peut le traduire par "réseau étendu".

Un WAN à une **Topologie hybride** et n'est autre qu'une association de plusieurs LAN de différentes topologies (bus, étoile, anneau ...)

Il répond à des besoins de communication entre **sites géographiques distants**. et peut être vu comme un réseau maillé dans le sens logique du terme.

Les équipements sont reliés entre eux pour former une toile (Web) d'araignée (comme Internet). Chaque nœud a un rôle de « routeur ». Pour atteindre un nœud, les chemins sont multiples et choisis en fonctions de critères comme la disponibilité d'un nœud ou d'un WAN, la qualité de transmission ou la charge ponctuelle sur un tronçon WAN donné.....

2. Les Matériels

Il faut savoir que pour construire un réseau, il faut du matériel pour rendre possible la communication entre les ordinateurs. Voyons dans le cas courant les moyens de connecter des ordinateurs entre eux.

a. Les câbles

Un des médias d'accès les plus utilisés est le câble. Les câbles sont des liaisons physiques entre ordinateurs. Mais il en existe différentes sortes, nous allons en voir 2 principales.

Câble Ethernet

Le câble Ethernet est sûrement le type de câble le plus utilisé pour connecter des ordinateurs entre eux dans un réseau local. Il relie généralement un ordinateur personnel à un routeur (ce que vous connaissez sous l'appellation "box"). Il existe 2 références :

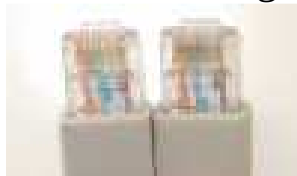
- UTP-CAT5 (débit de 100 mégabits par seconde) **soit $100 \times 2^{20} = 100\,048\,576$ bits/s**
- UTP-CAT6 (débit de 1 gigabit par seconde). **soit $2^{30} = 1\,073\,741\,824$ bits/s**

Il existe ensuite deux catégories de câble Ethernet :

- Les câbles **Ethernet droits** qui servent à relier un ordinateur à un autre appareil comme un routeur, hub ou un switch que l'on abordera plus loin.
- Les câbles Ethernet croisés. Ces derniers permettent de relier directement entre eux deux ordinateurs.

Comment faire pour les reconnaître ?

C'est noté sur l'emballage ou il suffit de regarder les embouts des câbles :



Si les couleurs des fils à l'intérieur des embouts sont dans le même ordre sur les deux *connecteurs* : c'est donc un câble **droit**.

Ces câbles sont appelés communément "**RJ-45**" (c'est le nom de l'embout).

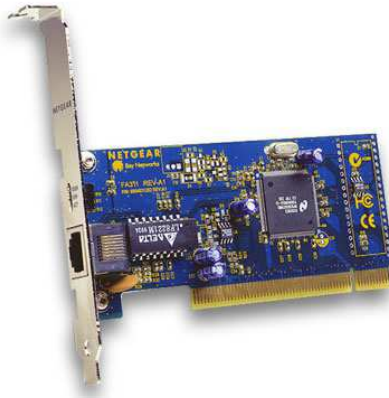
Câble téléphonique

Le câble téléphonique est communément appelé **RJ11** (c'est également le nom de l'embout). C'est ce qui relie le téléphone aux prises en T très courantes en France.

b. la carte réseau

La carte réseau est le composant le plus important, elle est indispensable. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau dans un ordinateur. Elle possède une **adresse MAC** : c'est l'adresse physique de la carte (attribuée à sa fabrication) qui permet d'identifier la machine dans un réseau,

Voici à quoi peut ressembler une carte réseau :



La carte réseau de la photo comporte un port femelle Ethernet : ce port peut accueillir un câble Ethernet mâle (connecteur RJ45). Les cartes réseau internes sont souvent des cartes PCI, c'est à dire qu'elles s'enfoncent dans un port PCI de la carte mère de l'ordinateur.

c. Les boitiers de regroupement

Concentrateur (hub)

Un hub est un matériel qui permet de mettre plusieurs ordinateurs en contact. Ce qu'il fait est tout simple : il reçoit des données par un port, et envoie ce qu'il reçoit aux autres. Il a une interface de réception (un port) et une interface de diffusion (plusieurs autres ports par où les autres ordinateurs sont connectés).



j'ai un hub à 8 ports, avec 5 ordinateurs connectés aux ports 1, 3, 4, 6 et 8 (ici, interface = port). Si l'ordinateur 3 (au port 3) veut communiquer avec les autres, moi le hub, je reçois les données au port 3 (c'est mon port de réception), je les renvoie aux ports 1, 4, 6 et 8 (ce sont les ports de diffusion).

Je ne renvoie plus les données au port 3, car c'est mon port de réception.

Ce qu'on lui reproche est le manque de confidentialité et tout ce qu'un ordinateur lui dit, il l'envoie aux autres. Heureusement, les autres vérifient bien si ça leur est destiné, et si ça ne l'est pas, ils laissent tomber les données et ne les lisent pas.

Remarque : à partir du moment où les données arrivent jusqu'à la carte réseau, elles peuvent toujours être lues (Pb de sécurité informatique).

Commutateur (switch)

Un commutateur fonctionne à peu près comme un hub, sauf qu'il qu'il envoie uniquement au destinataire. Si l'ordinateur 3 envoie des données à l'ordinateur 1, seul ce dernier les recevra et pas les autres ordinateurs. Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le switch se base sur les adresses physiques **MAC** des cartes réseau.



Un commutateur ou switch

Exemple d'adresse MAC :
00 0D C5 D3 1E 04

d. Le routeur

Un routeur ressemble à un switch sur le plan de l'utilisation. En effet, il permet de mettre plusieurs ordinateurs en réseau. Mais cela va plus loin : il permet de mettre en contact 2 réseaux fondamentalement différents.

Si je prends le cas d'une habitation avec plusieurs ordinateurs connectés à une "box".

Cette "box" qui n'est autre qu'un routeur et elle permet :

- De se connecter au réseau Internet (généralement, cela se traduit par un câble branché sur la prise téléphonique) et est la frontière entre le réseau local et Internet.
- Et plusieurs autres interfaces sur lesquels se connectent des ordinateurs voulant accéder à Internet (ça se traduit matériellement par des câbles Ethernet **RJ-45** ou des connexions Wi-Fi).

Notez aussi que le routeur n'est pas uniquement utilisé pour aller sur Internet, on peut l'utiliser aussi dans une communication strictement locale.

Bilan des matériels

Tableau de synthèse du matériel vu et de son utilité :

Matériel	Utilité
Carte réseau	La carte réseau est le matériel de base indispensable, qui traite tout au sujet de la communication dans le monde du réseau.
Concentrateur (hub)	Le concentrateur permet de relier plusieurs ordinateurs entre eux, mais on lui reproche le manque de confidentialité.
Commutateur (switch)	Le commutateur fonctionne comme le concentrateur, sauf qu'il transmet des données aux destinataires en se basant sur leurs adresses MAC (adresses physiques). Chaque machine reçoit seulement ce qui lui est adressé.
Routeur	Le routeur permet d'assurer la communication entre différents réseaux pouvant être fondamentalement différents (réseau local et Internet).

