

10. Safety of networks and network safety

10.1 Introduction

10.2 ASI

10.3 CAN

10.4 FIP/WorldFIP

10.5 Profibus

10.6 Interbus

10.7 Réseaux de sécurité

10.1 Introduction

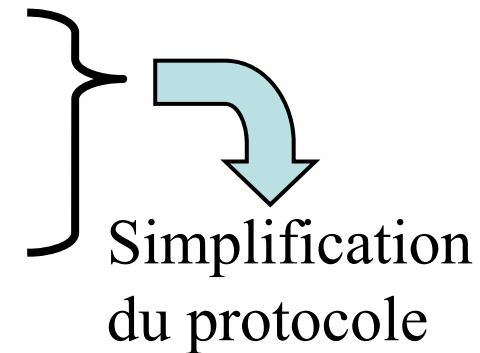
10.1 Fieldbuses

- Development
 - principalement durant les années 80
 - améliorés durant la décennie suivante
 - à l'initiative de constructeurs,
 - consortia regroupant les constructeurs, les utilisateurs et les chercheurs.
- Problem
 - Interopérabilité
 - interchangeabilité...
- Norme IEC 61158 sur les "communications de données numériques pour la mesure et le contrôle, les réseaux de terrain utilisés dans les systèmes de contrôle industriels" (*"Digital data communications for measurement and control - Fieldbus for use in industrial control systems"*)
 - Concaténation des spécifications de plusieurs réseaux de terrain

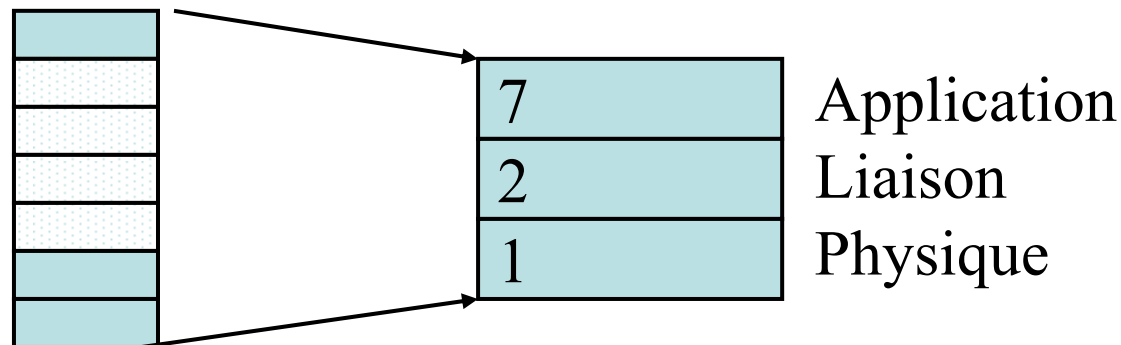
Cas du réseau de terrain

- Objectifs / contraintes / caractéristiques de la communication de terrain :

- Informations de petite taille
- Délais d'acheminement réduits
- Coût des composants réduit



- Solution généralement retenue :
Simplification du modèle OSI :



Méthodes d'accès

- Accès aléatoires :
 - Accéder librement au bus, dès que le médium est libre sans autorisation préalable
 - Risque de collisions
- Accès contrôlés :
 - attente d'un droit de parole (éviter tout conflit)
 - gestion centralisée :
 - 1 station contrôlant les accès
 - gestion décentralisée :
 - pl. stations contrôlant les accès

Accès aléatoires

Principe : Protocoles à compétition

- CSMA/CD :

(Carrier Sense Multiple Access / Collision Detection)

- émission dès que le canal est libre
- en cas de collision :
 1. émission d'une séquence de brouillage
 2. après un délai : nouvelle tentative
 3. abandon après trop d'échecs

- CSMA/CA :

(Carrier Sense Multiple Access / Collision Avoidance)

Mécanisme de priorité en cas d'émission simultanée (Wireless networks)

- CSMA/AMP :

(Carrier Sense Multiple Access / Arbitration by Message)

