

Introduction aux Réseaux et Communications Industriels

(Bus de terrain)

Buses de communication dans la pratique

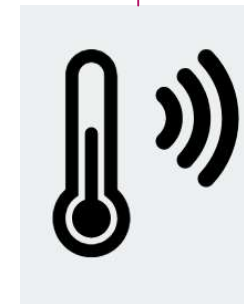
Exemple 1 :



Bus de
communication

Contrôle, Diagnostic et
lecture de données de capteurs

Actionneur



Capteur

Système Electronique
Complexe

Buses de communication dans la pratique

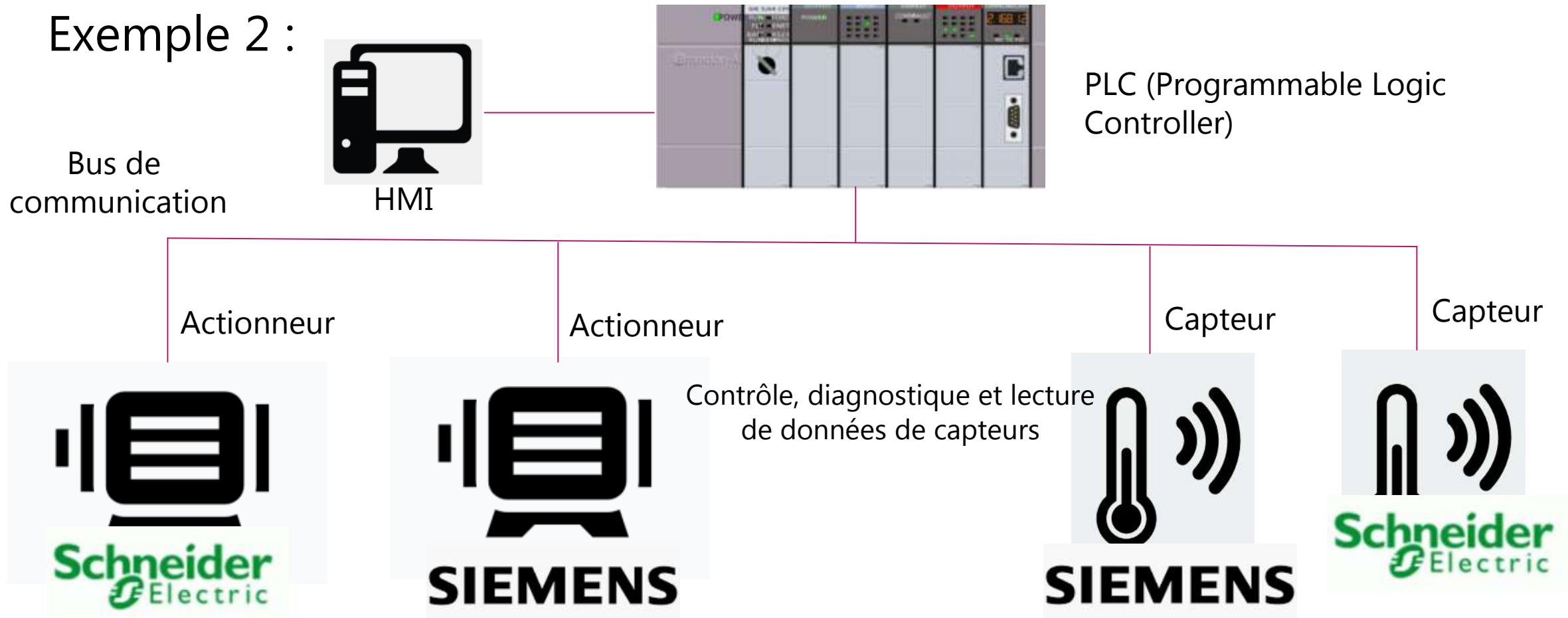
Exemple 1 :



Scanner Automobile

Buses de communication dans la pratique

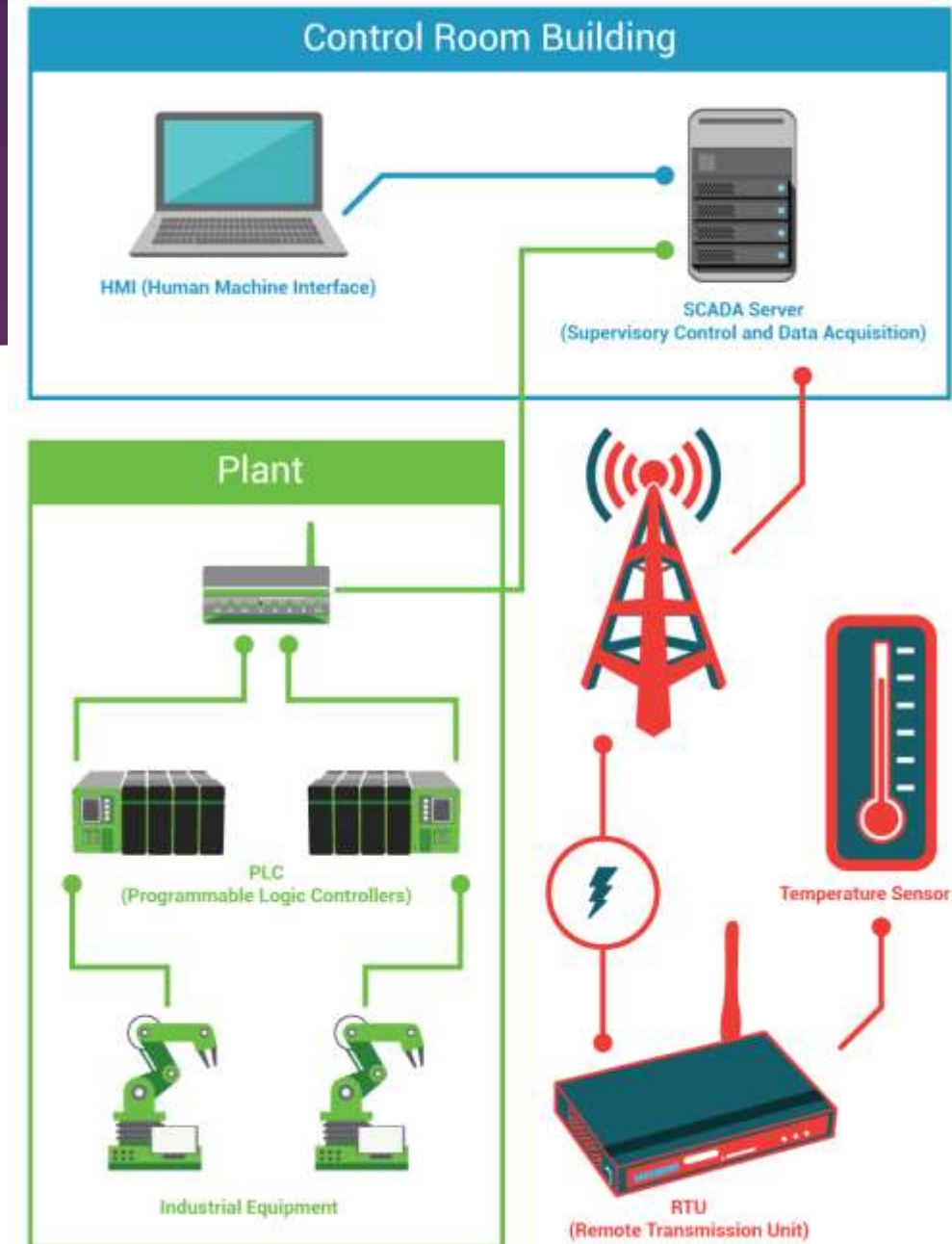
Exemple 2 :



Buses de communication dans la pratique

Exemple 2 :

Système SCADA
(Supervisory control and data acquisition)



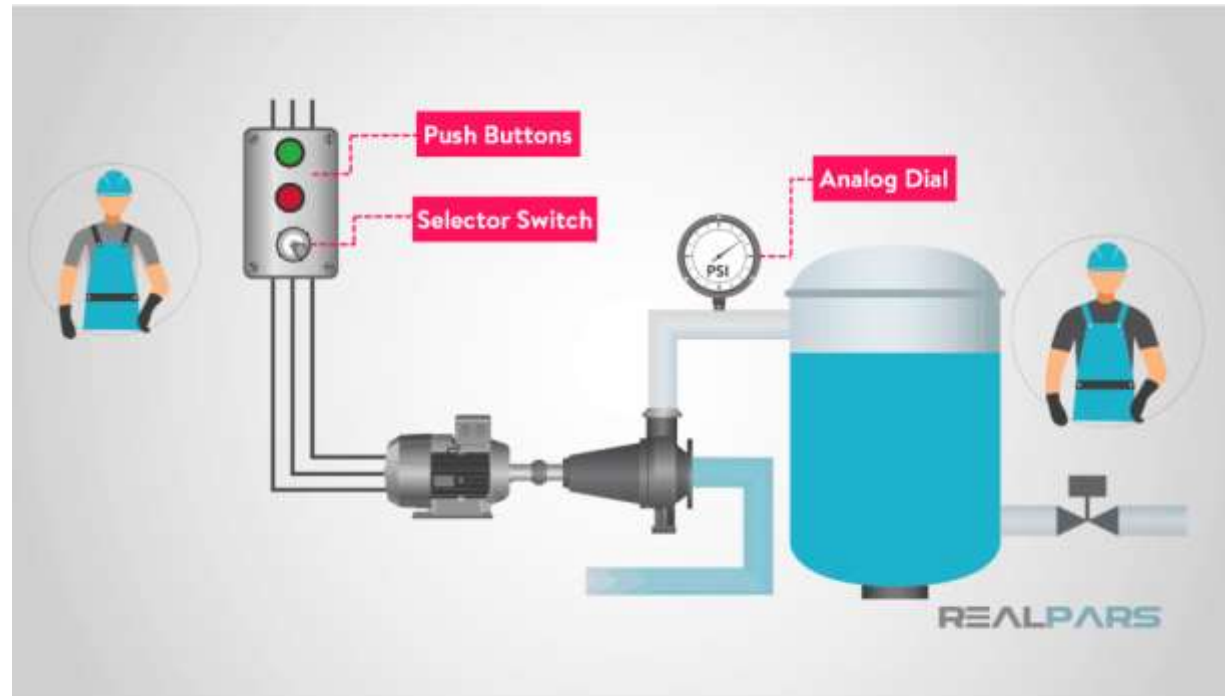
Buses de communication dans la pratique

Exemple 2 :



Buses de communication dans la pratique

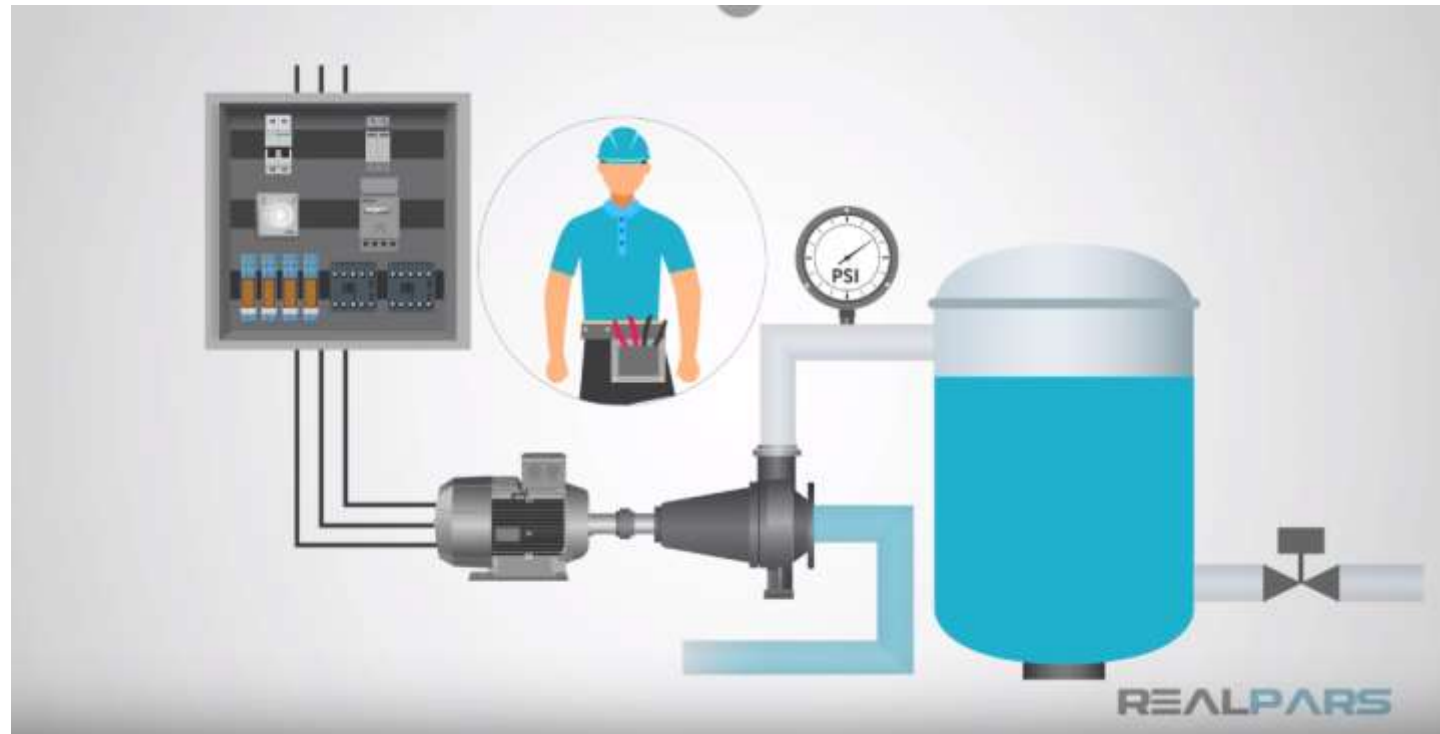
Exemple 2 :