Nous venons d'examiner les composants les plus couramment utilisés pour communiquer avec des ordinateurs. Dans le monde industriel (systèmes de production et d'énergie) on retrouvera les mêmes matériels avec des packagings différents de ceux présentés précédemment.

3. Les adresses de communication.

Pour communiquer, il faut savoir à qui on veut s'adresser et où l'on va !

Dans le point 4 sur le matériel (pg 5 et 6), j'ai parlé d'identification du matériel connecté au réseau par son **adresse MAC** (*adresse physique de la carte réseau attribuée à sa fabrication*).

Le matériel (switch par ex) se base donc sur ces adresses **MAC** pour assurer la communication entre les machines appartenant au même sous-réseau car il est **central**. (*Topologie étoile*)

Par contre, dans un grand réseau, comme un **WAN**, ou même **Internet**, il n'y a pas d'élément central qui connaît l'emplacement du destinataire et qui peut renvoyer les données en conséquence. On utilise alors des **adresses IP** pour faire communiquer des machines de sous-réseaux différents. Ceci n'est possible que grâce à un processus appelé **routing** qui sera expliqué plus loin.

Voilà pourquoi il y a des adresses **IP** et des adresses **MAC**.

a. Adresses MAC : l'adresse relative à la carte réseau

Une adresse **MAC** est donc un identifiant unique attribué à chaque carte réseau. C'est une **adresse physique**. Concrètement, c'est un numéro d'identification composé de 12 chiffres hexadécimaux. Par convention, on place le symbole deux-points (:) tous les 2 chiffres. Une adresse **MAC** ressemble à cela : **00:14:08:18:C3:47**

b. Adresse IP : l'adresse relative au réseau

Une adresse IP n'est "rien d'autre" que l'endroit où habite une machine distante ou sous-réseau de machines (on peut prendre une box avec son réseau d'ordinateurs privé).

Attention : cette adresse est relative au réseau. Une machine n'aura pas forcément la même adresse IP sur un réseau X et un réseau Y sauf si vous bénéficiez d'une **IP fixe**.

Les adresses IP sont le seul moyen d'identification des machines sur Internet et il existe 2 versions du protocole Internet : **IPv4** et **IPv6**.

Chaque version utilise sa propre structure d'adresse IP :

Les "**adresses IPv4**" sont constituées de 4 nombres correspondant à **4 octets** compris entre 0 et 255, séparés par des points. Exemple : 192.168.0.44. De nos jours, ce sont les plus connues.

Les "**adresses IPv6**" sont encore plus complexes : elles sont représentées par une suite de 8 groupes de 2 octets représentés en hexadécimal : 1fff:0000:0a88:85a3:0000:0000:ac1f:8001.

c. Les adresses IPv4

Remarque 1 : En y regardant d'un peu plus près, on peut calculer le nombre de machines que l'on peut identifier à l'aide de cet adressage. Ainsi, on utilise 4 octets, soit 32 bits, soit encore 2^{32} adresses soit un peu plus de 4 milliards d'adresses !!!

Remarque 2 : Comme cette suite de numéros est trop complexe pour l'homme, celle-ci a été traduite par le "nom internet", qui a la même fonction, mais permet d'être plus mémorisable pour l'homme.

- Le nom internet.

Ex : Le nom internet est composé de trois parties séparées par un point .

www.univ-lyon2.fr				
www	.	univ-lyon2	.	fr
serveur (le 3w)		sous domaine (nom de l'entreprise)		domaine (France)

- La segmentation des réseaux

Pour gérer ces milliards d'adresses, on a segmenté cet énorme réseau en différents petits réseaux. Et c'est au sein de ces petits réseaux que l'on donne des adresses aux machines pour leur envoyer l'information. Ainsi, il suffit de connaître l'adresse du réseau pour envoyer l'information à une machine de celui-ci, et c'est à l'intérieur de ce réseau que l'information sera redirigée vers la bonne machine.

(C'est exactement comme lorsque vous envoyez un paquet par la poste, vous mettez le nom de la ville, le paquet arrive à la poste de la ville, et c'est elle qui distribue le paquet à la bonne adresse)

Or l'adressage retenu pour les machines ne définit qu'une seule adresse. On a donc décidé de segmenter cette adresse en deux parties distinctes, l'une pour le réseau, et l'autre pour la machine.

N° de réseau network ID (Adresse réseau)				N° d'hôte host ID (Adresse de l'hôte : machine)		
Classe A	0	7bits		8bits	8bits	8bits
		0 à 2^7-1 soit de 0 à 127		0 à 2^8-1 soit 0 à 255	0 à 2^8-1 soit 0 à 255	0 à 2^8-1 soit 0 à 255
		Soit 128 (2^7) adresses possibles		Soit 16 777 216 (2^{24}) adresses possibles		
Classe B	1	0	6bits	8bits	8bits	8bits
			2^7 à $(2^7+2^5+2^4+...+1)$ soit de 128 à 191	0 à 2^8-1 soit 0 à 255	0 à 2^8-1 soit 0 à 255	0 à 2^8-1 soit 0 à 255
			Soit 16384 (2^{14}) adresses possibles	Soit 65 536 (2^{16}) adresses possibles		
Classe C	1	1	0	5bits	8bits	8bits
				2^7+2^6 à $(2^7+2^6+2^4+...+1)$ soit de 192 à 223	0 à 2^8-1 soit 0 à 255	0 à 2^8-1 soit 0 à 255
				Soit 2 097 152 (2^{21}) adresses possibles		

- **Les masques de sous-réseau** (désigné par subnet mask, netmask ou address mask en anglais) permettent la séparation des deux adresses vues au-dessus.
- Ils permettent de faire la séparation entre les parties adresse réseau et machine d'une adresse IP,
- La partie adresse réseau est représentée par des bits à **1** et la partie adresse machine par ceux à **0**,
- Le masque ne représente rien sans l'adresse IP à laquelle il est associé.

Soit l'adresse IP **172.17.5.232** qui est de classe B car $128 < 172 < 191$ (cf. classes ci-dessus)

L'adresse réseau est obtenue en appliquant l'opérateur ET entre l'adresse IP et le **masque réseau**.

Ex :

	172.17.5.23		10101100.00010001.00000101.11101000
	2		
	ET 255.255.0.0	ET	11111111.11111111.00000000.00000000
Adresse réseau	172.17.0.0		10101100.00010001.00000000.00000000

L'adresse machine à l'intérieur du réseau est quant à elle obtenue en appliquant l'opérateur ET entre l'adresse IP et le **complément** du masque.

Ex :

	172.17.5.23		10101100.00010001.00000101.11101000
	2		
	ET 0.0.255.255	ET	00000000.00000000.11111111.11111111
Adresse machine	0.0.5.232		00000000.00000000.00000101.11101000

Question : Calculer le nombre d'adresses possibles de machines dans ce sous-réseau sachant que le système d'adressage impose de réserver 2 adresses :

2 adresses réservées soit **0** et **65535**

$2^{16}-2 = 65534$ soit les adresses :1 (00000000.00000001) à 65534 (11111111.11111110)

➤ Faire Cours_6 EX1

4. Les protocoles de communication.

Pour que des machines puissent communiquer entre elles, elles doivent respecter certains **protocoles**. En français, on dit qu'un protocole **est un ensemble de règles qui définissent comment se produit une communication dans un réseau.**

➤ **Le protocole : un genre de pilote**

Un protocole joue un peu le même rôle qu'un pilote pour un périphérique d'ordinateur (imprimante souris ...). Sans un pilote, votre souris d'ordinateur ne peut pas fonctionner, elle ne peut pas communiquer avec le système. Vous comprenez donc que le pilote est l'interface de communication entre le système et le matériel, il en est de même pour le protocole.