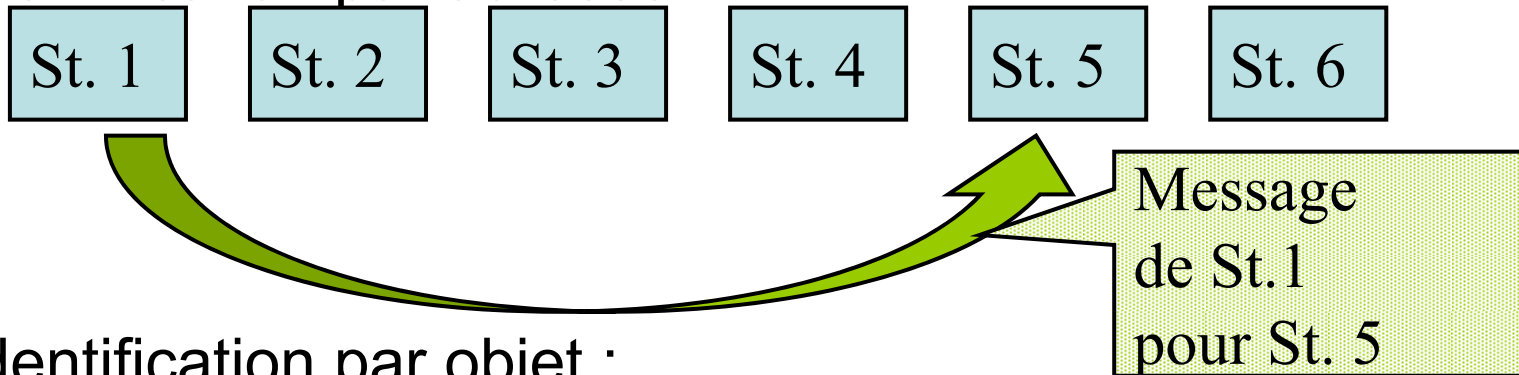
Each message has its own priority

Accès contrôlés

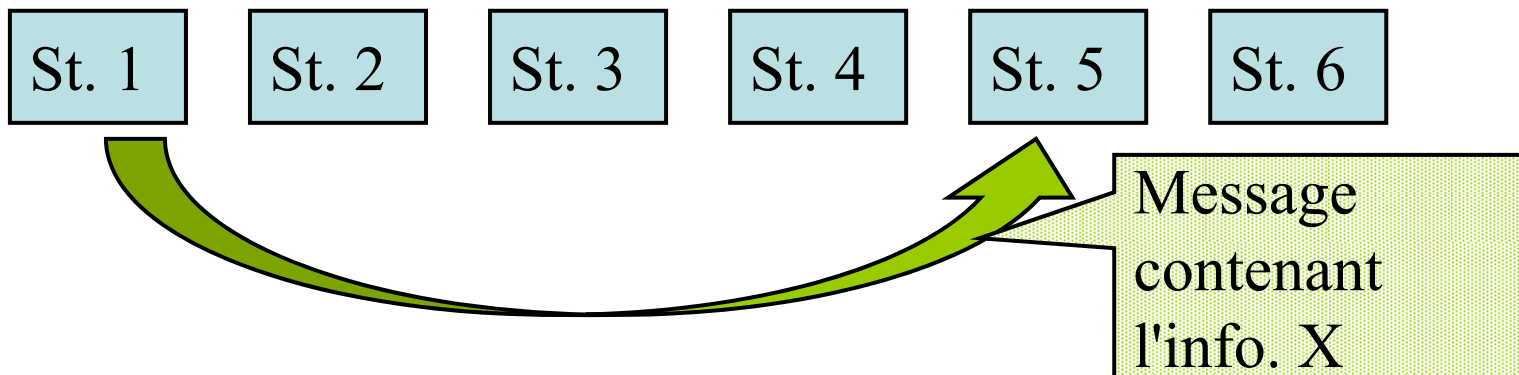
- Accès centralisé par "polling" :
 - Chaque abonné peut émettre à tour de rôle selon un ordre prédéfini.
 - Nécessité :
 1. d'un contrôleur des accès
 2. d'une table de scrutation
- Méthode du jeton sur bus :
 - Création d'un anneau logique dans lequel tourne un jeton
 - Droit de parole et contrôle de l'accès détenu par le possesseur du jeton
 - possession du jeton limité dans le temps

Identification des messages

- Identification par adresse :