Avant SCADA

Buses de communication dans la pratique

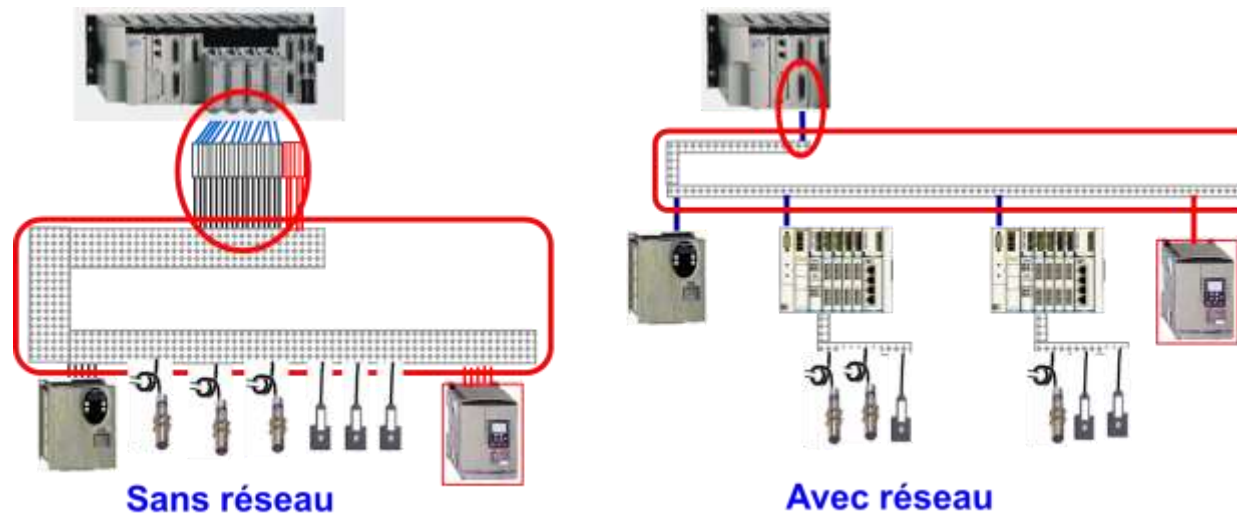
Exemple 2 :



Avant SCADA

Buses de communication dans la pratique

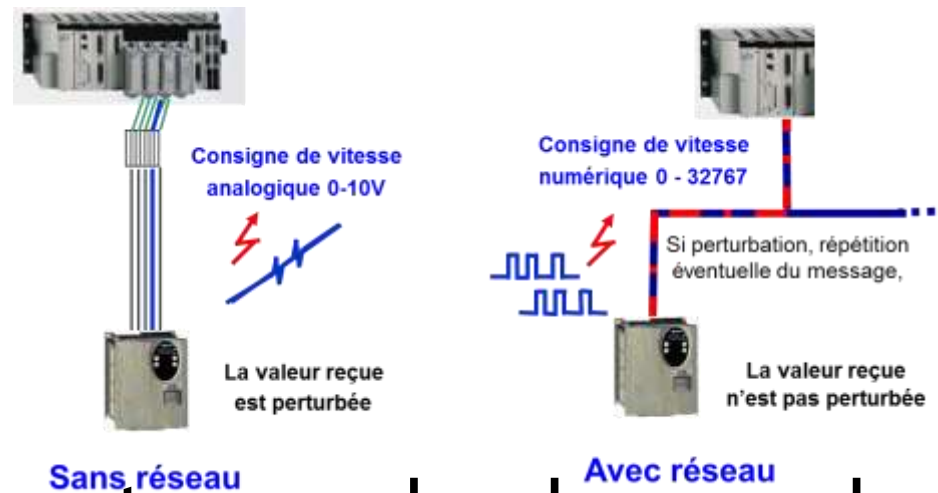
Exemple 2 : Réduction des coûts d'installation



Les avantages des buses de terrain dans SCADA

Buses de communication dans la pratique

Exemple 2 : Diminution de la sensibilité aux perturbations électromagnétiques



Les avantages des buses de terrain dans SCADA

Buses de communication dans la pratique

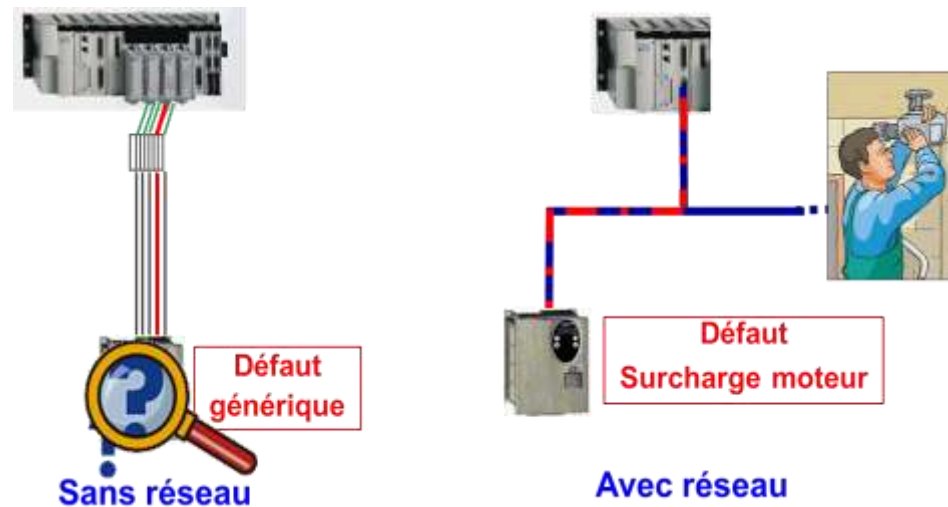
Exemple 2 : Répartition possible de l'intelligence



Les avantages des buses de terrain dans SCADA

Buses de communication dans la pratique

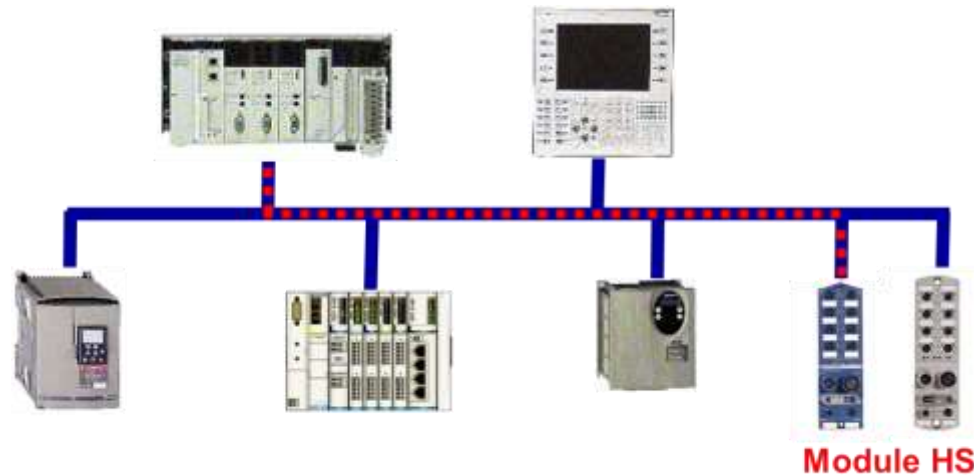
Exemple 2 : Précision du diagnostic en cas de défaut



Les avantages des buses de terrain dans SCADA

Buses de communication dans la pratique

Exemple 2 : Remplacement d'équipements défectueux
facilité



Les avantages des buses de terrain
dans SCADA

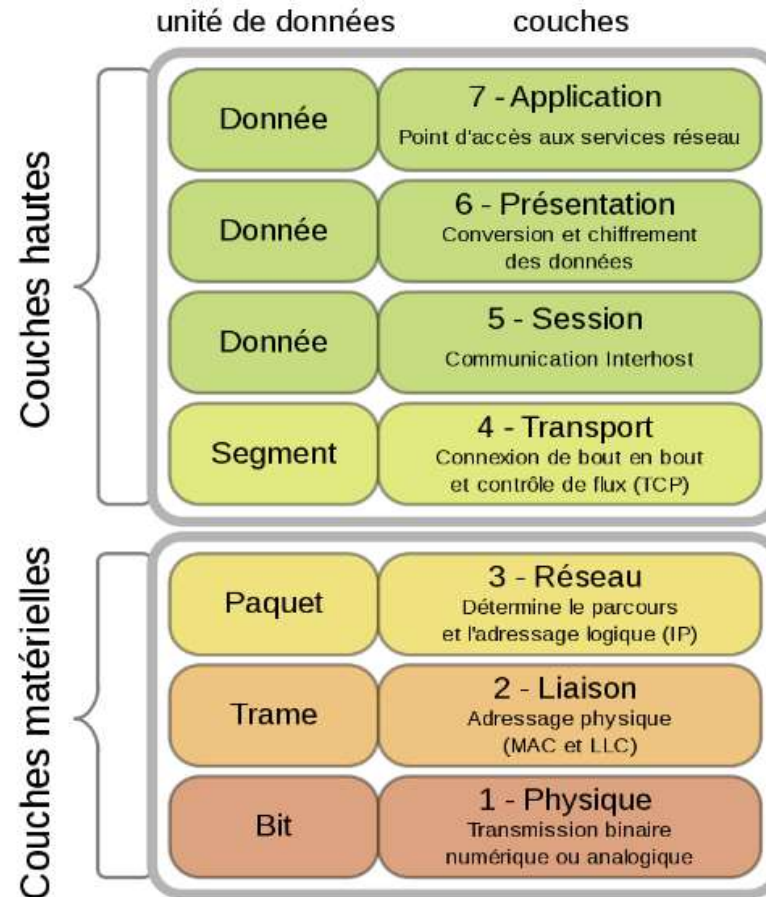
Un définition des bus de terrain

- ▶ **Terrain** : Espace géographique limité.
- ▶ **Bus** : Ensemble de conducteurs commun à plusieurs circuits.
- ▶ **Réseau** : bus ou ensemble de bus répartis sur un terrain.

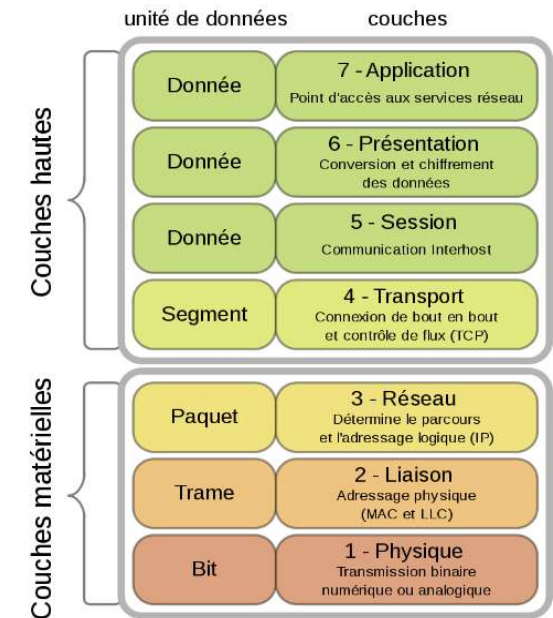
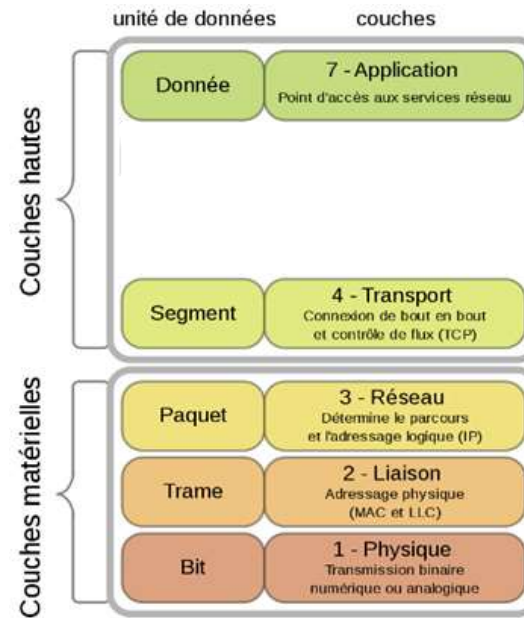
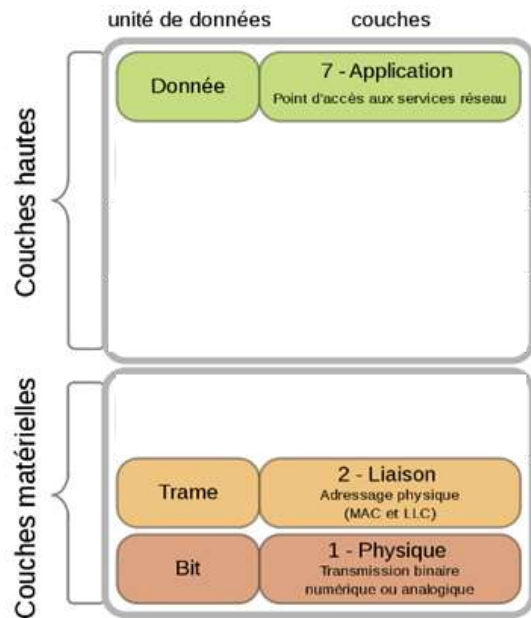
Un **bus de terrain** est donc un système de communication entre plusieurs ensembles communiquant dans une zone géographique limitée (capteurs, calculateurs, automates, actionneurs, ...)