➤ **Le protocole : un genre de langue**

Communiquer est l'une des activités les plus courantes. Les personnes qui communiquent ne peuvent se comprendre que dans deux cas :

- Si elles parlent la même langue
- Si elles ont un intermédiaire qui parle leur deux langues respectives (rôle d'interprète)

En réseau, c'est la même chose. La langue que les humains parlent, c'est un **protocole de communication** pour les hôtes dans un réseau.

Quant à l'interprète de notre exemple, dans un réseau, ce sera la **passerelle** (applicative) qui permettra de faire communiquer deux réseaux basés sur des protocoles différents.

4.1 Les exigences d'un protocole

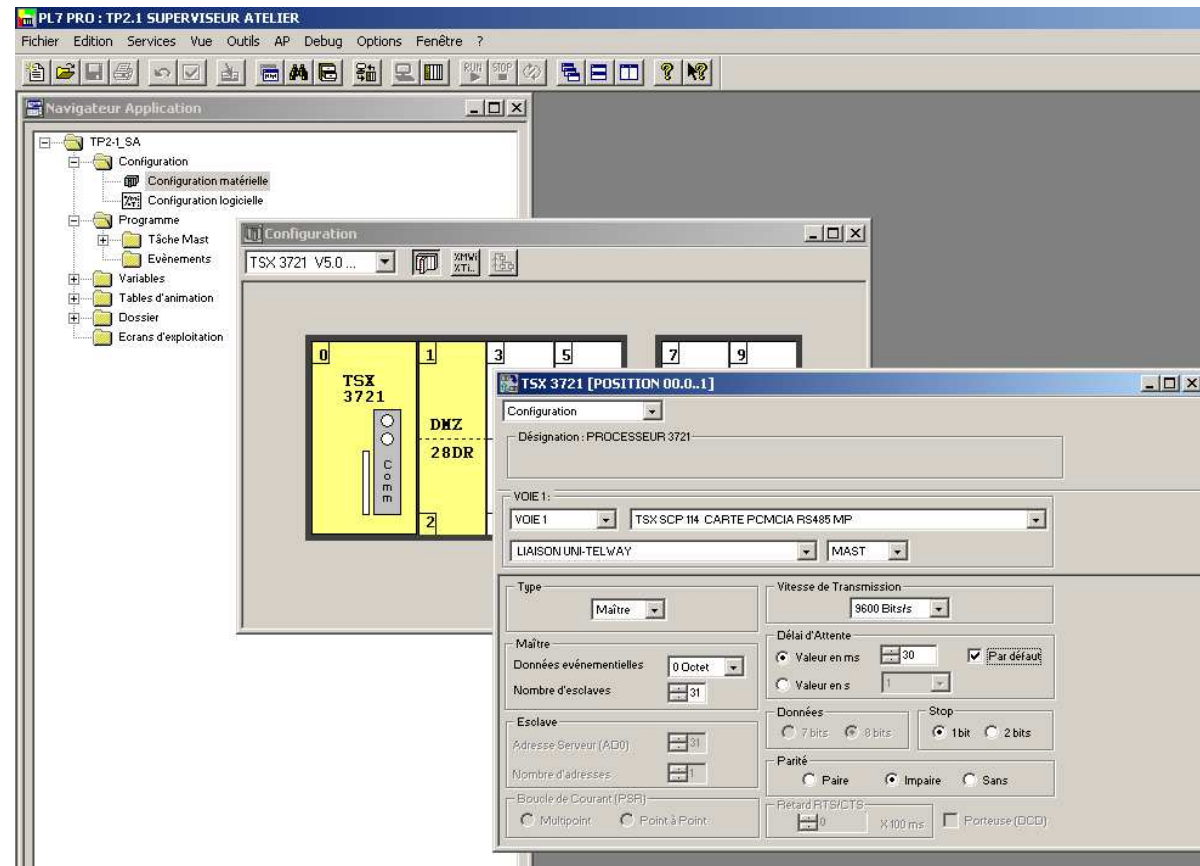
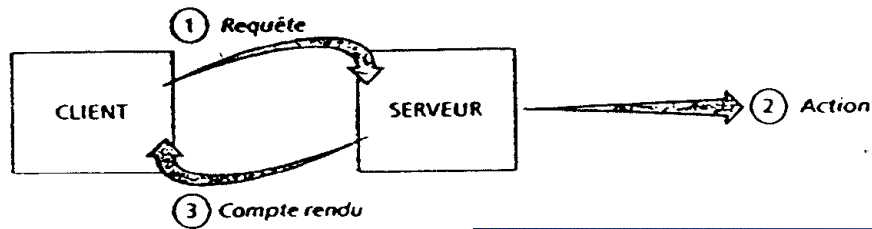
Un protocole est un ensemble de règles dictant comment doit s'effectuer la communication entre deux entités. Il existe plusieurs exigences qu'un protocole de communication doit être capable de remplir :

- **La gestion du format des données** : Qui dit communication dit échanges de données. Le protocole doit permettre de gérer le format des données à transmettre. En général, les données seront constituées de deux choses : d'une entête et du contenu. L'entête sera un plutôt réservée au protocole (*c'est à ce niveau que l'on trouve des informations techniques*).
- **La gestion du format d'adresses** : Durant la procédure de transmission, il faut gérer les adresses : qui est l'émetteur, qui est le récepteur (*destinataire*). Analogie : Quand on écrit une lettre papier, dans l'entête, on met l'adresse de l'émetteur et celle du destinataire, et même sur l'enveloppe d'ailleurs. Si on ne le fait pas, on ne sait pas à qui envoyer la lettre, et celui qui la reçoit ne sait même pas si elle lui est destinée (*de qui elle provient*).
- **Correspondance d'adresses**: Quand vous inscrivez l'adresse du destinataire sur une enveloppe, cette dernière est "logique" dans ce sens que le destinataire n'habite pas sur cette enveloppe, mais cette adresse indique l'adresse physique du destinataire. Le facteur doit donc faire une correspondance entre cette adresse logique sur l'enveloppe et l'adresse physique. Par analogie, un protocole doit assurer des fonctions de correspondance entre les adresses logiques (**IP**) et les adresses physiques (**MAC**).