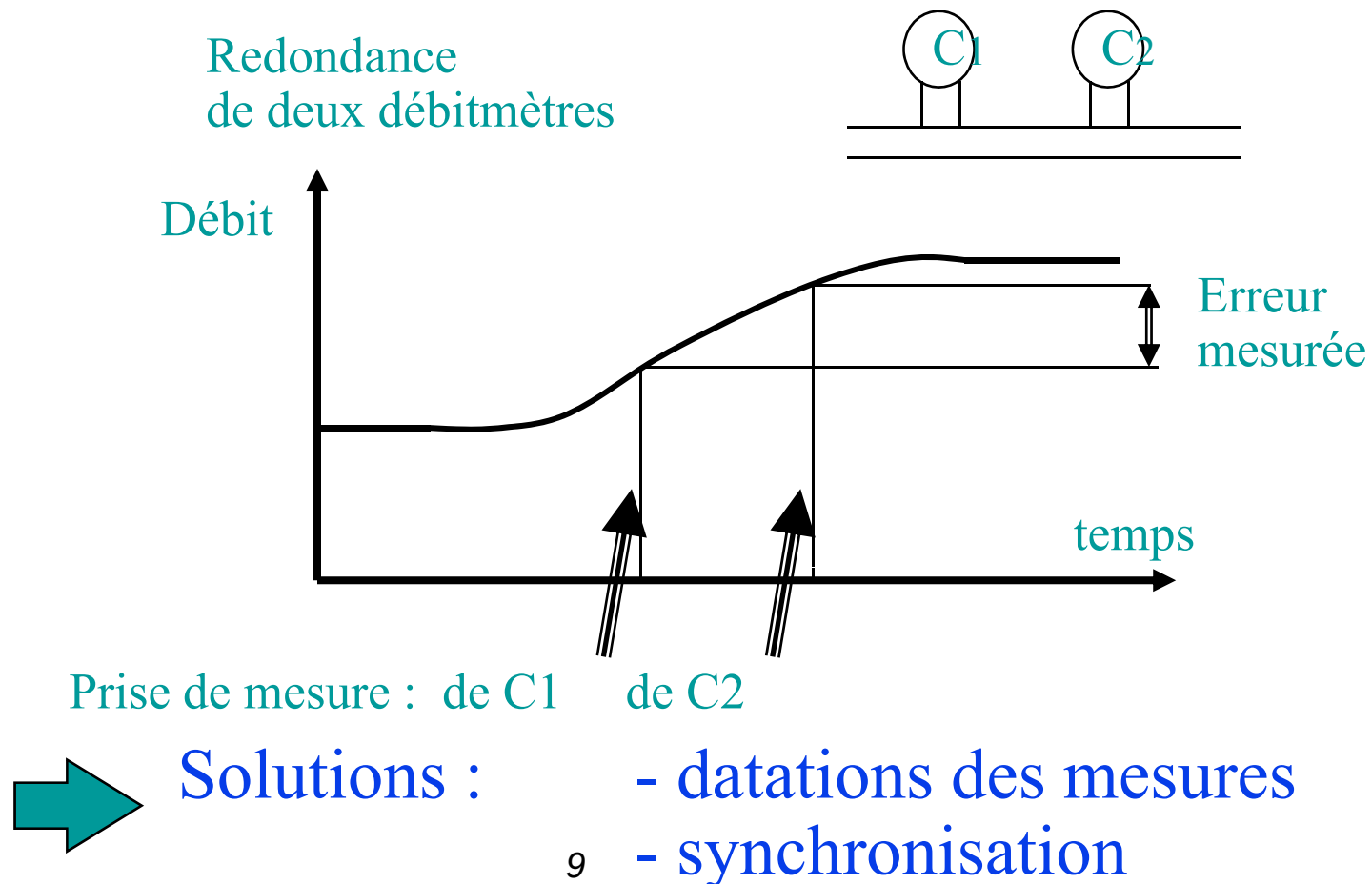
- Identification par objet :



- Diffusion possible vers un groupe de stations (plus simple dans le second cas)

Aspects temporels

- Nécessité d'une datation et/ou d'une synchronisation



Inter...

- **Interopérable :**

coopération avec d'autres Composants d'Automatisme dans et pour une application particulière

⇒ standard de communication commun pour permettre l'échange d'informations

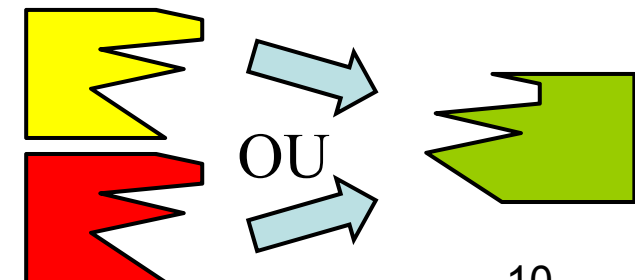
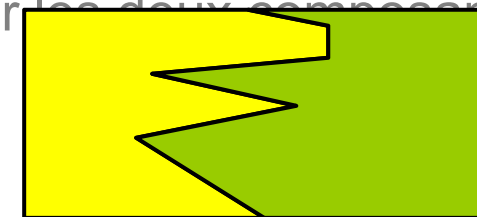
⇒ même interprétation de l'information par les deux composants

- **interchangeable :**

remplacement de l'équipement d'un fabricant par le composant d'un autre fabricant

sans aucune altération

des comportements prévus



Choix d'un bus

Critères de sélection :	Importance		
	Très	plutôt	sans
Vous allez prendre le bus que préconise votre fournisseur d'automatismes préféré	29,3%	41,5%	28%
Vous prendrez le bus qui présente les performances tech. les plus intéressantes	54,9%	35,4%	2,4%
Vous prendrez le bus qui semble avoir le plus d'avenir	56,1%	31,7%	8,5%
Vous prendrez le bus pour lequel l'offre correspond à vos besoins actuels	47,5%	37,8%	11%

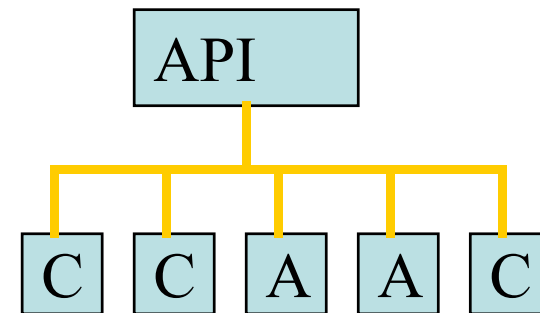
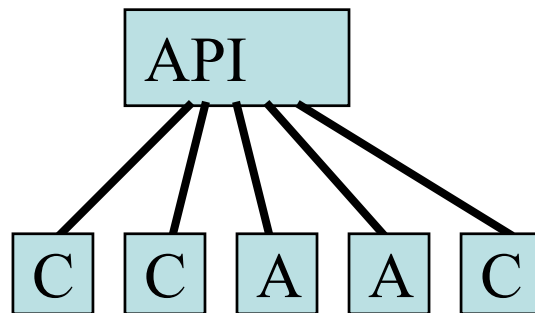
(établi sur 82 réponses)

Source : Mesures 722, Fév. 2000

AS-Interface

AS-I : Pourquoi ?