Couches OSI et Bus de terrain

- Les protocoles de bus de Communication se trouvent au niveau Application.

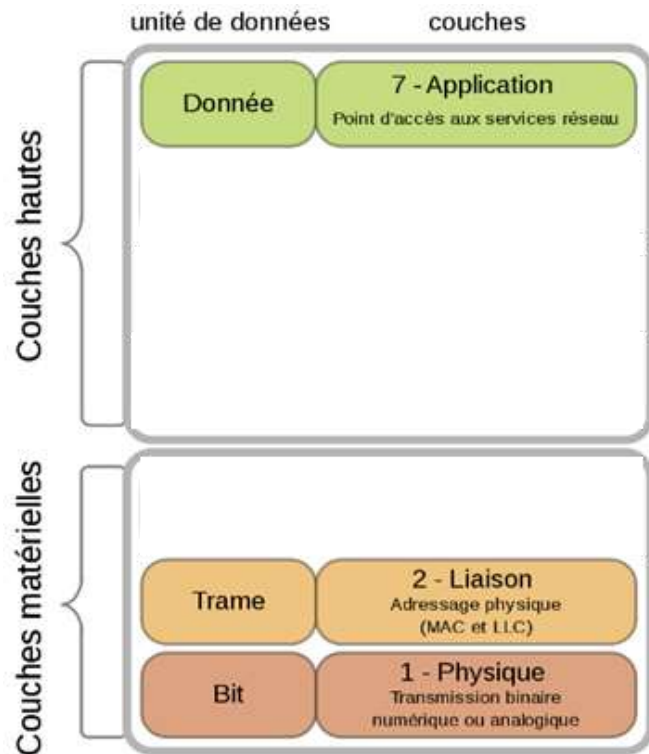


Couches OSI et Bus de terrain



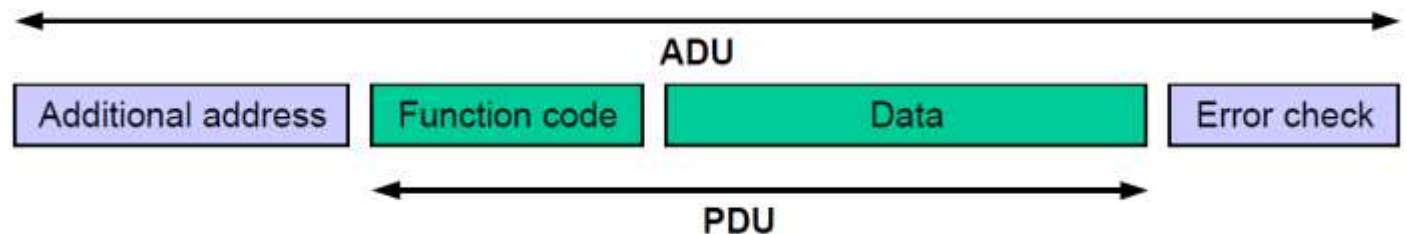
Plusieurs utilisations possibles

Couches OSI et Bus de terrain

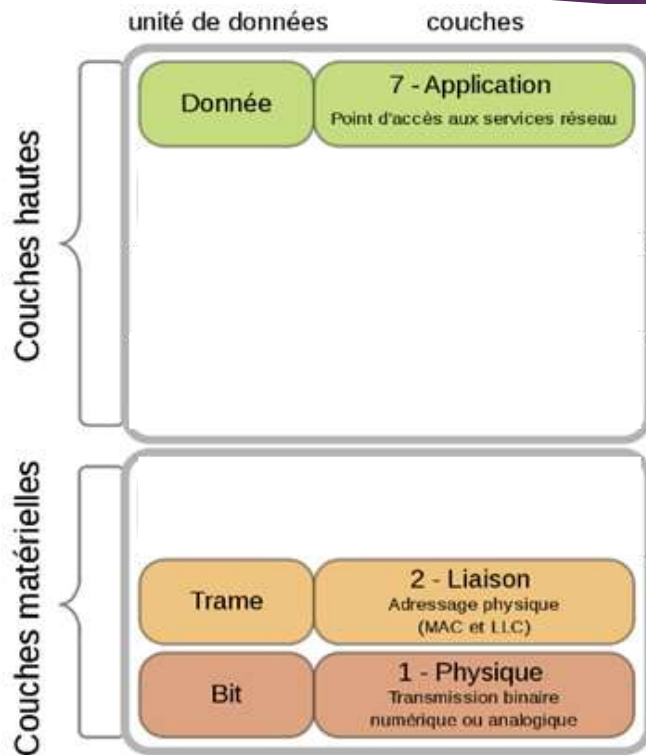


Modbus Over RS232 (Communication point-à-point)

Modbus fournit un modèle de trame. Pas d'adressage physique.



Couches OSI et Bus de terrain

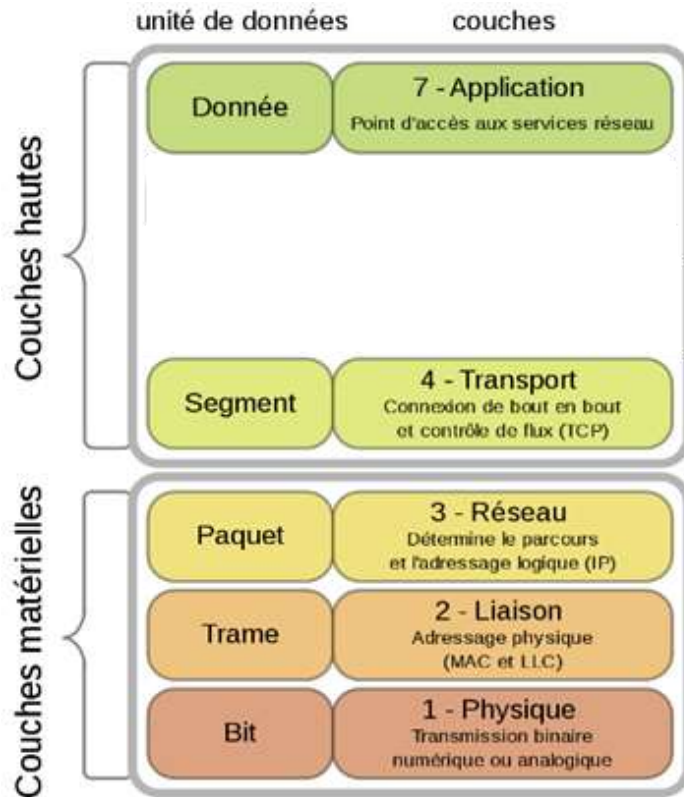


Modbus Over RS485 (Communication en bus), EtherCat, Bus CAN

Modbus/Ethercat/Bus CAN fournissent un modèle de trame. Adressage physique avec MAC pour EtherCat, Attribution Id pour Bus Can, et Unit Id pour ModBus. Bus CAN inclut une gestion de collision.

La communication en Bus de terrain majoritairement utilise les 2 premières couches.

Couches OSI et Bus de terrain



Modbus Over TCP/IP ou UDP/IP, CANOpen, EtherCat sur TCP/CP

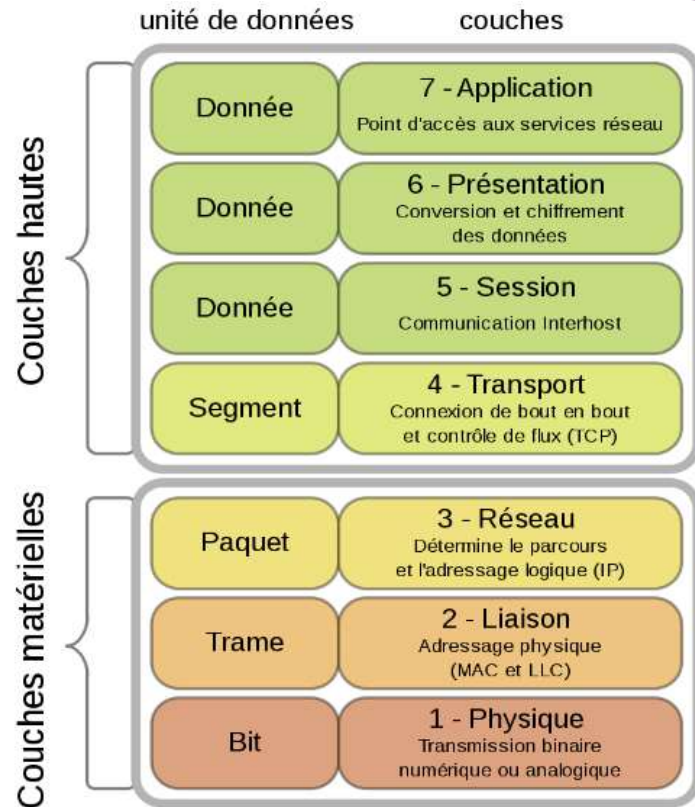
Le contrôle d'erreur, segmentation/Désegmentation, contrôle de flux sont fournis par TCP

L'adressage logique et le routages sont fournis par IP.
Modbus fournit aussi l'adressage dans certains cas.

Ethernet fournit un modèle de trame et gère les collisions.



Couches OSI et Bus de terrain



Modbus Over TLS

TLS gère le chiffrement.

TLS gère l'authentification.

Le contrôle d'erreur, segmentation/Désegmentation, contrôle de flux sont fournis par TCP

L'adressage logique et le routages sont fournis par IP.

Modbus fournit aussi l'adressage dans certains cas.

Ethernet fournit un modèle de trame et gère les collisions.

Couches OSI et Bus de terrain

Life Is On

Schneider Electric

Welcome to the Schneider Electric Blog
Global Specialist in Energy Management and Automation

Log in

f in t y

Search

Machine and Process Management

Modbus Security – New Protocol to Improve Control System Security

 Daniel Desruisseaux | August 30, 2018 | 8,713 views

eMail

452

Share

3

Tweet

Like 0

In August of 2018, Modbus.org published the Modbus Security protocol. The use of secure protocols is a fundamental component in efforts to secure [Industrial Control System](#) (ICS) traffic. Secure protocols can mitigate many common cyber-attacks, including replay and man in the middle exploits.



Visit our NEW Internet of Things Center

Go

Life Is On

Schneider Electric

Featured Bloggers


Peter Harbeck


Murali Tejada


Anna Varygina


Guest Blogger

[View the Blogger Directory](#)

Additional Resources

[Schneider Electric IoT Homepage](#)

Couches OSI et Bus de terrain

The new protocol will provide robust protection through the blending of Transport Layer Security (TLS) with the traditional Modbus protocol. TLS was selected as it is a well-known, widely accepted internet standard. TLS will encapsulate Modbus packets to provide both authentication and message integrity protection. The new protocol leverages X.509v3 digital certificates for authentication of the server and client. The protocol also supports the transmission of role based access control information utilizing an X.509v3 extension to authorize the request of the client. Modbus Security will utilize a new port – traditional Modbus uses port 502, the new Modbus Security protocol will utilize port 802.

Protocol interoperability was demonstrated in May of 2017 at an interoperability event attended by four Modbus.org member companies. Products leveraging the new protocol are expected to be available in the market in by 2020. For more information, refer to the [Modbus.org website](https://modbus.org).

Couches OSI et Bus de terrain

SECURITY

Experts assess damage after first cyberattack on U.S. grid

Blake Sobczak, E&E News reporter

Energywire: Monday, May 6, 2019



Reports of an unprecedented grid "cyber event" caused a stir last week in power sector and cybersecurity circles.
(Ian Mutton/Flickr)

Last week, the U.S. power sector marked a sober milestone: an anonymous Western utility became the first to report a malicious "cyber event" that disrupted grid operations.

The hack itself occurred two months ago, on March 5, when a "denial-of-service" attack disabled Cisco Adaptive Security Appliance devices ringing power grid control systems in Utah, Wyoming and California, according to multiple sources and a vague summary of a Department of Energy filing.