- **Routage** : le routage consiste à « diriger » les données entre deux réseaux d'un plan d'adressage différent.
- **Détection d'erreurs de transmission** : Il se peut qu'une erreur se produise dans la procédure de transmission des informations. Un protocole doit donc être en mesure de détecter ces erreurs.
- **Accusé de réception** : Quand vous recevez un mail, très souvent vous y répondez. Cette réponse informe explicitement à l'émetteur que vous avez reçu son mail. C'est en quelque sorte un accusé de réception. Certains protocoles permettent donc à un hôte récepteur d'informer un hôte émetteur qu'il a reçu le paquet envoyé pour empêcher ce dernier de renvoyer les mêmes choses. D'autres protocoles n'ont pas cette fonction.
- **La gestion de perte d'informations** : De même que des erreurs peuvent se produire lors de la transmission, il peut y avoir des pertes d'informations. Quand un paquet met trop du temps à arriver à son destinataire, "il se perd". Voilà pourquoi c'est important qu'un protocole gère la reconnaissance des paquets. Si l'hôte-récepteur B répond dans un intervalle de x secondes à l'hôte-émetteur A, ce dernier saura alors que B a bien reçu les données, dans le cas contraire ce dernier peut en conclure que les données « se sont perdues ».
- **La direction du flux d'informations** : A et B peuvent-ils communiquer simultanément ?
 - o Si oui, il s'agit d'un système de communication **full-duplex**.
 - o Si non, il s'agit d'un système de communication **half-duplex**.

- **Contrôle de séquences** : Toute information envoyée sur un réseau est segmentée en plusieurs « séquences » qui peuvent arriver « en désordre », ou même en double (s'il y a eu des retransmissions). Grâce au contrôle de séquences d'un protocole, on peut « numéroter » chaque « morceau » afin que le destinataire sache les « remettre en ordre » ou supprimer les doublons.
 - **Gestion de flux** : Quand deux personnes parlent, il est nécessaire de donner à celui qui "écoute" le temps de comprendre ce qui est dit, puisqu'il se peut que l'émetteur parle plus vite que le récepteur. Il faut donc gérer cette volubilité de flux. Dans les réseaux, il y a des cas où un hôte-émetteur peut transmettre plus vite que ne peut recevoir un hôte-récepteur. C'est là qu'intervient l'utilité de la gestion des flux.
- Voir ***Illustration dans le cas d'une communication industrielle de type LAN :***
Uni Telway de télé mécanique en annexe 2

Illustration dans le cas d'une communication industrielle de type LAN :
Uni Telway de télémécanique



Toutes les exigences citées précédemment **ne peuvent pas être réalisées par un seul protocole**. Il s'agit d'une suite protocolaire, une suite de protocoles. Il y a des protocoles qui s'occupent de la transmission, d'autres du routage, etc.

Vous avez déjà entendu l'expression «**TCP/IP** » ? En fait, c'est deux protocoles : l'un TCP et l'autre IP. Donc TCP/IP est un empilement de protocoles (*protocol stack en anglais*).

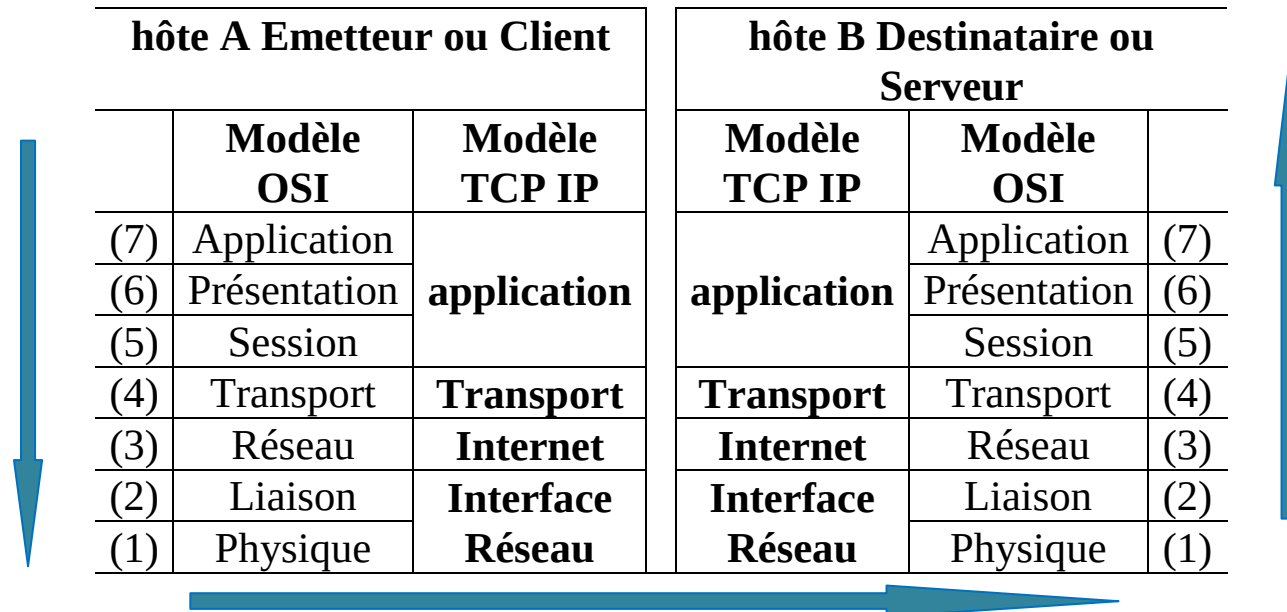
Les constructeurs informatiques ont proposé des architectures réseaux propres à leurs équipements. Par exemple, IBM a proposé SNA, DEC a proposé DNA... Ces architectures ont toutes le même défaut : du fait de leur caractère propriétaire, il n'est pas facile de les interconnecter, à moins d'un accord entre constructeurs. Aussi, pour éviter la multiplication des solutions d'interconnexion d'architectures hétérogènes, l'ISO (International Standards Organisation composé de 140 organismes nationaux de normalisation), a développé un modèle de référence appelé modèle OSI (Open Systems Interconnection). Ce modèle décrit les concepts utilisés et la démarche suivie pour normaliser l'interconnexion de systèmes ouverts (un réseau est composé de systèmes ouverts lorsque la modification, l'adjonction ou la suppression d'un de ces systèmes ne modifie pas le comportement global du réseau).

4.2 Du modèle protocolaire OSI vers le protocole TCP IP. (Comparaison)

Service réalisé	Modèle OSI	Modèle TCP IP
Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier (FTP), la messagerie (SMTP pour l'envoi d'un mail) ..	Application	application
Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises (l'aspect « visuel » de l'information). Un de ses services est la conversion d'un fichier codé vers un fichier codé en ASCII (American Standard Code for Information Interchange).	Présentation	
Cette couche organise et synchronise les échanges entre tâches distantes qui doivent communiquer. La couche session du modèle OSI vous permet principalement d'ouvrir une session, de la gérer (reprise du dialogue après une panne) et de la clore.	Session	
Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message dans le sens réception. Elle modifie également l'en-tête des données en y ajoutant des informations, parmi lesquelles les numéros de ports de la source et de la destination. Le protocole le plus utilisé à ce niveau est bien sûr TCP .	Transport	Transport
Cette couche précise l'adresse IP du récepteur. Elle se charge du routage (ou relai) des données du point A au point B et de l'adressage. L'en-tête subit une nouvelle modification. Il comprend désormais l'en-tête ajouté par la couche de transport + l'adresse IP source et l'adresse IP destinataire. Le protocole le plus utilisé à ce niveau est bien sûr l' IP .	Réseau	Internet
Cette couche fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquiescement renvoyées par le récepteur.	Liaison	Interface Réseau
La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu à 1)	Physique	