- Pourquoi AS-Interface (ex-ASI) :
 - Réduction des coûts par simplification du câblage



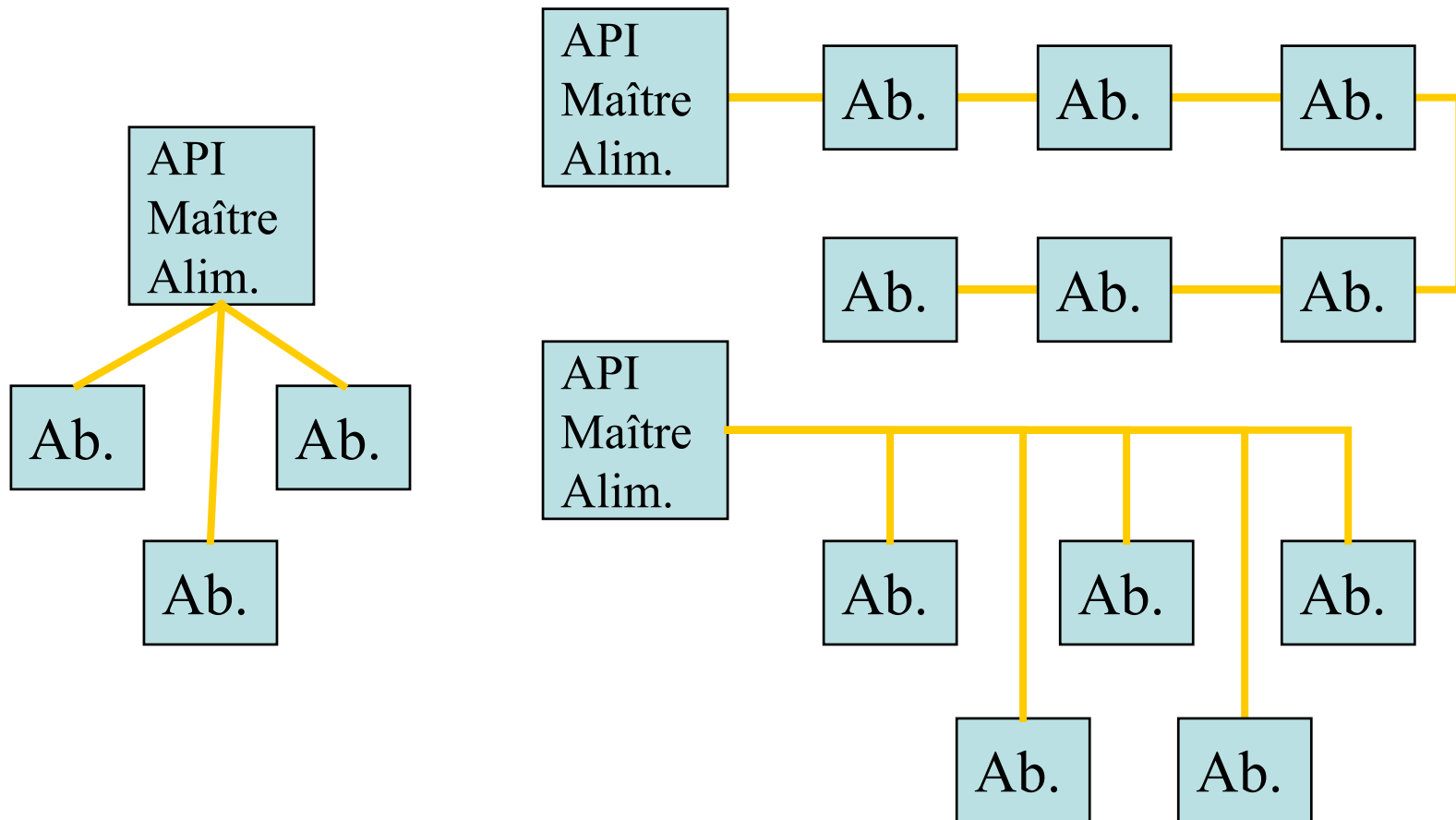
- Répondre au besoin d'Intelligence dans les instruments :