There were no blackouts, no harm to power generation and evidently very little effect on the Western transmission grid, according to multiple sources and officials. The most direct impact was likely a temporary loss of visibility to certain parts of the utility's supervisory control and data acquisition (SCADA) system, though all major transmission operators in the regions affected

Couches OSI et Bus de terrain

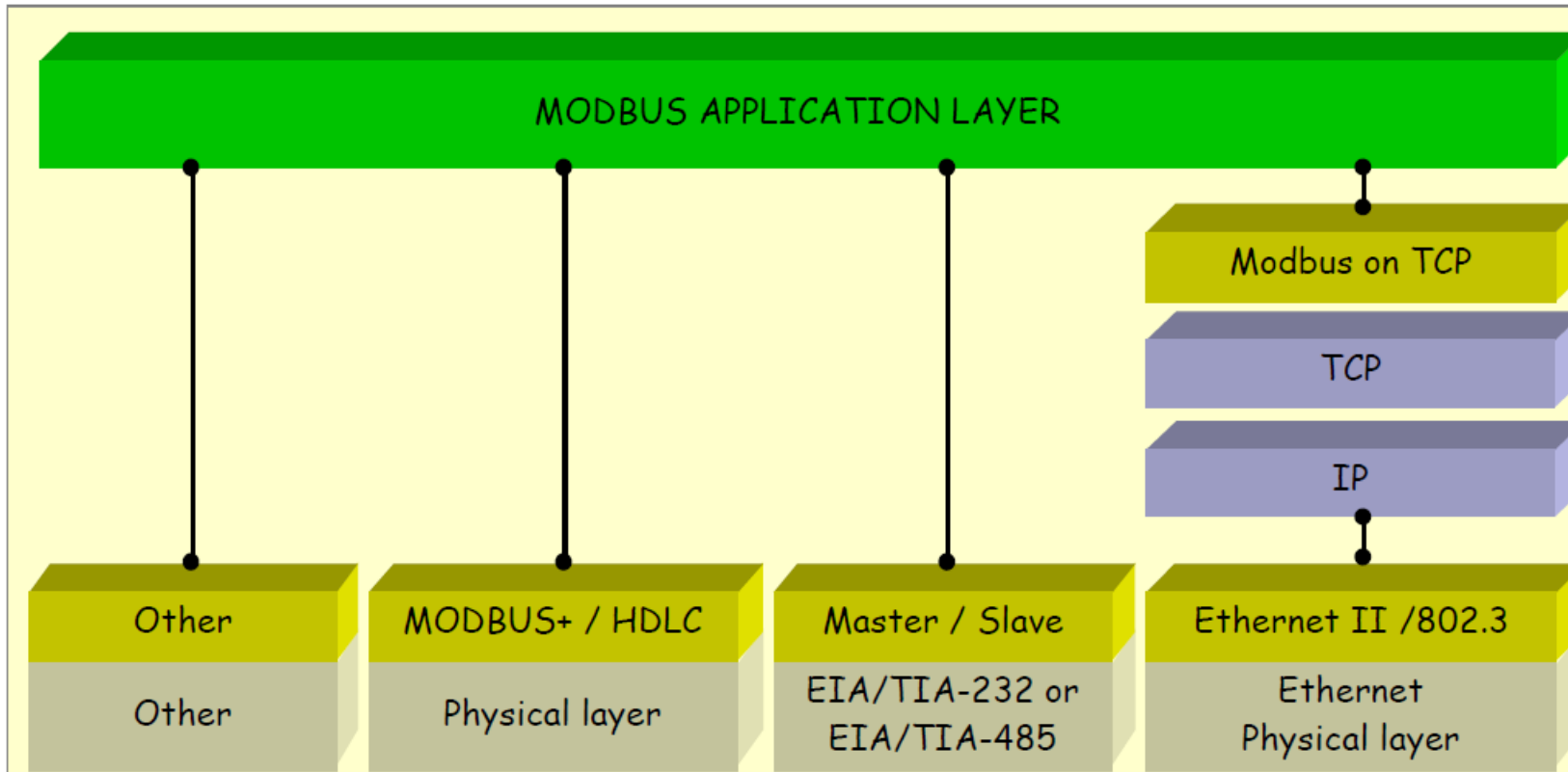


Figure 1: MODBUS communication stack

Couches OSI et Bus de terrain

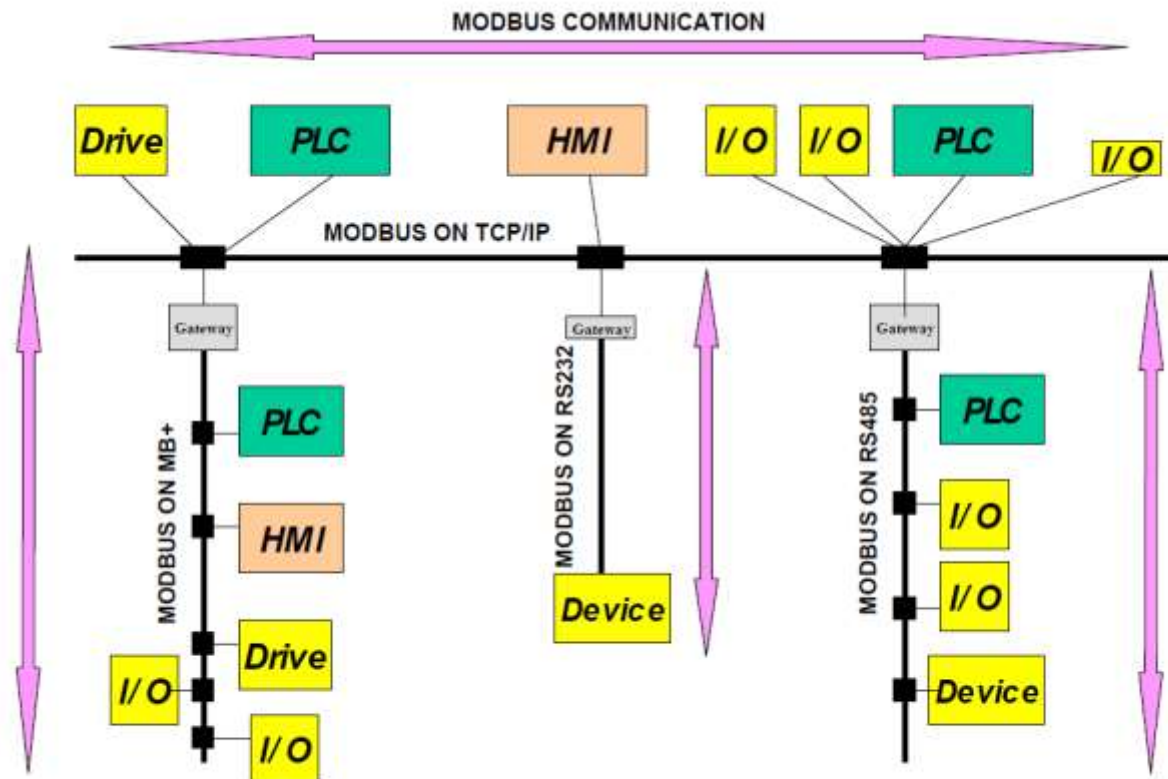


Figure 2: Example of MODBUS Network Architecture

Couches OSI et Bus de terrain

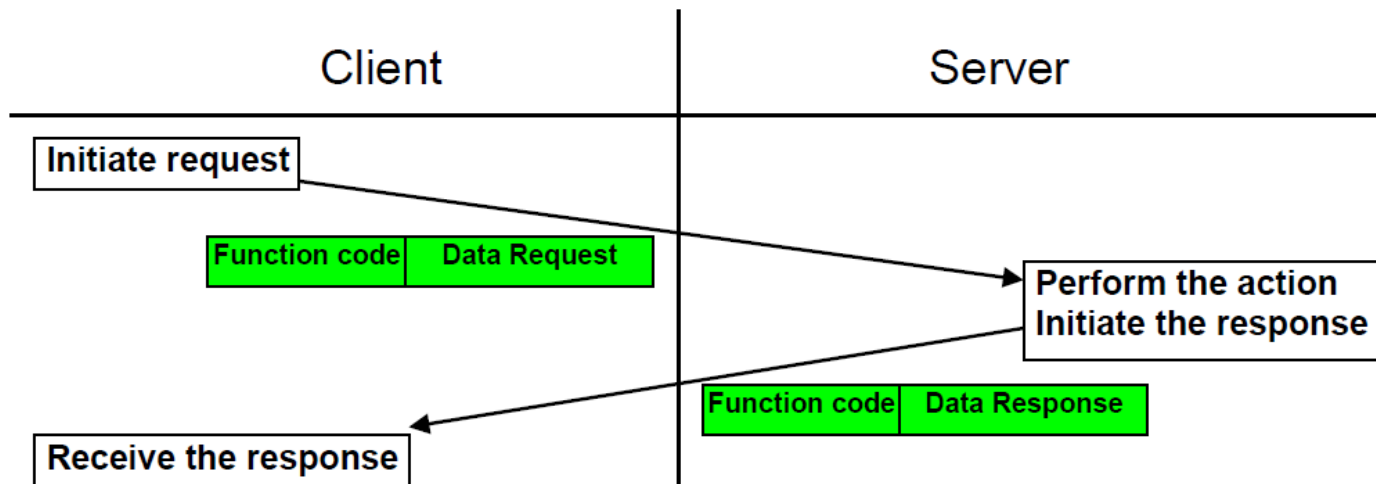


Figure 4: MODBUS transaction (error free)

Modèle de requête/réponse au niveau applicatif

Couches OSI et Bus de terrain

- Donnée en entrée/en sortie (Commande moteur, Capteur).
- Donnée binaire/analogique (On/Off, Vitesse moteur).

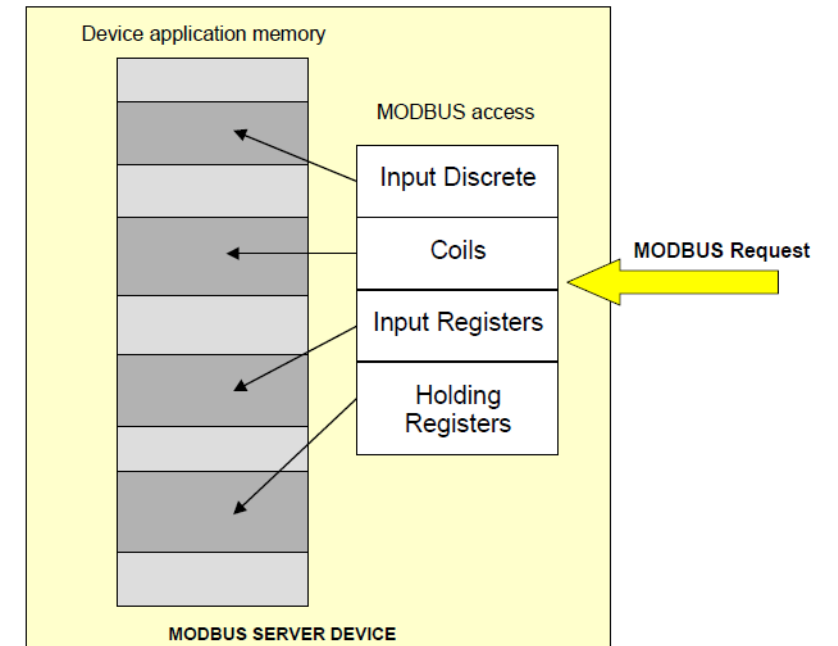


Figure 6 MODBUS Data Model with separate block

Modèle de donnée au niveau applicatif

Couches OSI et Bus de terrain

Les connecteurs



RJ-45 (Ethernet)



Connecteur profibus
(DB-9)

OSI – Niveau Physique



USB

DB-9

Couches OSI et Bus de terrain

Les connecteurs

Connecteurs fibre optique (Ethernet)

OSI – Niveau Physique



Couches OSI et Bus de terrain

Les câbles



Cable fibre optique



Cable Ethernet CAT-8
(40 Gbps)



Cable Profibus

OSI – Niveau Physique

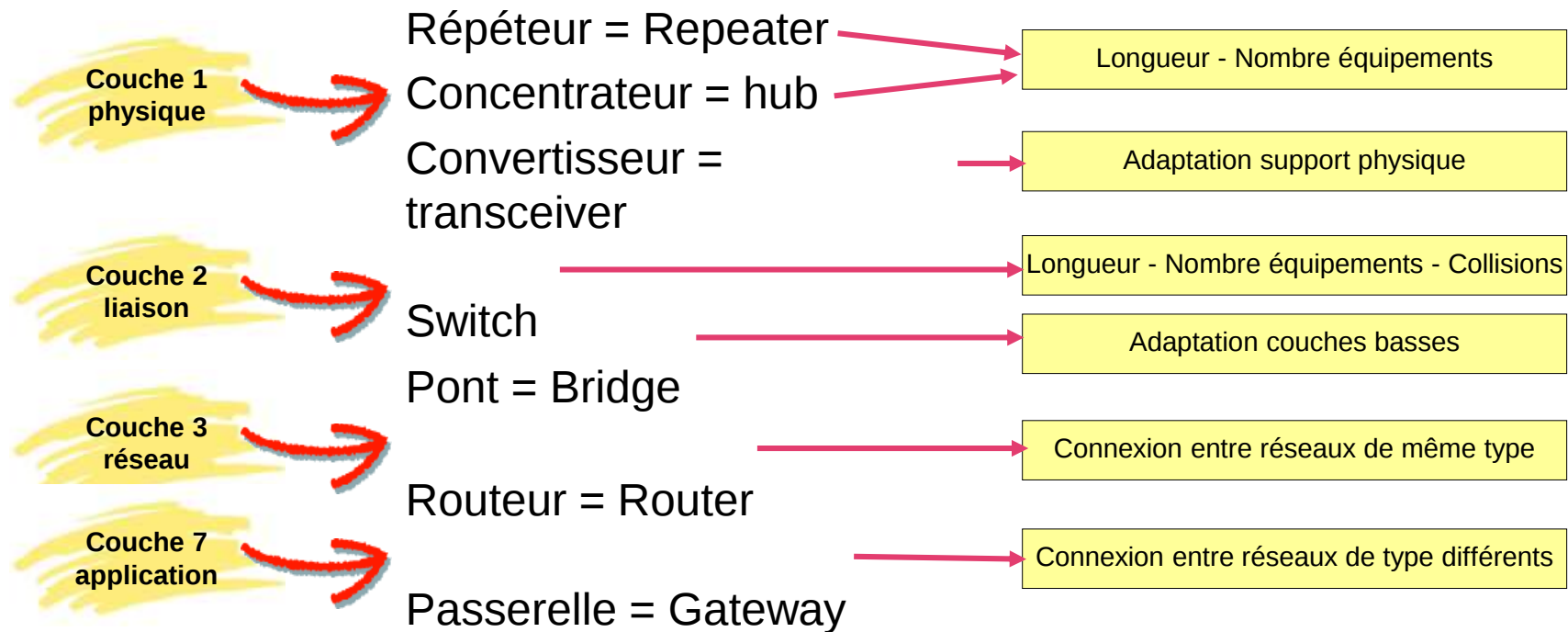
Couches OSI et Bus de terrain

Les câbles

- ▶ Le choix du câble ou support de transmission influe sur 4 aspects importants :
 - ▶ La vitesse.
 - ▶ La distance.
 - ▶ L'immunité électromagnétique.
 - ▶ Le coût.