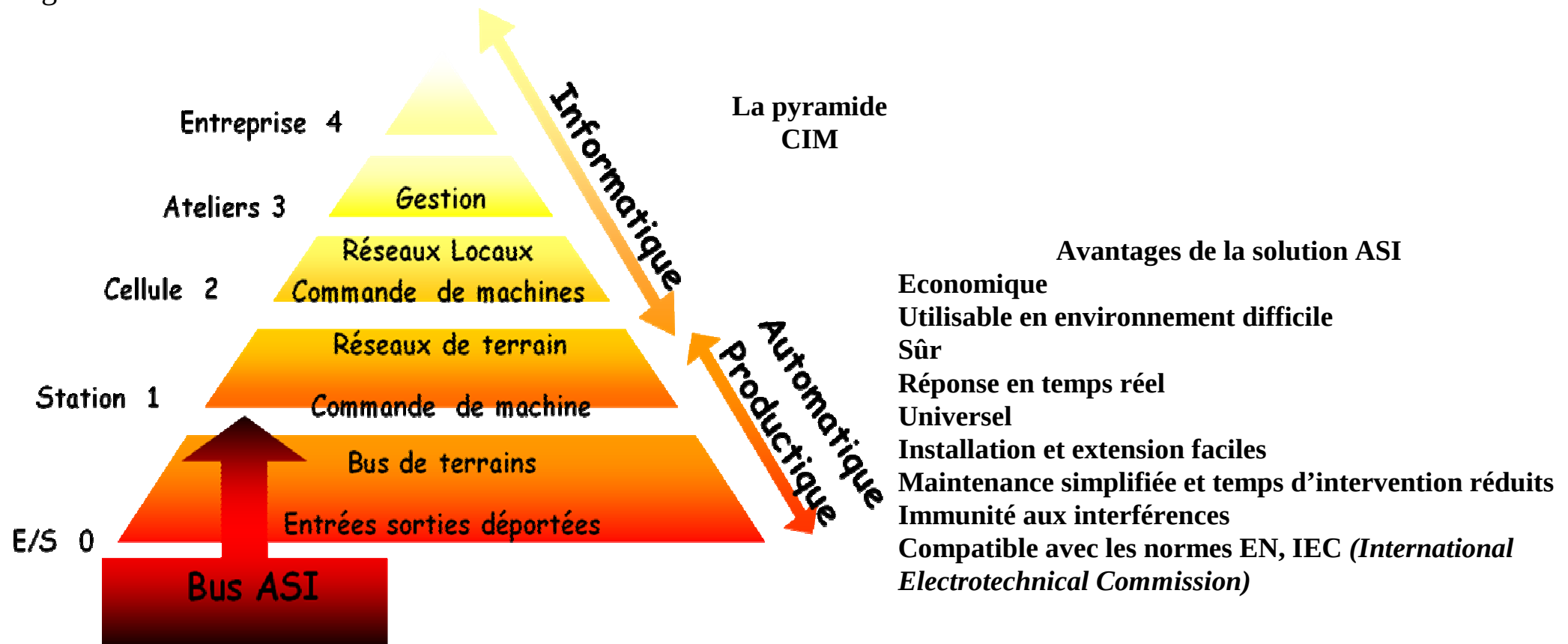
➤ Processus de transmission/réception

Quand un hôte A envoie un message à un hôte B, le processus d'envoi va de la couche 7 (application) à la couche 1 (physique). En revanche, quand il s'agit de recevoir, le message emprunte le chemin inverse : il part de la couche 1 (physique) pour arriver à la couche 7 (application).



C. Bus industriel à vocation Automatique.

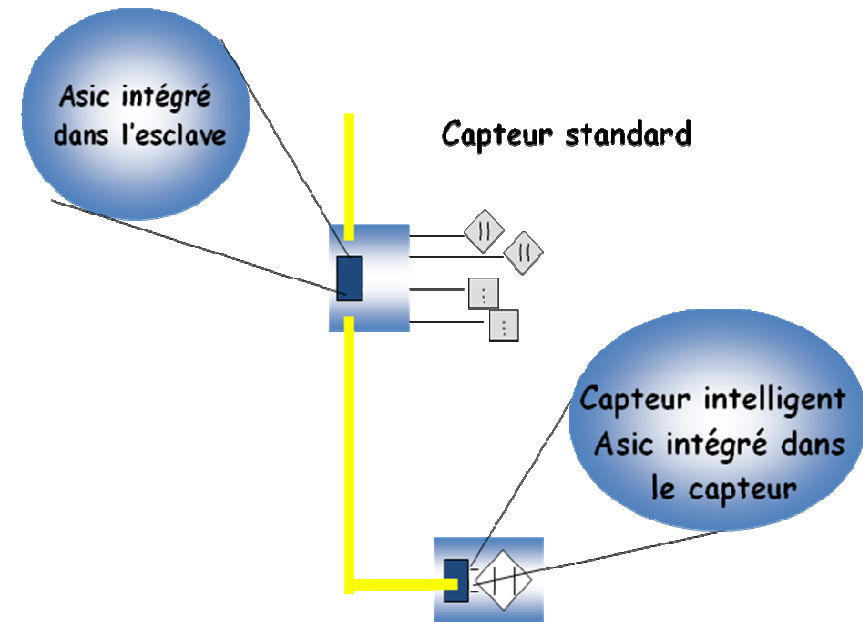
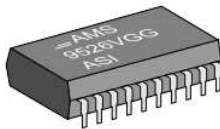
AS-Interface a été développé afin de minimiser les coûts de connexion des capteurs, des actionneurs et des systèmes intégrés.



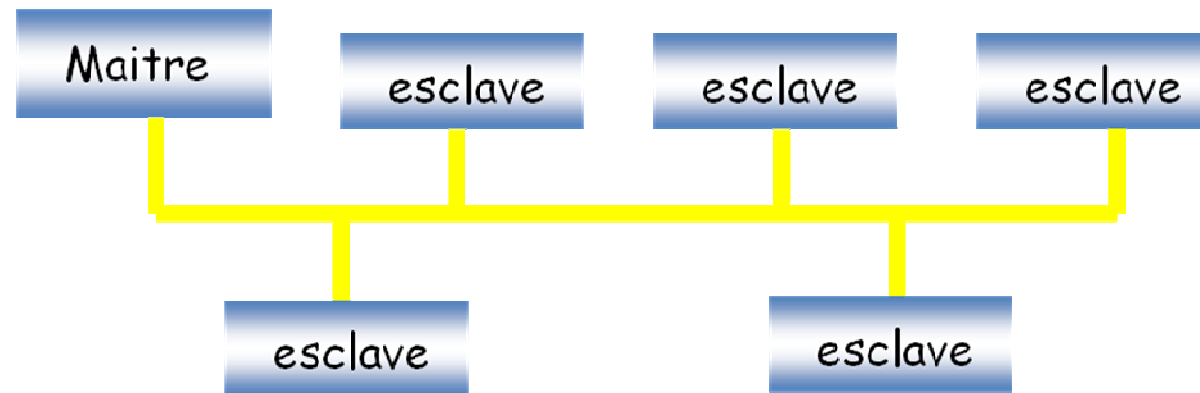
Principe Général

L'intelligence est en partie regroupé dans un CI (circuit intégré) spécifique situé :

- soit dans les récepteurs: *constituants communicants*
- Soit dans un module qui accepte des récepteurs traditionnels : *constituants non communicants*