- ← Commande
- ← Auto-test
- Position (fin de course)
- Alarmes

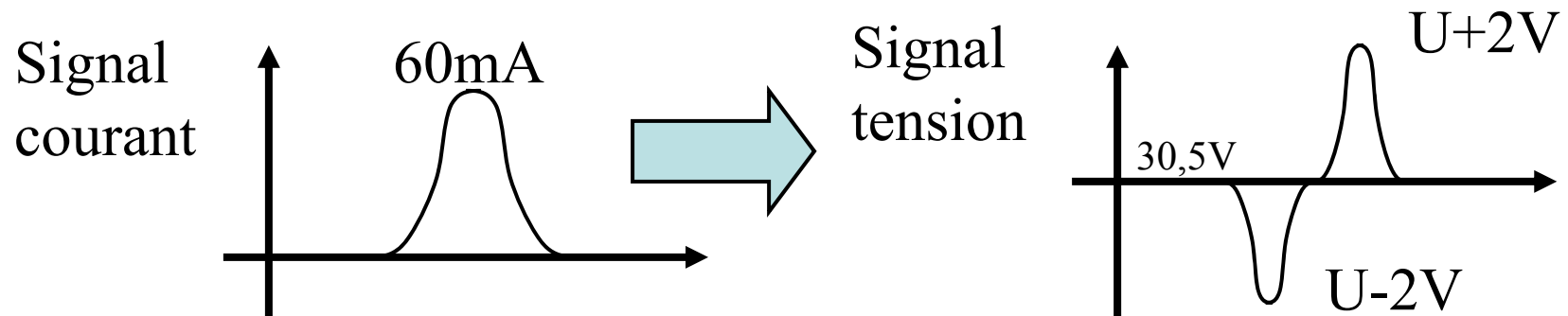
AS-I : Topologie

- Topologie du réseau



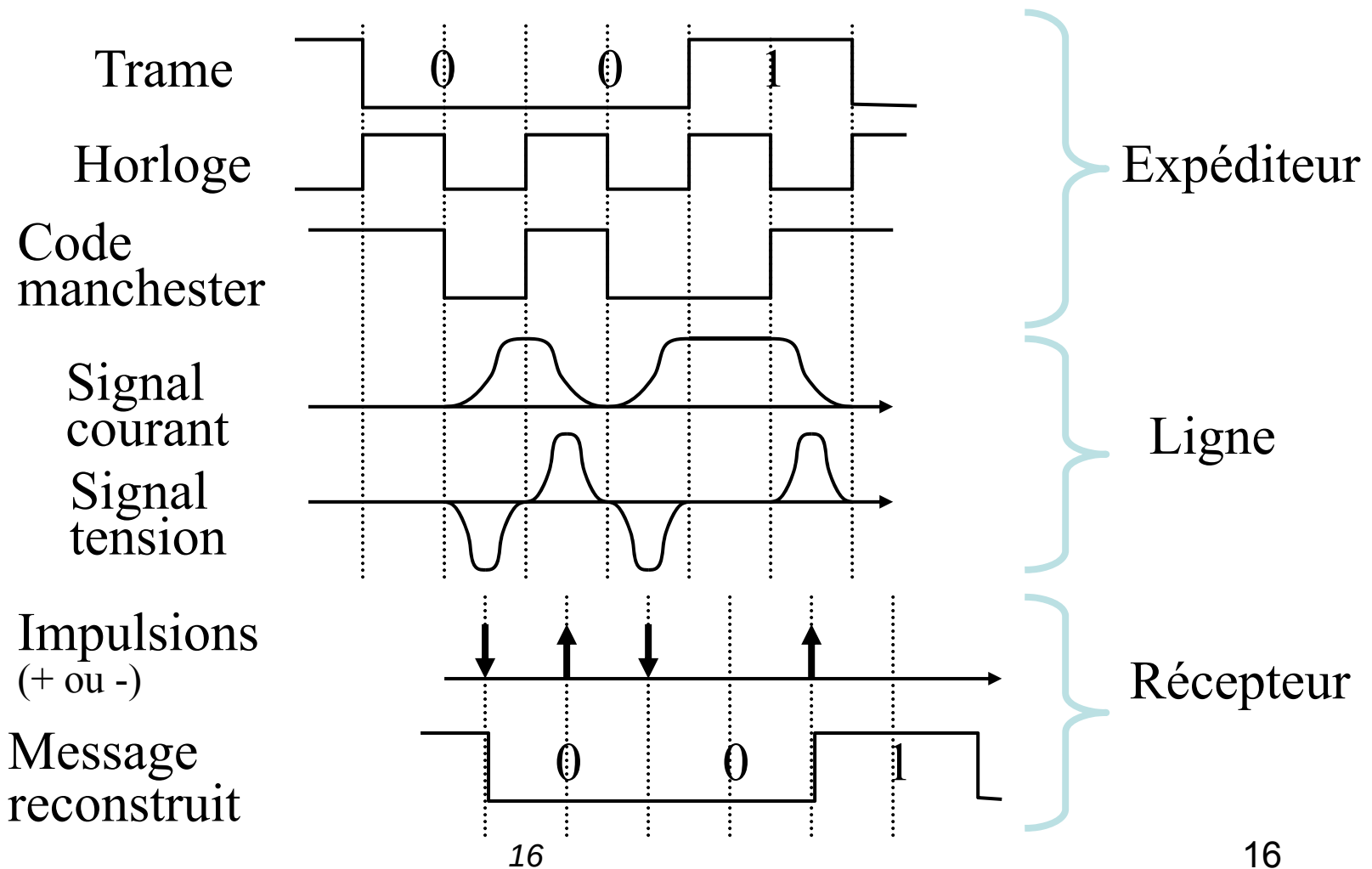
AS-I : Principe de modulation

- Contraintes :
 - Bande passante étroite (nature du câble),
 - Pas de composante continue (alimentation),
 - Faible coût souhaité des modems,
- Solution retenue :
 - Modulation à pulses alternées :