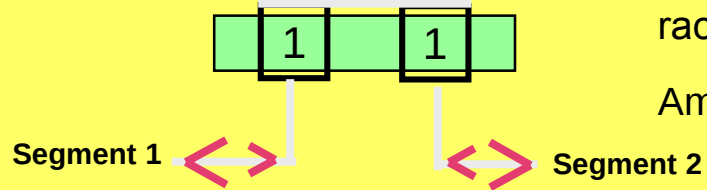
OSI – Niveau Physique

Les équipements de réseaux



Les équipements de réseaux

Répéteur = Repeater



Augmentation longueur et nombre d'équipements
raccordables par ajout d'un nouveau segment

Amplificateur de signal



Exemple :

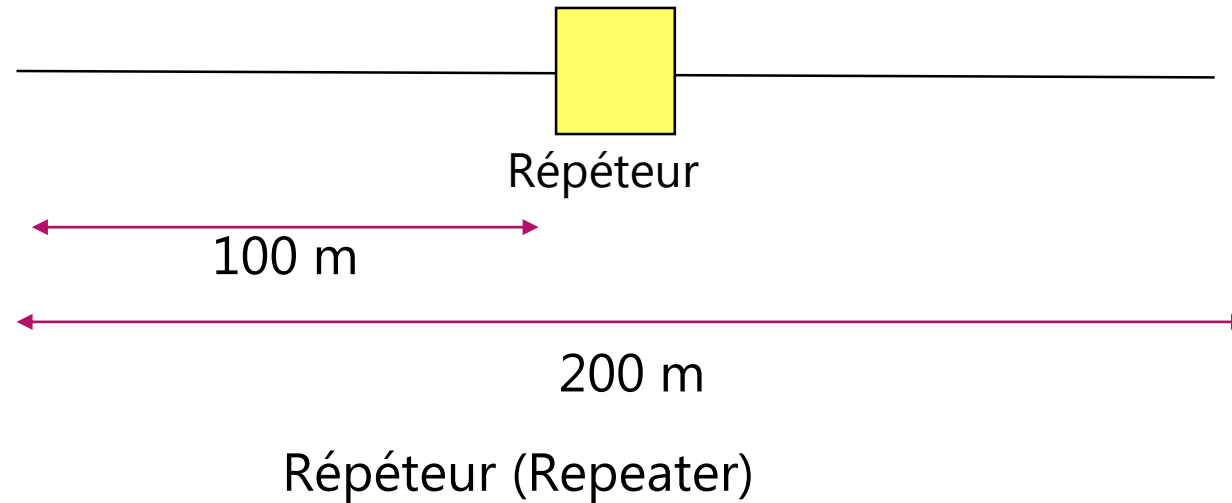
Répéteur ASi

Référence : XZMA1

Connexion sur câble plat par prise
vampire

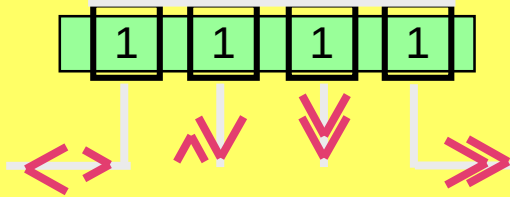
Répéteur (Repeater)

Les équipements de réseaux



Les équipements de réseaux

Concentrateur = Hub



Augmentation longueur et nombre d'équipements par ajout de plusieurs segments. 1 équipement par segment.

Topologie en étoile.

Il amplifie un signal reçu sur un port vers tous les autres ports



Exemple :

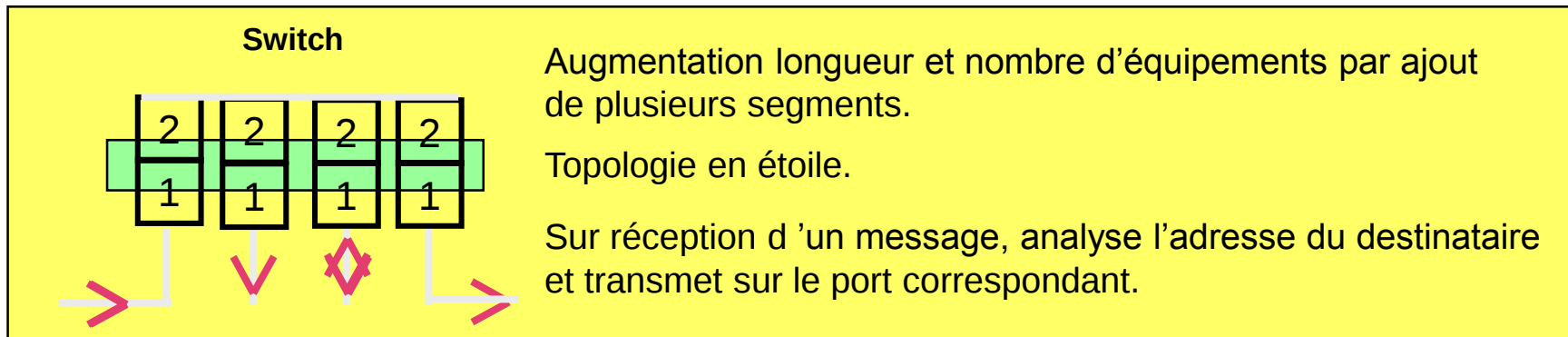
Hub Ethernet 10 Mbits/s - 4 ports RJ45

Référence : 499NEH10410

4 x 10baseT

Concentrateur (Hub)

Les équipements de réseaux



Exemple :

Switch Ethernet 10/100 Mbits/s 8 ports

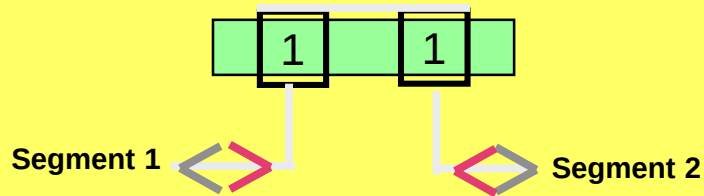
Référence : 499NES18100

8 x 10baseT / 100baseTX (RJ45)

Switch

Les équipements de réseaux

Convertisseur = Transceiver



Adaptation de supports physiques de nature différente.

Convertisseur de signaux.



Exemple :

Transceiver Ethernet 100 Mbits/s paires torsadées - fibre optique

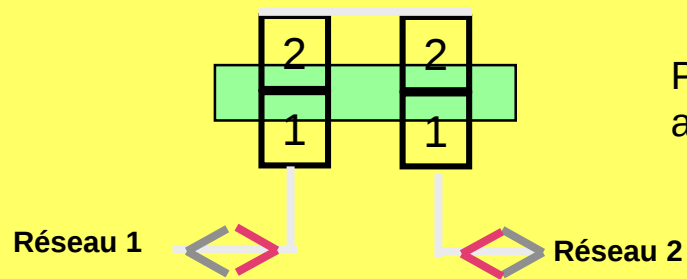
Référence : 499NTR10100

Conversion 100baseTX (RJ45) - 100baseFX (SC)

Convertisseur (Transceiver)

Les équipements de réseaux

Pont = Bridge



Permet de relier 2 réseaux utilisant la même couche application mais des couches basses différentes



Exemple :

Bridge Ethernet TCP-IP Modbus / Modbus
liaison série

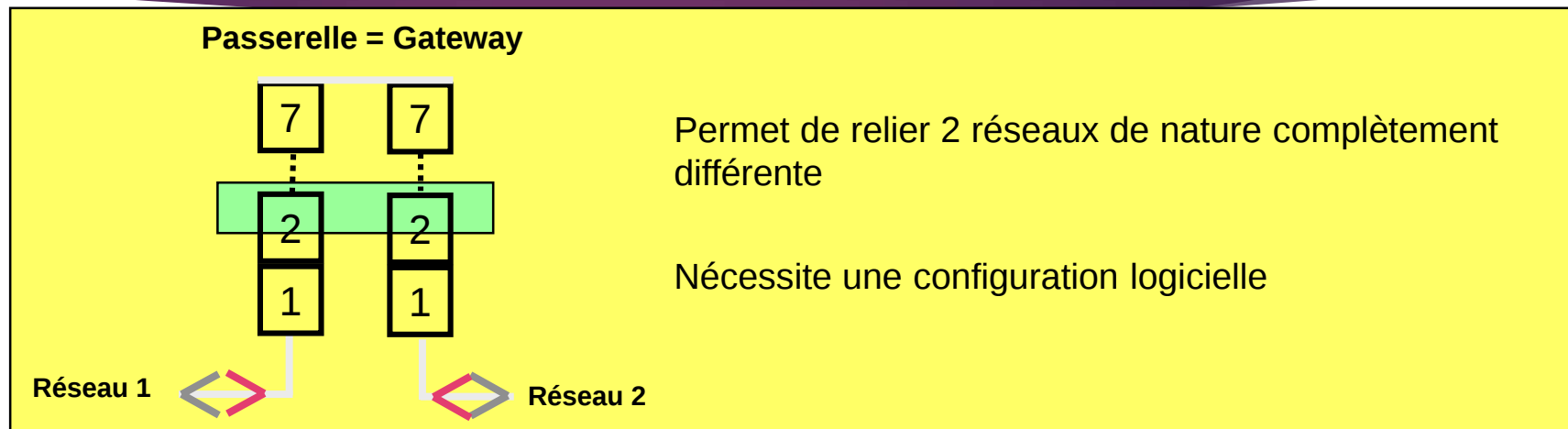
Référence : 174CEV30010

Interface Ethernet : 1 x 10baseT = RJ45

Interface Modbus : RS232 ou RS485 sur RJ45
ou bornes à vis

Pont (Bridge)

Les équipements de réseaux



Exemple :

Passerelle Profibus-DP - Modbus liaison série

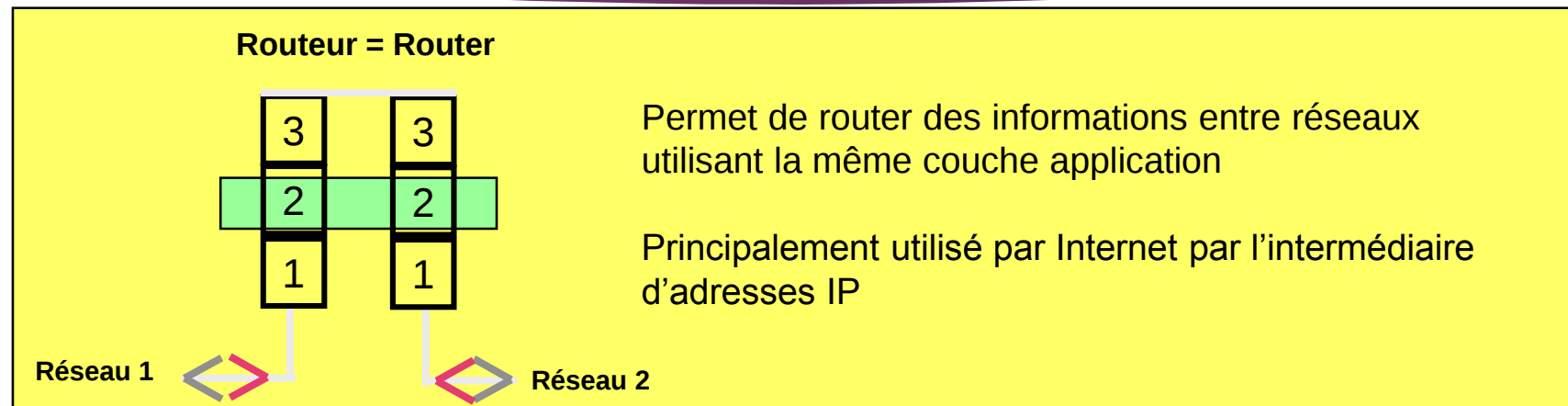
Référence : LUFP7

Interface Profibus-DP (esclave) : Sub-D 9 points

Interface Modbus (maître) : RS485 sur RJ45

Passerelle (Gateway)