La Topologie ASI :

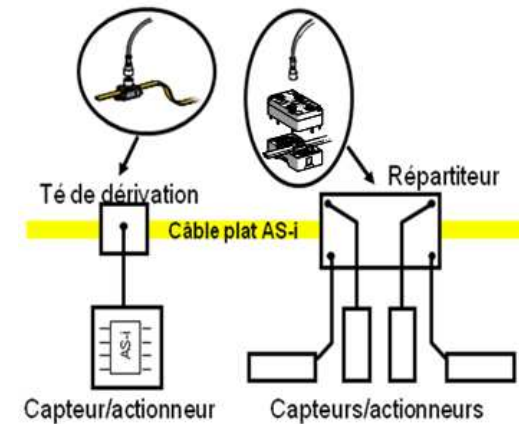
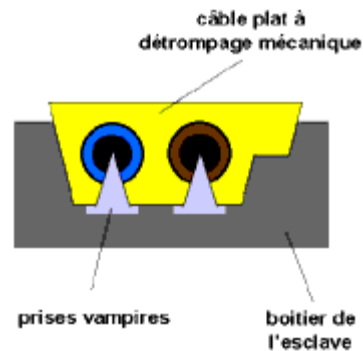


Le BUS ASI :

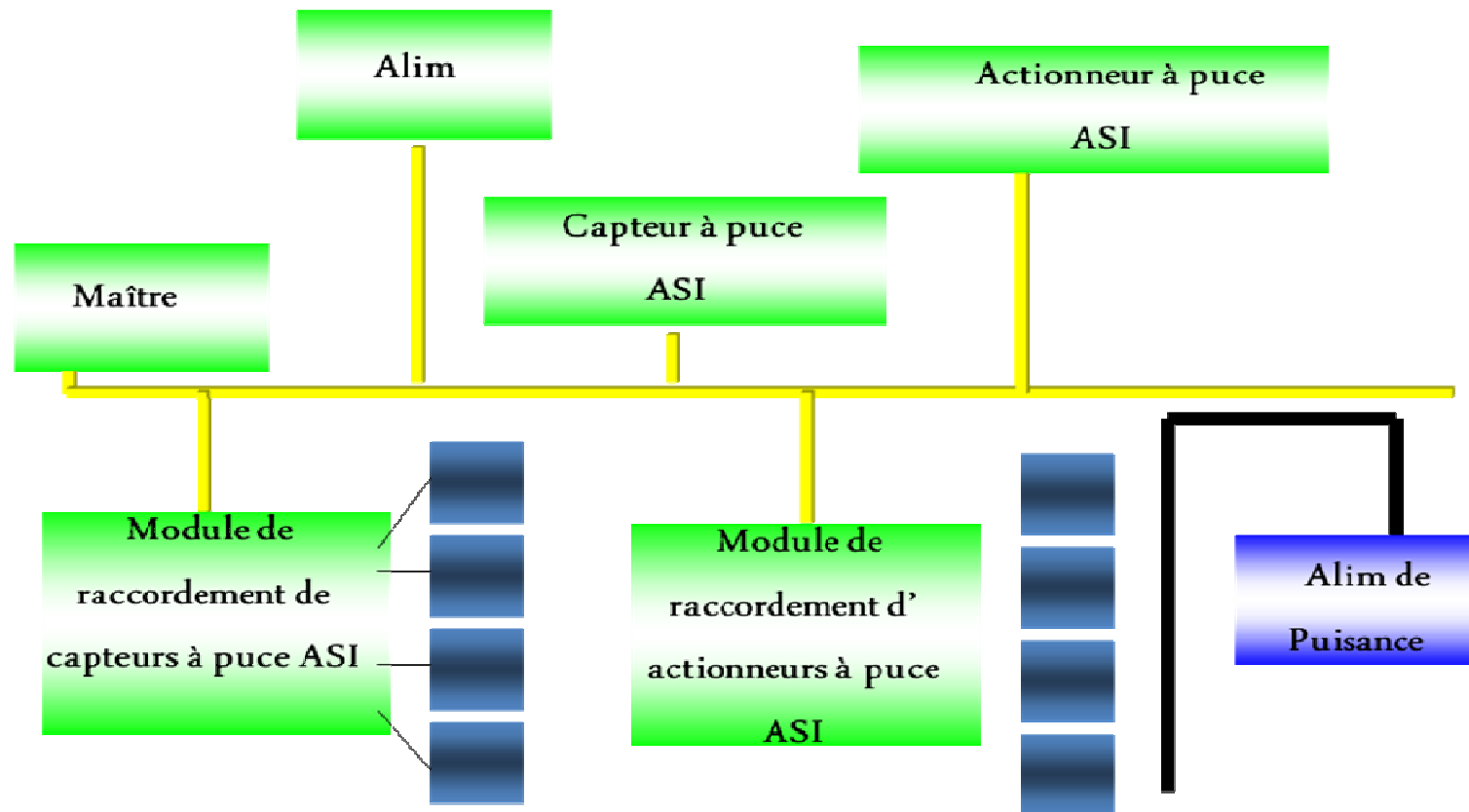
Un seul câble pour alimenter les entrées et le transfert des données. transmission données et puissance sur 2 fils non blindés, non torsadés

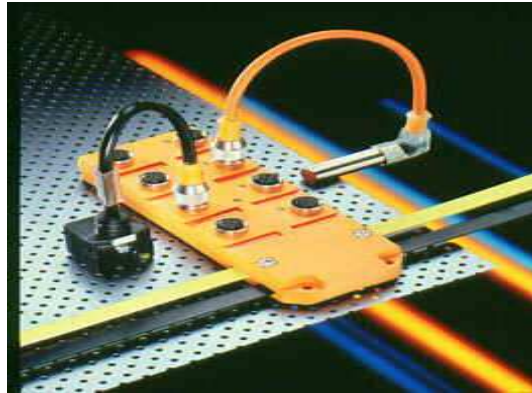
Normalement, l'information et la puissance sont transmises sur le même câble jaune.

Remarque: Si l'esclave consomme plus de puissance, vous pouvez utiliser une alimentation auxiliaire avec un câble noir séparé, utilisant le même système de raccordement



Que trouve-t-on sur le bus ?