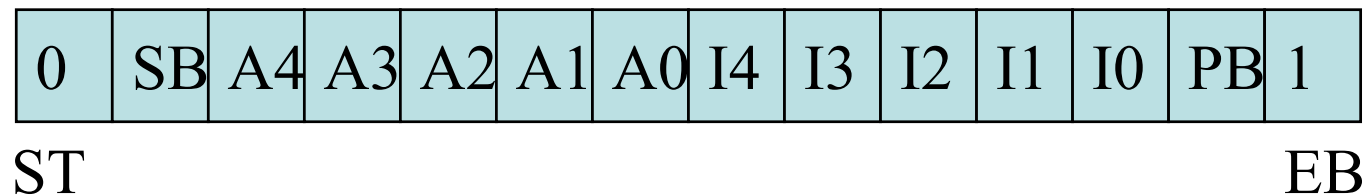
AS-I : Principe de modulation

- Principe de transmission :

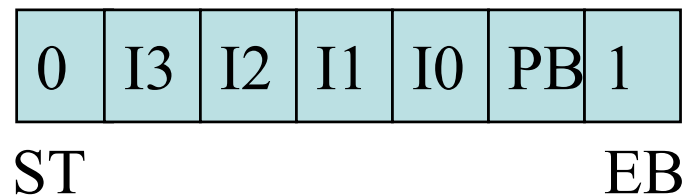


AS-I : Trame

- Caractéristique :
 - 167 kbits/s $\rightarrow$ 1 transaction 150 μ s (=25bits)
- Message maître vers esclave :

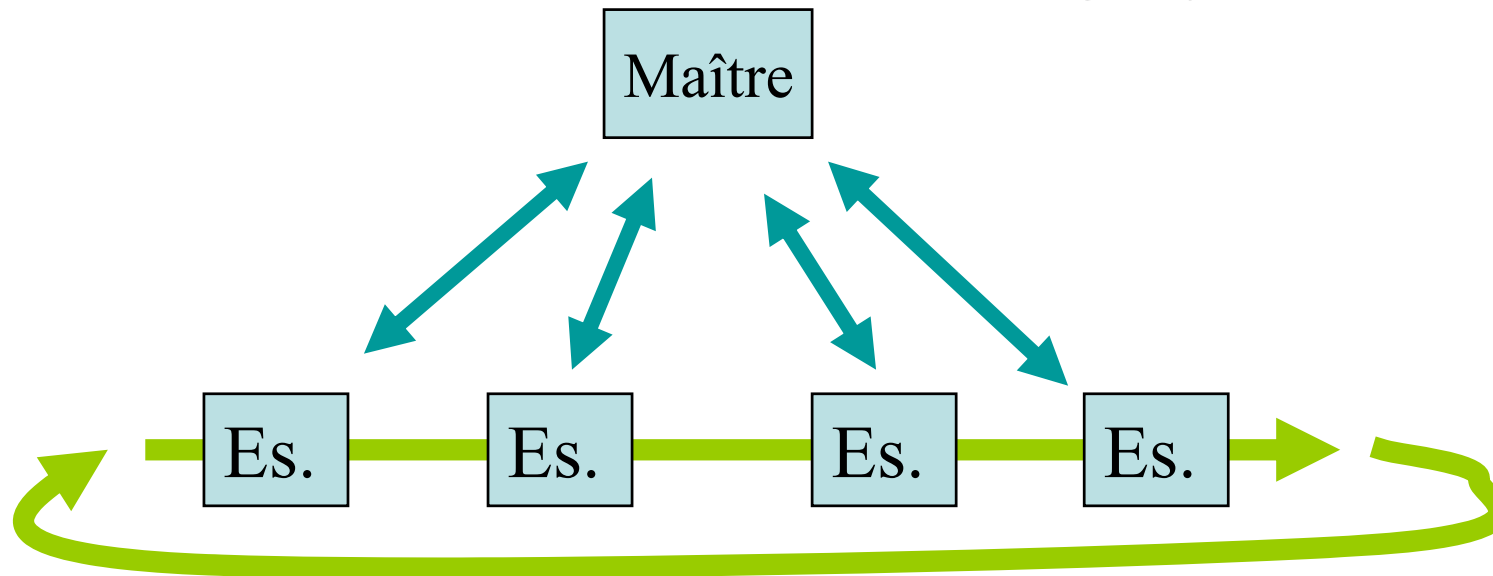


- Message esclave vers maître :