Les équipements de réseaux

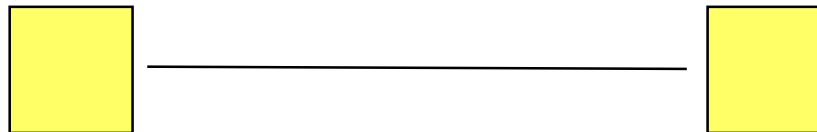


Exemple :
Routeur Ethernet d'Allied Data

Routeur (Router)

Topologie

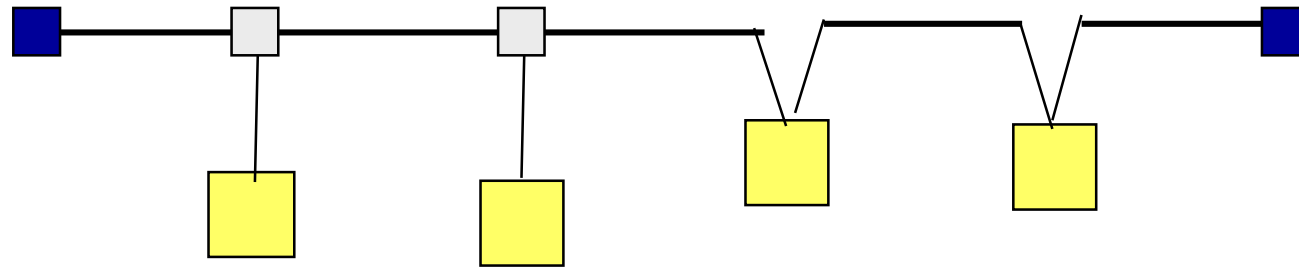
RS232



Point-a-Point

Topologie

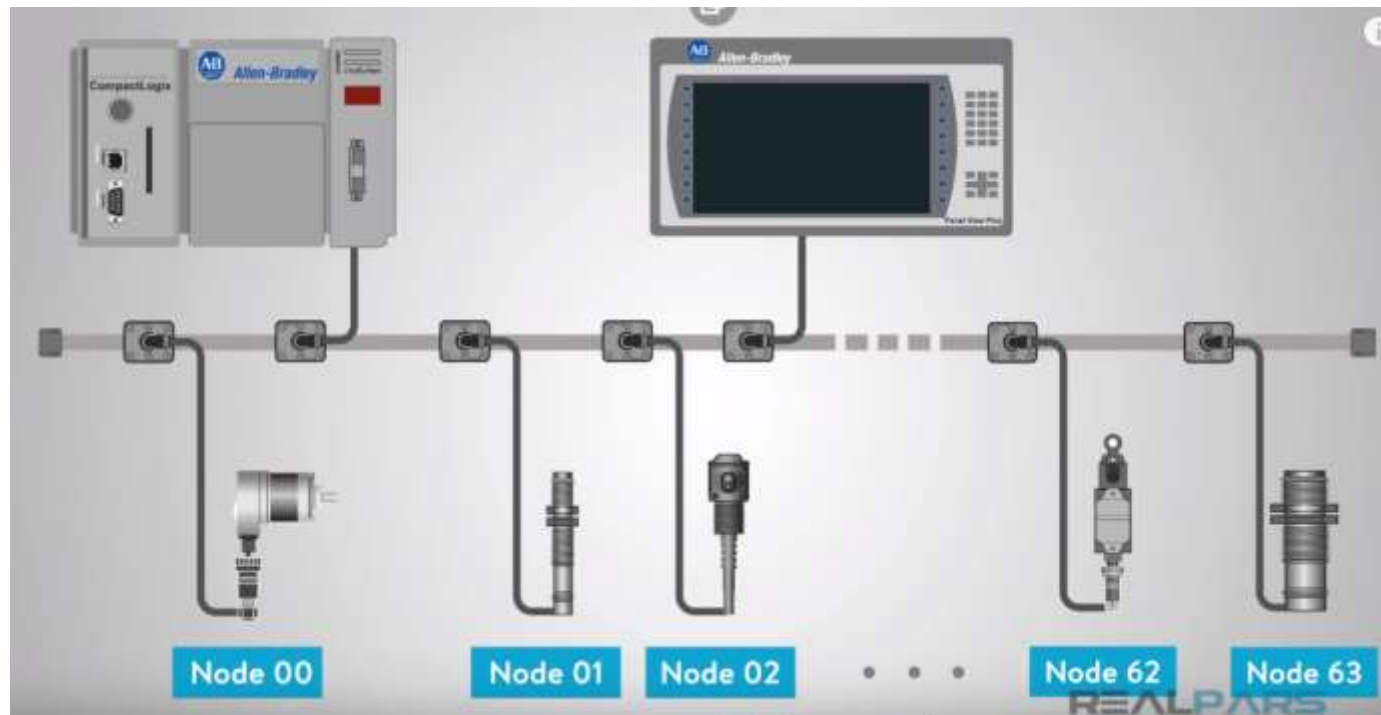
ModBus Over RS285, DeviceNet



Bus

Topologie

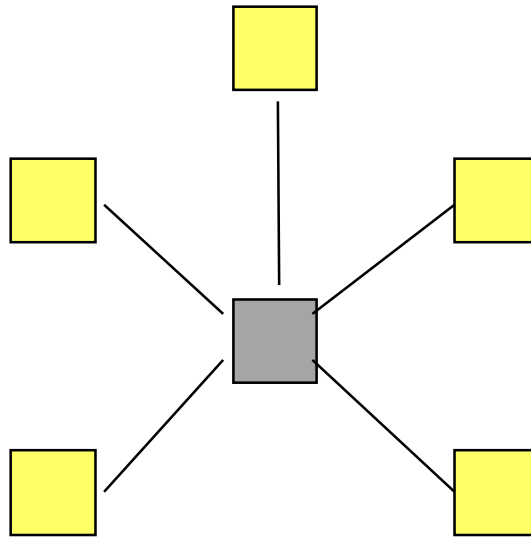
DeviceNet



Bus

Topologie

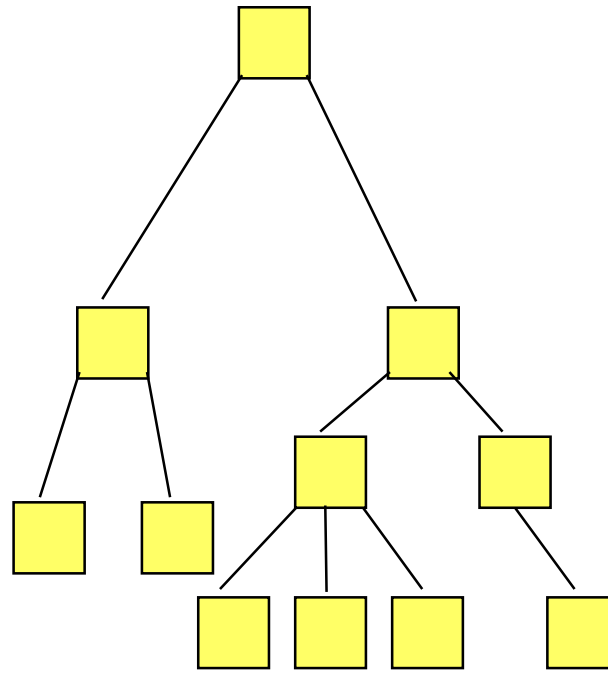
ModBus Over TCP/IP
(Couche Liaison Seulement, Ethernet)