Exemple d'architecture d'un réseau industriel :

- 1 TBX SAP 10 :
- 2 TBX BLP 01 :
- 3 TBX FP ACC 4 :
- 4 TSX FP ACC 12 :
- 5 TSX FP CA 00 :
- 6 TSX FP CG 00 :
- 7 TSX SUP A0 :
- 8 XZ-SDE1113 + XZ-SDP :
- 9 XZ-SDE1103 + XZ-SDA00D00 :
- 10 XZ-CG0020 :
- 11 ABE-8000S00 :
- 12 LFe-P ou LFe-M :
- 13 XS7-C40AS101 ou XS8-C40AS101 :
- 14 XUJ-000000AS :
- 15 XAL-S200 :
- 16 XBL-C50120581 :
- 17 XZ-CB10001 :
- 18 XZ-CG0122 :
- 19 ATV 58EU000 :

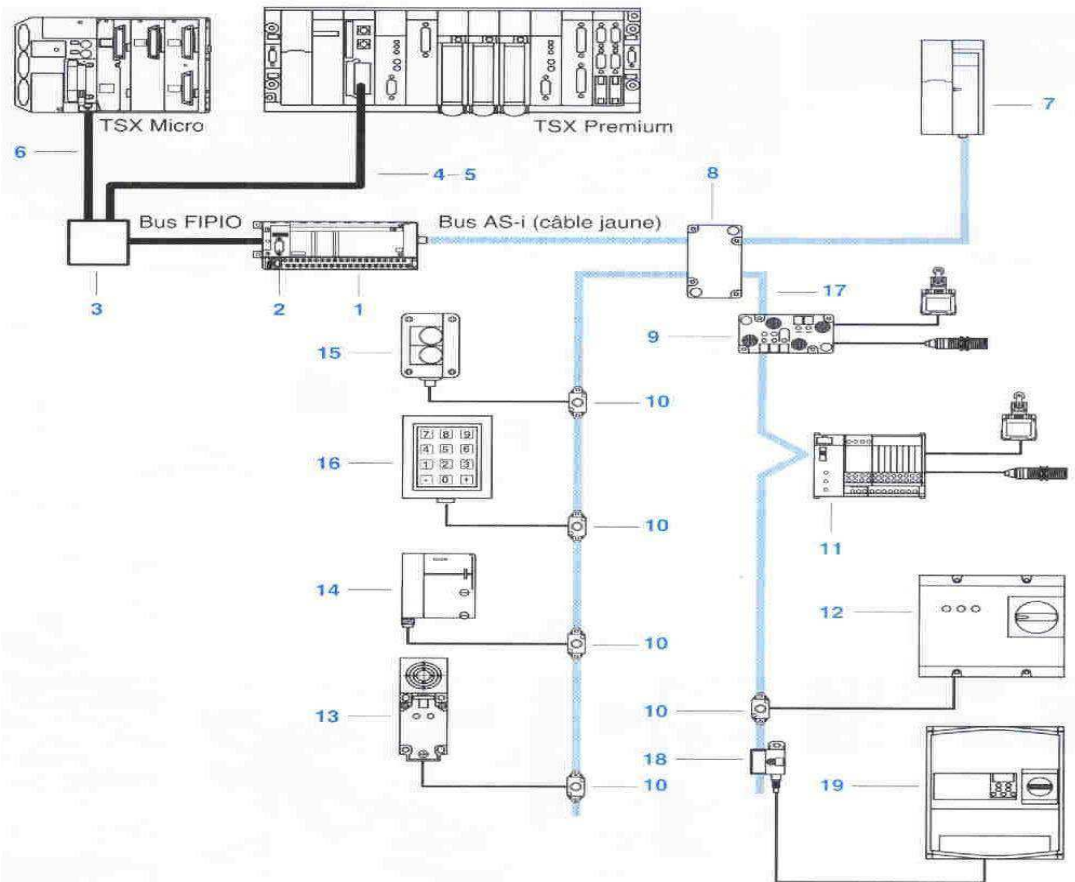
Module passerelle FIPIO/AS-i.
Connecteur de raccordement pour modules TBX SAP 10.
Boîtier de dérivation du câble principal et de connexion de deux équipements. Il possède en plus un connecteur Sub-D 9 points pour le raccordement d'autres équipements (FTX, CCX...).

Connecteur Sub-D 9 points pour raccordement sur TSX Premium.
Câble principal, paire torsadée blindée 150 Ω (diamètre 8 mm).
Câble avec connecteur Sub-D 9 points pour raccordement sur TSX Micro avec carte PCMCIA TSX FPP 10.

Module d'alimentation pour l'ensemble des capteurs/actionneurs du bus AS-i.
Répartiteur passif permettant le raccordement par prises vampires de deux câbles AS-i.
Répartiteur actif, constitué d'un module de connexion + un module utilisateur, permettant le raccordement de capteurs ou actionneurs traditionnels (2E/2S, 4E, 4S).

Tête de raccordement sur le bus par prise vampire.
Interface de raccordement Telefast SB2, permettant le raccordement de capteurs ou actionneurs traditionnels.
Démarreur direct un ou deux sens de marche en coffret.
Détecteur de proximité inductif, corps débrochable et tête orientable 5 positions.

Détecteur photoélectrique, type compact XUJ.
Boîte à boutons, avec deux poussoirs éventuellement lumineux.
Clavier 12 touches à effet tactile.
Câble plat jaune pour bus avec profil spécial permettant d'éviter les inversions de polarité, constitué de 2 conducteurs, non torsadés, non blindés.
Dérivation pour câble plat.
Variateurs de vitesse pour moteur asynchrone Altivar 58.



Le Fonctionnement :

Il est de type « maître / esclaves »

Le maître : C'est l'entité intelligente qui gère les échanges sur le bus AS-i.

Ce sont les entités "communicantes" reliées au bus (31 au maximum par segment AS-i).

Les esclaves :

Ce sont des capteurs, des actionneurs, des répartiteurs ou des constituants de dialogue ou de signalisation.

Ils échangent des tables d'entrées et/ou de sorties d'une longueur fixe de 4 bits avec le maître.

Un esclave = une adresse AS-i.

Caractéristiques générales :

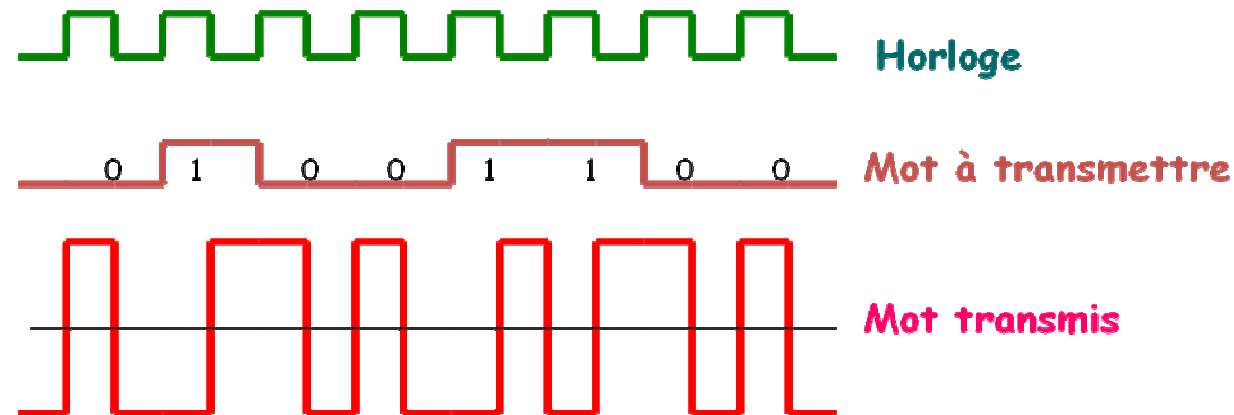
1 seul maître pour 31 esclaves maximum.

4 entrées et / ou 4 sorties TOR par esclave. (Soit au max de 248 (8x31) capteurs ou actionneurs TOR)

Réseau de longueur limitée à 100 m. Si plus long, il faut utiliser des Repeteur.

Communication par interrogation cyclique de tous les participants.