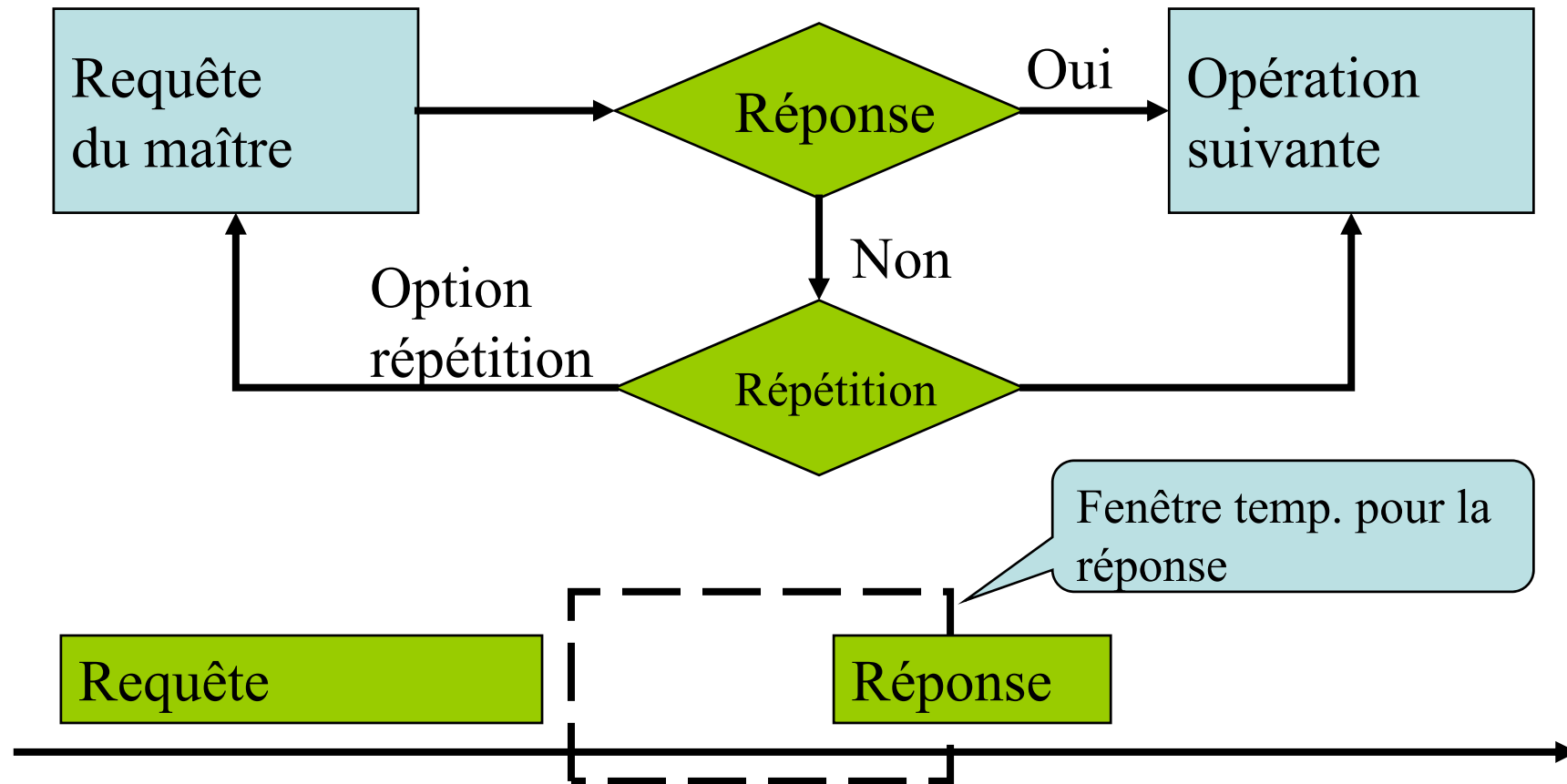
AS-I : Mode de com.

- " Maître / Esclave avec polling cyclique "



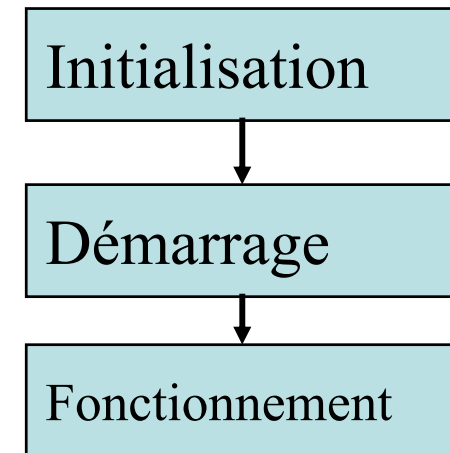
AS-I : les erreurs ?