Etoile

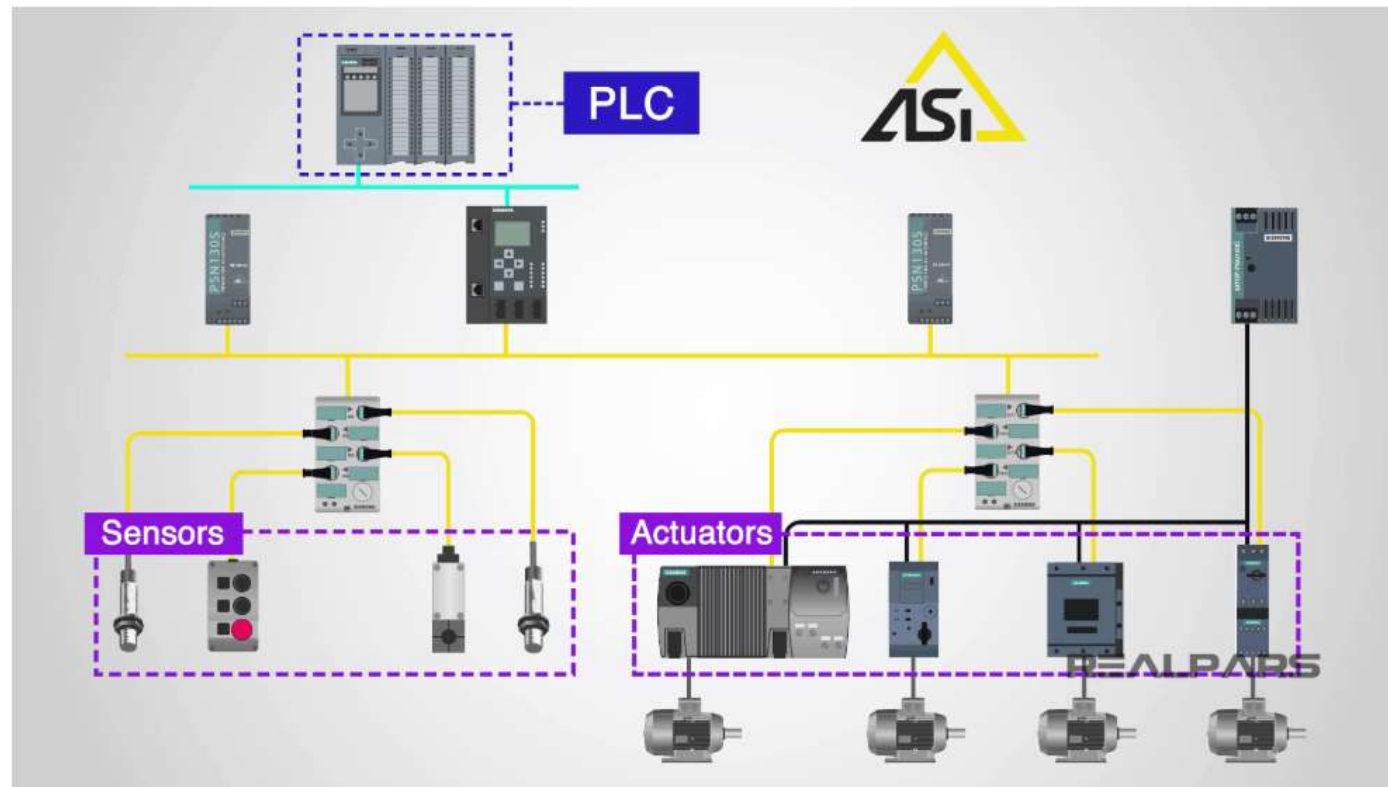
Topologie

ModBus Over TCP/IP, Seriplex



Arbre

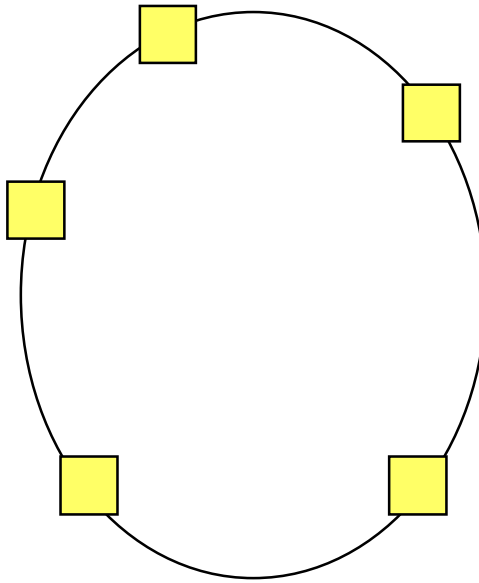
Topologie



Arbre

Topologie

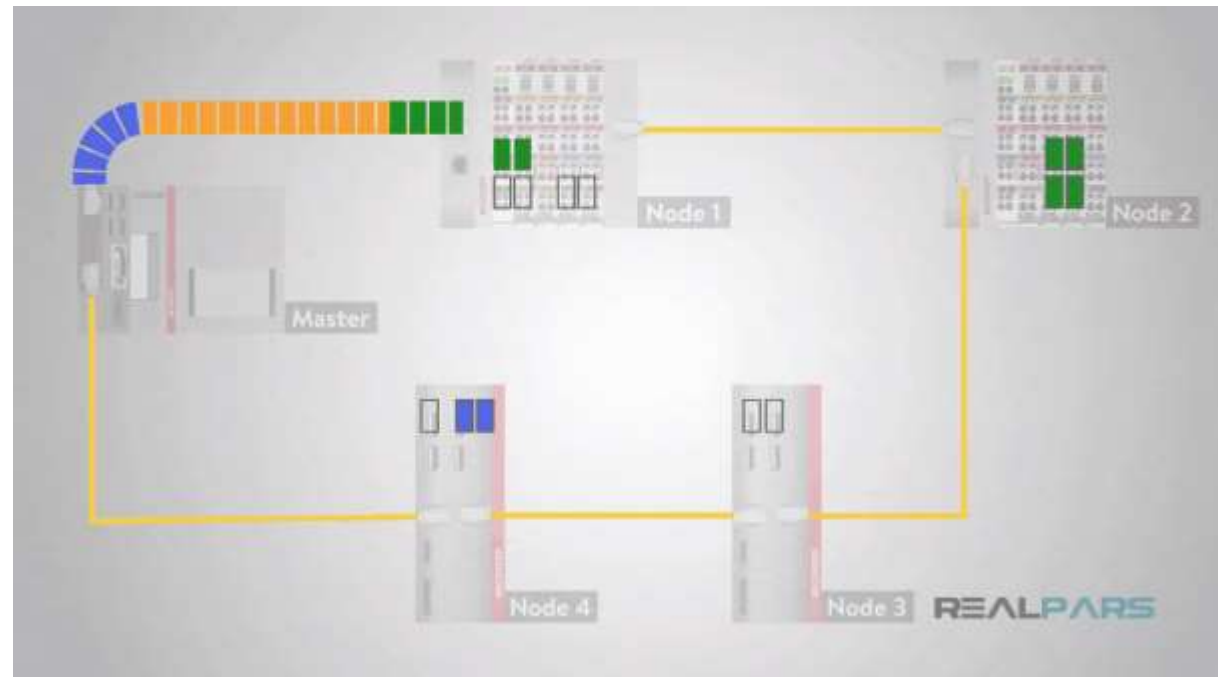
EtherCat



Anneau

Topologie

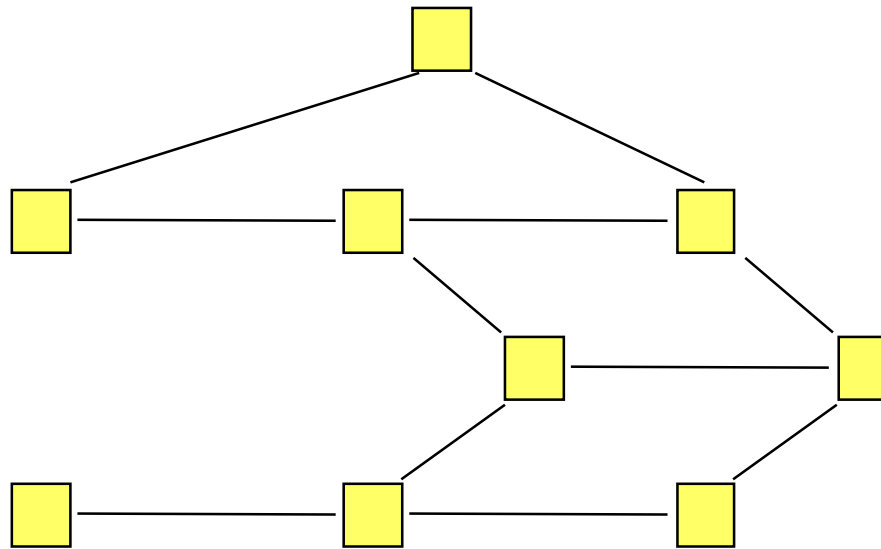
EtherCat



Anneau

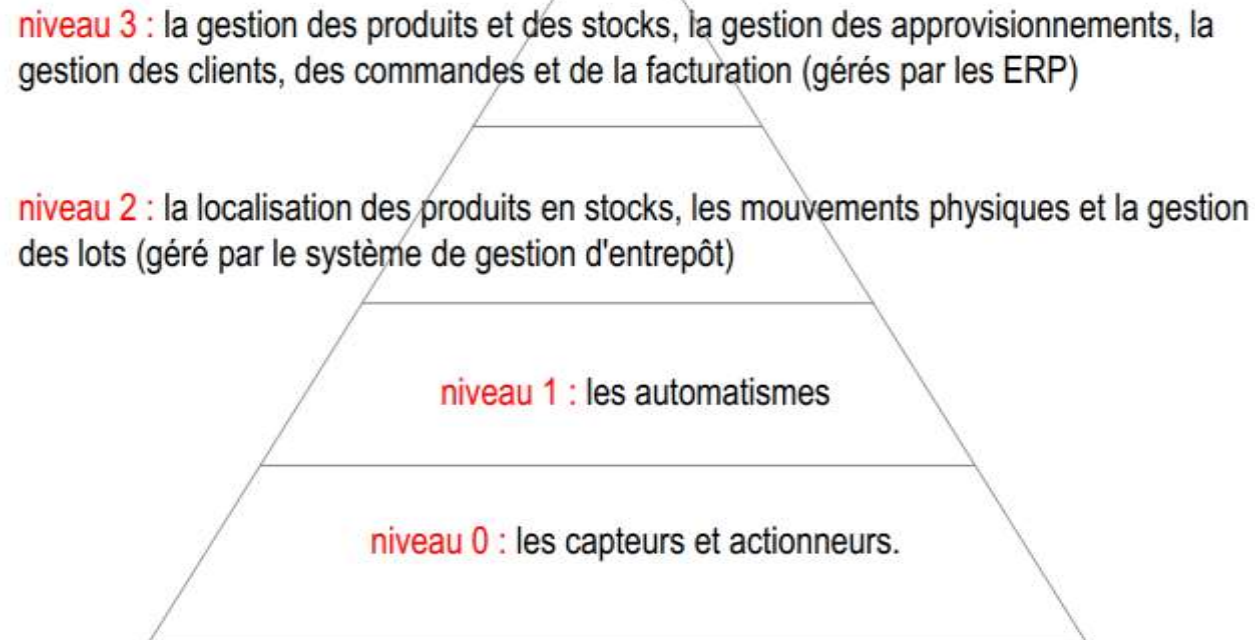
Topologie

ModBus Over TCP/IP



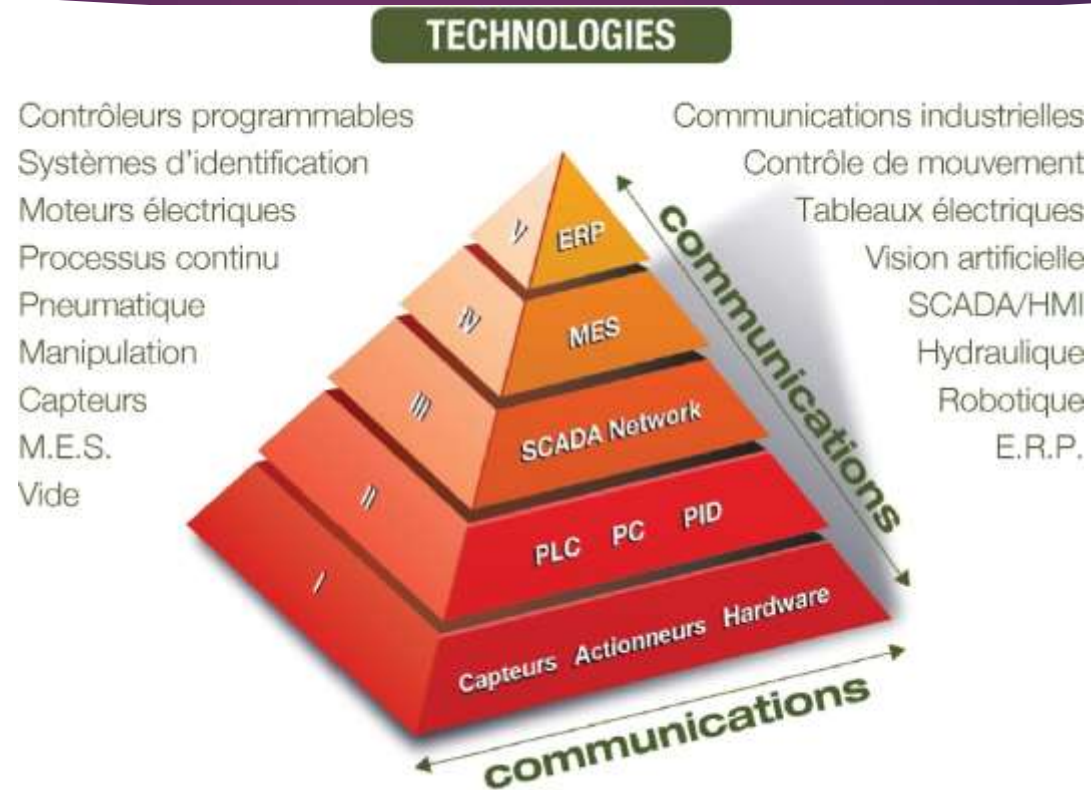
Maillée

Pyramide CIM et Réseaux locaux



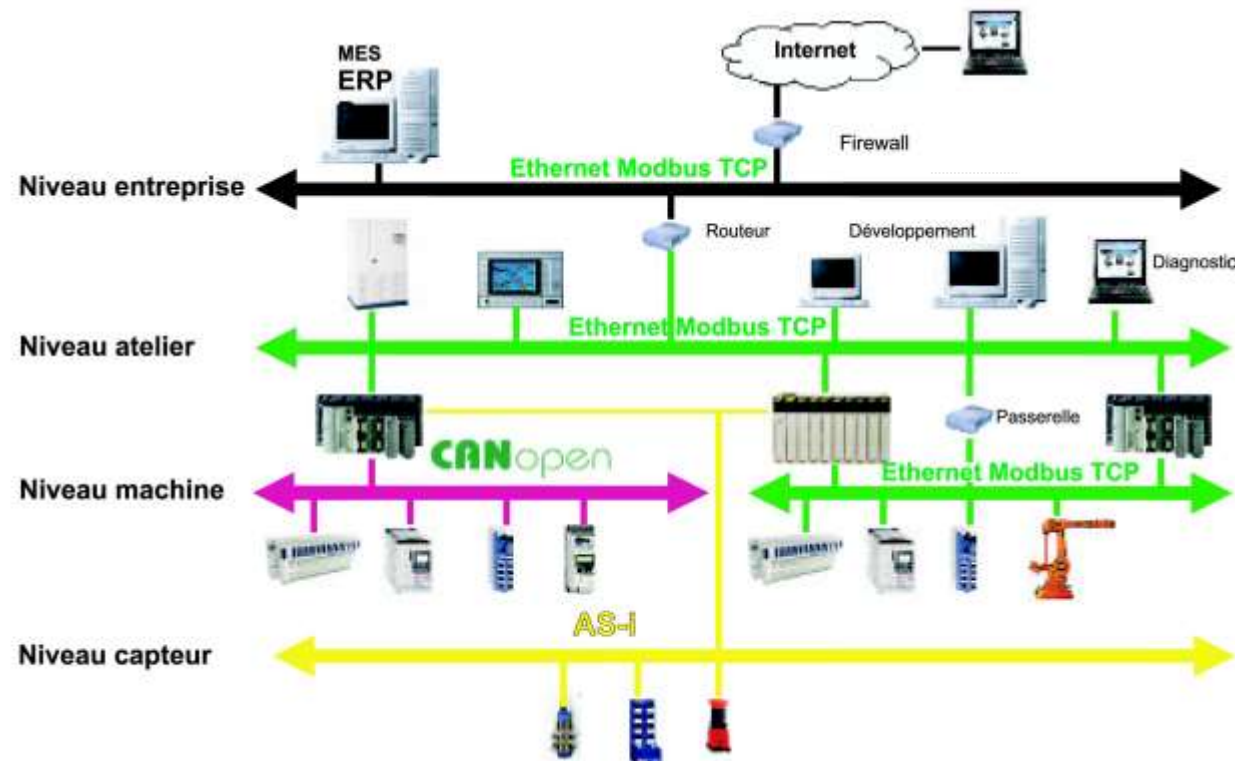
Pyramide CIM

Pyramide CIM et Réseaux locaux



Pyramide CIM

Pyramide CIM et Réseaux locaux



Les niveaux de communication retenus par Schneider Electric

Niveau 3
Entreprise

Data bus

Niveau 2
Atelier

Field bus

Niveau 1
Machine

Device bus

Niveau 0
Constituants

Sensor bus

Système d'information

PC - Serveurs

Gestion de production
Supervision

Automates - IHM

Le contrôle commande

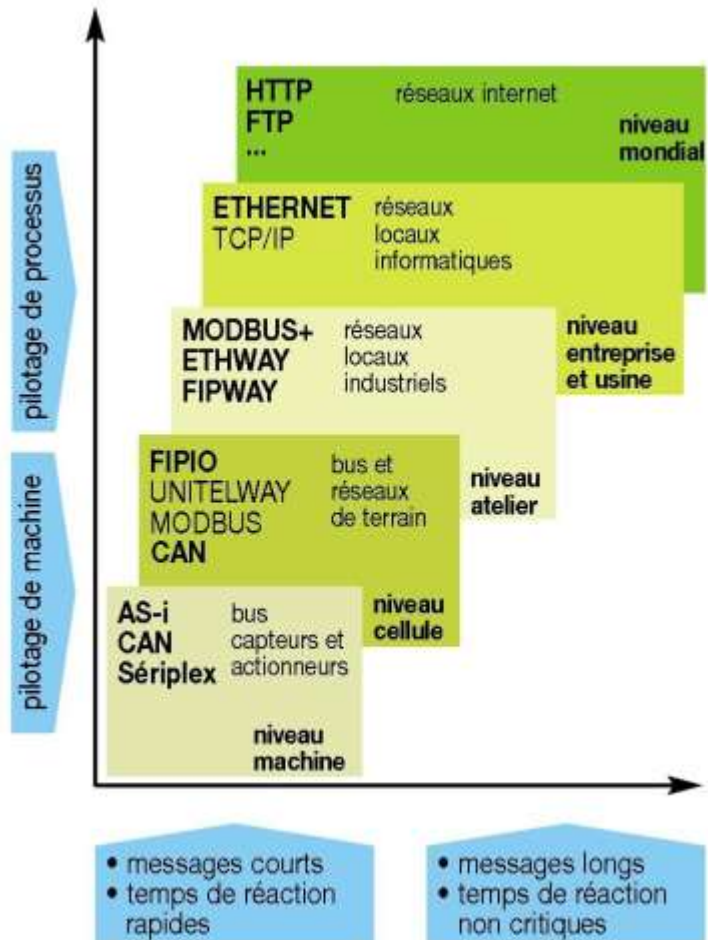
Variateurs de vitesse
Ilots d'automatismes