Energie : 24VDC, jusqu'à 8A

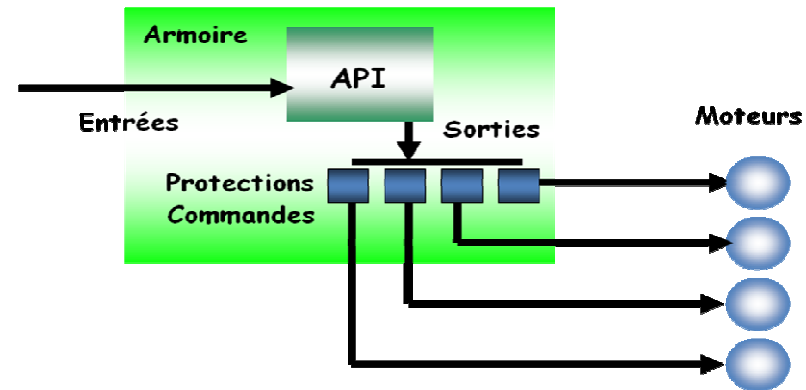


On réalise un OU EXCLUSIF entre le signal d'horloge et le mot à transmettre,

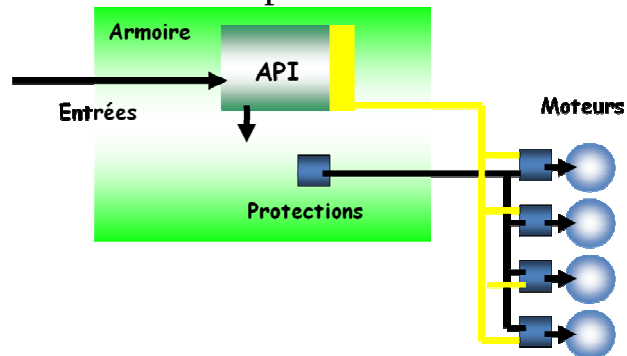
L'information se retrouve dans le front observé au milieu du bit de donnée soit sur le front de descente de l'horloge.

Exemples d'application :

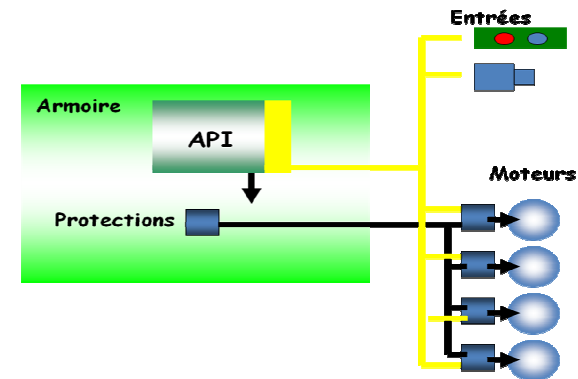
Solution traditionnelle :



Solution traditionnelle pour les entrées et décentralisée pour les sorties.

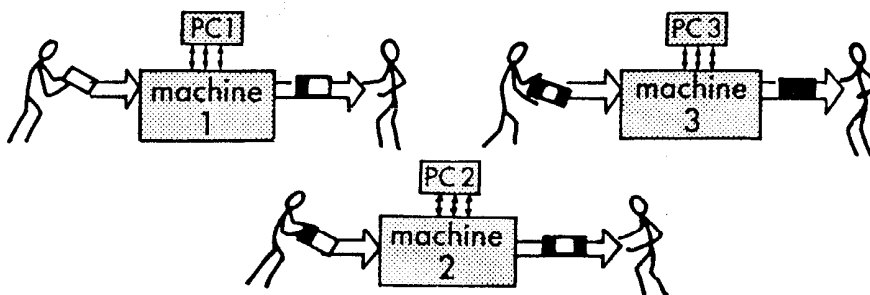


Solution décentralisée entrées /sorties:

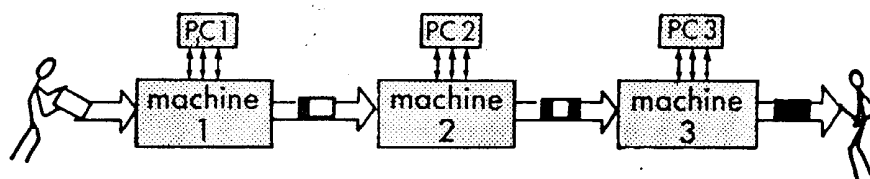


Machines autonomes

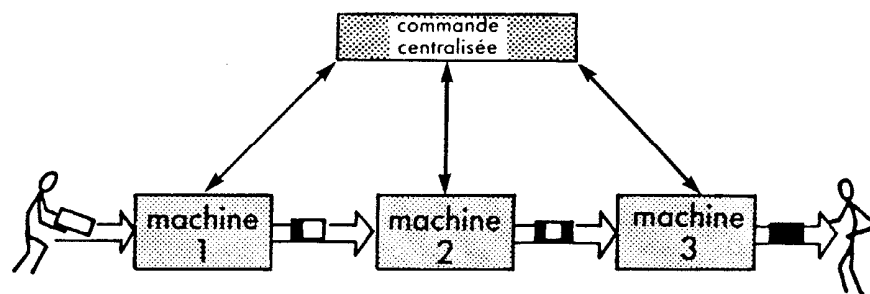
Chaque machine réalise une étape dans l'élaboration du produit. La manutention entre machines, les chargements et déchargements sont nombreux, coûteux et longs. Ils sont le plus souvent manuels.

**Machines associées en ligne**

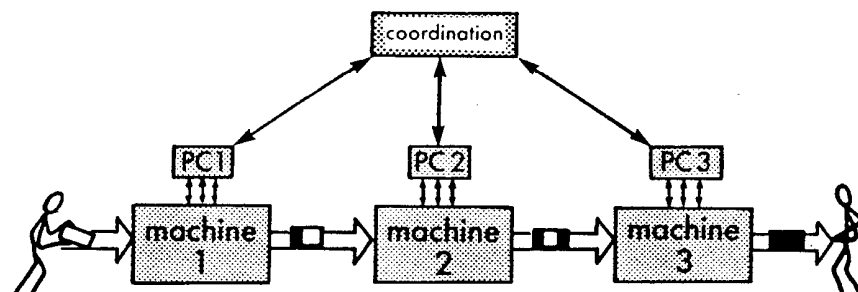
Ici, le produit passe automatiquement d'une machine à la suivante. Dans ce cas simple, c'est le transfert du produit lui-même qui assure la liaison entre machines.

**Cellule de production à commande centralisée**

La nécessité de coordonner l'action des machines a d'abord conduit à centraliser leurs commandes, ce qui par ailleurs a compliqué les interventions locales de réglage et de dépannage.

**Cellule à C^{de} décentralisée et coordonnée**

Un retour aux commandes décentralisées s'est imposé, mais avec une coordination entre machines ici assurée par liaisons inter-niveaux.

**Cellule flexible à C^{de} répartie et hiérarchisée**

- Le besoin de flexibilité conduit à prévoir des transferts libres de produits de machine à machine : une machine donnée peut traiter ou non, le produit présenté.
- Par ailleurs, pour la commande de la cellule, des liaisons, iso-niveau complètent les liaisons inter-niveaux qui assurent la communication avec la supervision, puis éventuellement vers un niveau supérieur.