Détection réaction

Capteurs actionneurs digitaux

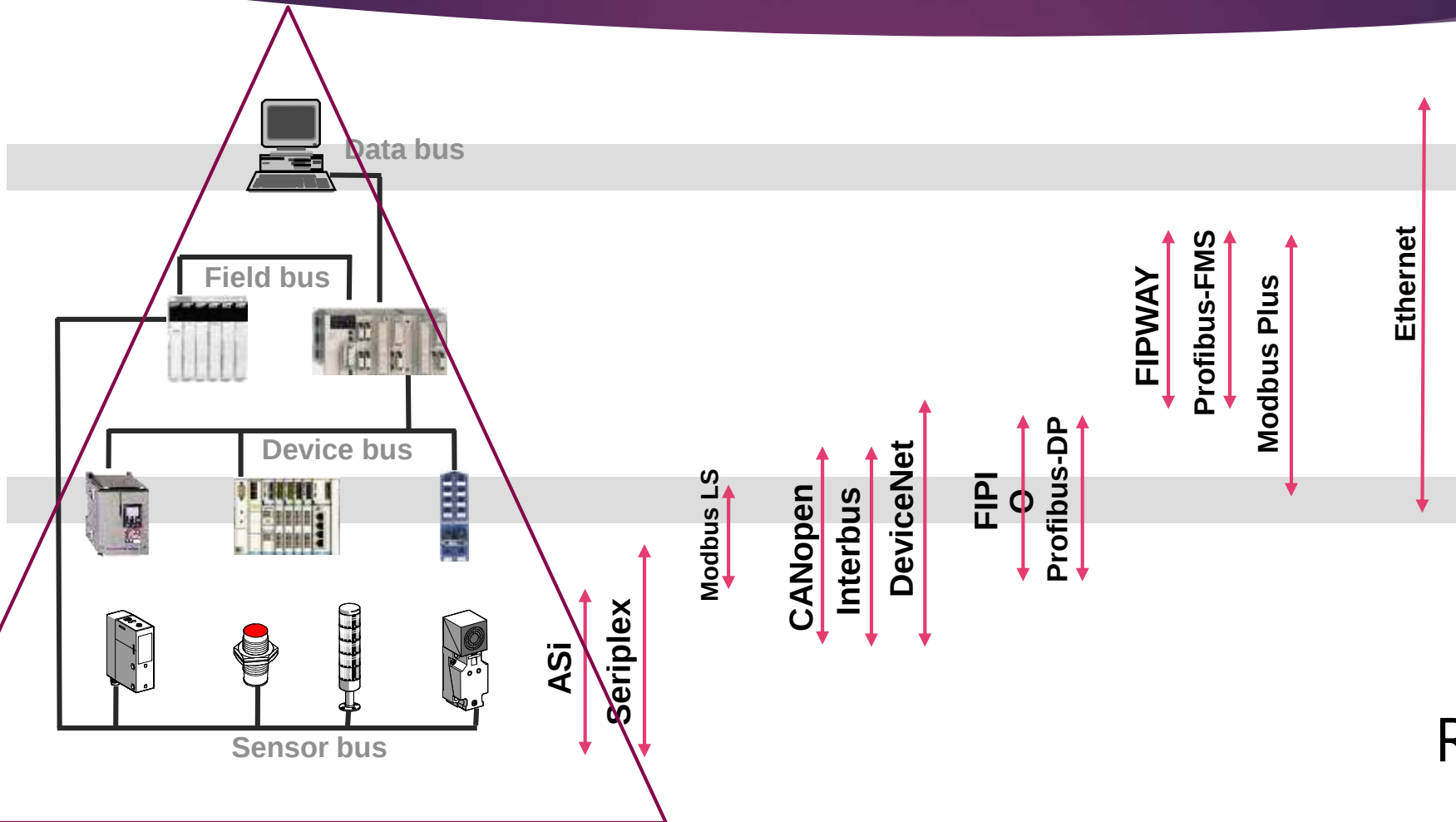
Réseaux Locaux

Pyramide CIM et Réseaux locaux



Réseaux Locaux

Pyramide CIM et Réseaux locaux



Réseaux Locaux

Historique

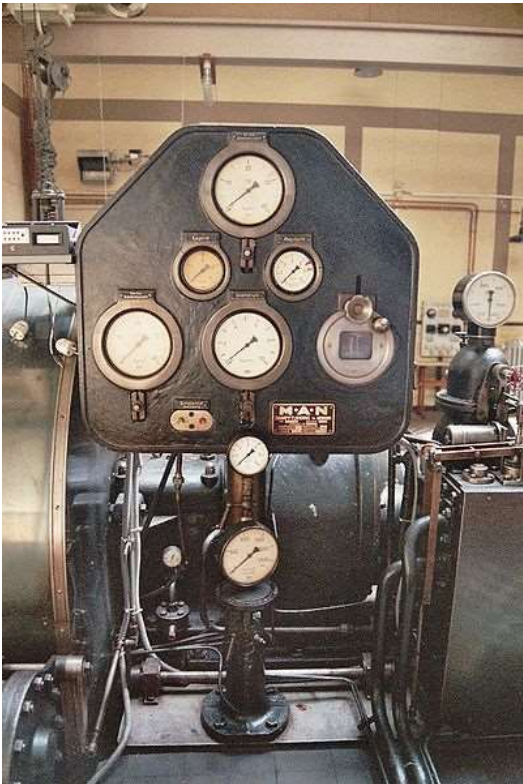


Figure n°1

*Poste de
commande
pneumatique
d'une turbine à
vapeur*

Avant les années 1950, les systèmes de commande pour les longues distances étaient souvent **pneumatiques** et utilisaient des compresseurs bruyants et encombrants de 20 à 50 ch pour le contrôle **HVAC/R** d'un bâtiment par exemple.

HVAC/R : Heating, ventilation and Air Conditioning / Refrigeration (Chauffage, ventilation et climatisation / réfrigération)



Figure n°2

*Régulateur PID
pneumatique*

Historique



Figure n°3 Salle de contrôle (1950)

A partir des années 1950, les systèmes **de contrôle électriques puis électroniques** ont remplacé la technologie pneumatique.

Figure n°4 Salle de contrôle (1960)



Les câbles électriques étant plus faciles à passer qu'une distribution pneumatique, **cette technologie électronique** permet de mettre en œuvre des algorithmes de contrôles beaucoup plus élaborés et complexes.

Historique

- Transmettre sur de longues distances, sans distorsion, les informations fournies par les capteurs.
- Être le plus insensible possible aux perturbations.
- Limiter le nombre de conducteurs électriques (alimentation et information).
- Plusieurs récepteurs peuvent exploiter la même information.

La boucle de courant

4 – 20 mA

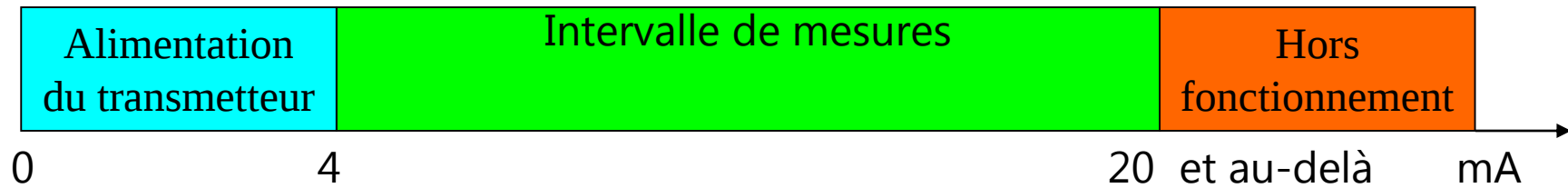
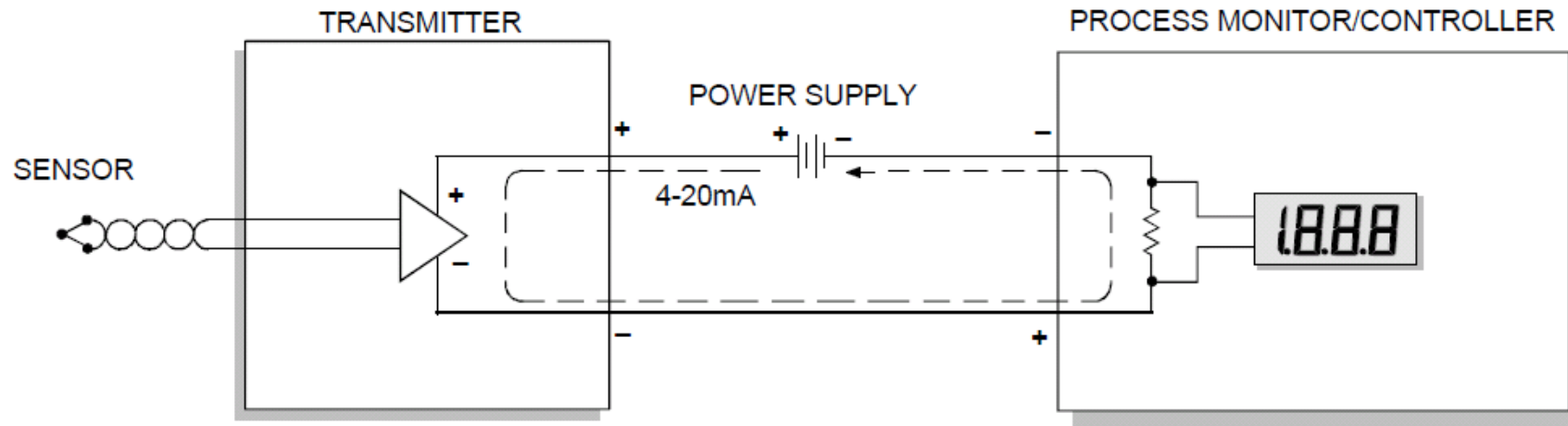
Objectifs à atteindre

Historique

- Une transmission **en tension** présente les caractéristiques suivantes :
 - **facilité de mise en œuvre,**
 - **distance franchissable faible en raison des chutes de tension dans les conducteurs,**
 - **sensible aux bruits surtout si l'impédance d'entrée des récepteurs est élevée (pour augmenter la distance $\Rightarrow$ I faible).**
- Une transmission **en courant** présente les caractéristiques suivantes :
 - **facilité de mise en œuvre avec un coût légèrement supérieur,**
 - **distance franchissable importante car les chutes de tension n'interfèrent pas dans la transmission de l'information,**
 - **insensible aux perturbations.**

Tension ou courant

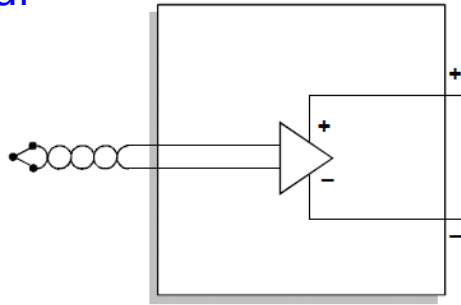
Historique



Principe et Fonctionnement de la boucle de courant

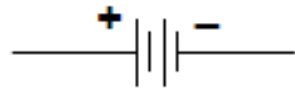
Historique

Transmetteur



- Assure la mesure à l'aide du capteur
- Convertit cette mesure en un courant de 4 mA à 20 mA

Alimentation



- Fournit le courant nécessaire dans la boucle. Les valeurs courantes de cette alimentation continue sont : 36, 24 ou 12 V

Les éléments de la boucle

Historique

- **Coût d'installation relativement faible**
- **2 conducteurs suffisent avec une alimentation continue**
- **Quasiment insensible aux bruits électriques et électromagnétiques**
- **Capacité de transporter des signaux analogiques sur de longues distances
« sans » problème de chutes de tension dans les conducteurs**
- **Plusieurs récepteurs peuvent être placés dans la boucle pour exploiter la même information.**

Avantages de la boucle de courant

Historique

Après l'apparition de la *communication numérique*, cette technique a été rapidement remplacée par **les bus de terrain**.

Cela permet plusieurs avantages:

Réduction des coûts initiaux :

- ✓ Réduction massive du câblage : un 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

Avantages de la boucle de courant