- Possibilités de répétition de trame



AS-I : Phases de fonctionnement

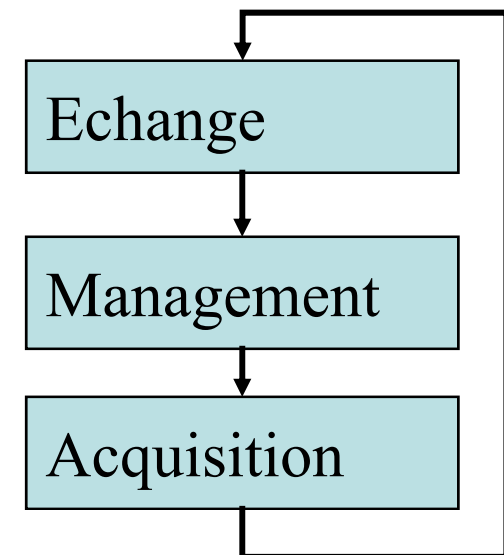
- 3 phases de fonctionnement
- Phase 1 : Initialisation
 - entrées à 0
 - sorties à 1
 - aucune transmission
- Phase 2 : Démarrage
 - phase d'inventaire
scrutation et configuration des esclaves
 - phase de d'activation
activation de chaque esclave avec ses paramètres



AS-I : Phases de fonctionnement

- Phase 3 : Cycle de fonctionnement normal

- Phase d'échange des données
interrogation successive
en cas de défaut : 3 tentatives
- Phase de management
 - Modification paramètres d'un esclave
 - Lecture des statuts
 - Lecture de la configuration
 - Lecture code identifiant
 - Remise à 0 de l'adresse
 - Ré-affectation d'une adresse
 - Reset



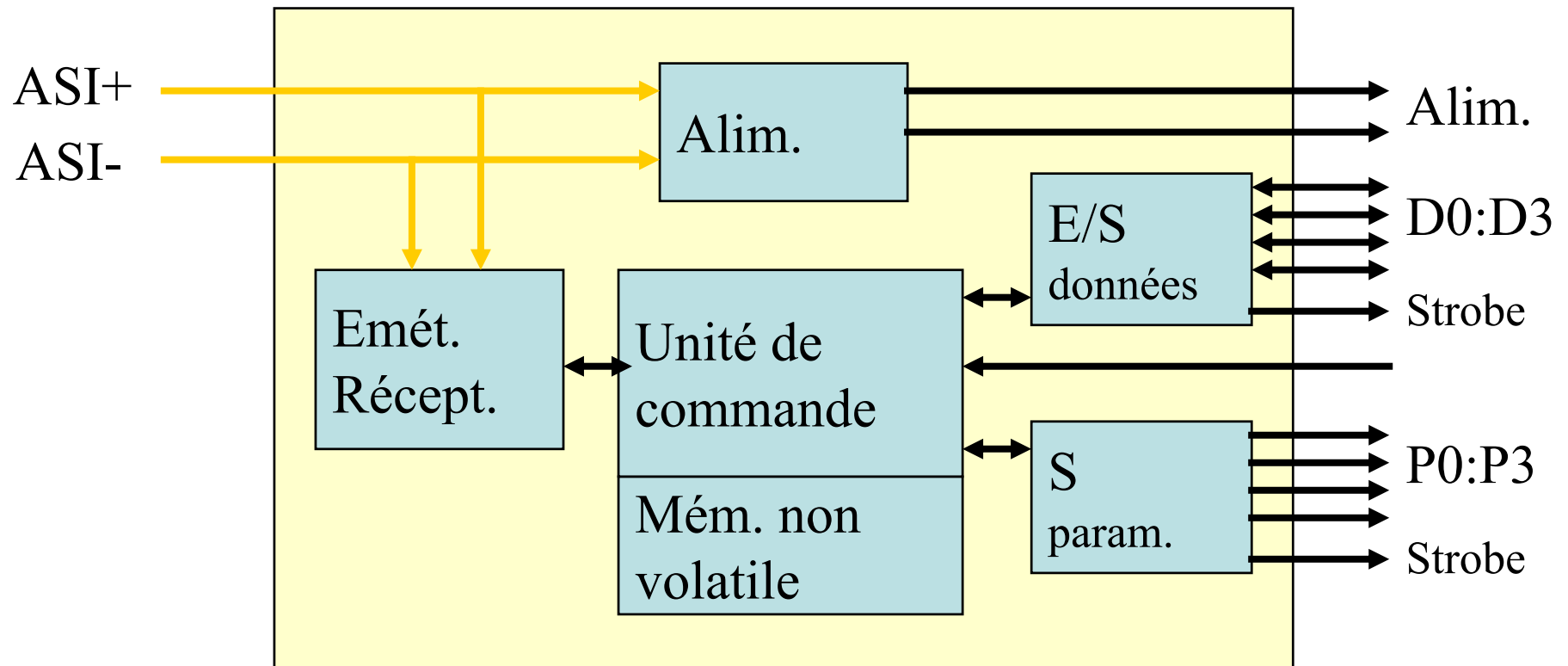
AS-I : Phases de fonctionnement

- Phase 3 : Cycle de fonctionnement normal
 - Phase d'acquisition
Interrogation d'une seule adresse
(dont la valeur est incrémentée à chaque cycle)
Si réponse d'une adresse non-répertoriée :
 - 1er cycle suivant :
mémorisation du code identifiant
 - 2nd cycle suivant :
activation suivant le mode prévu

Détection des nouveaux arrivants

AS-I : Les esclaves

- Synoptique :

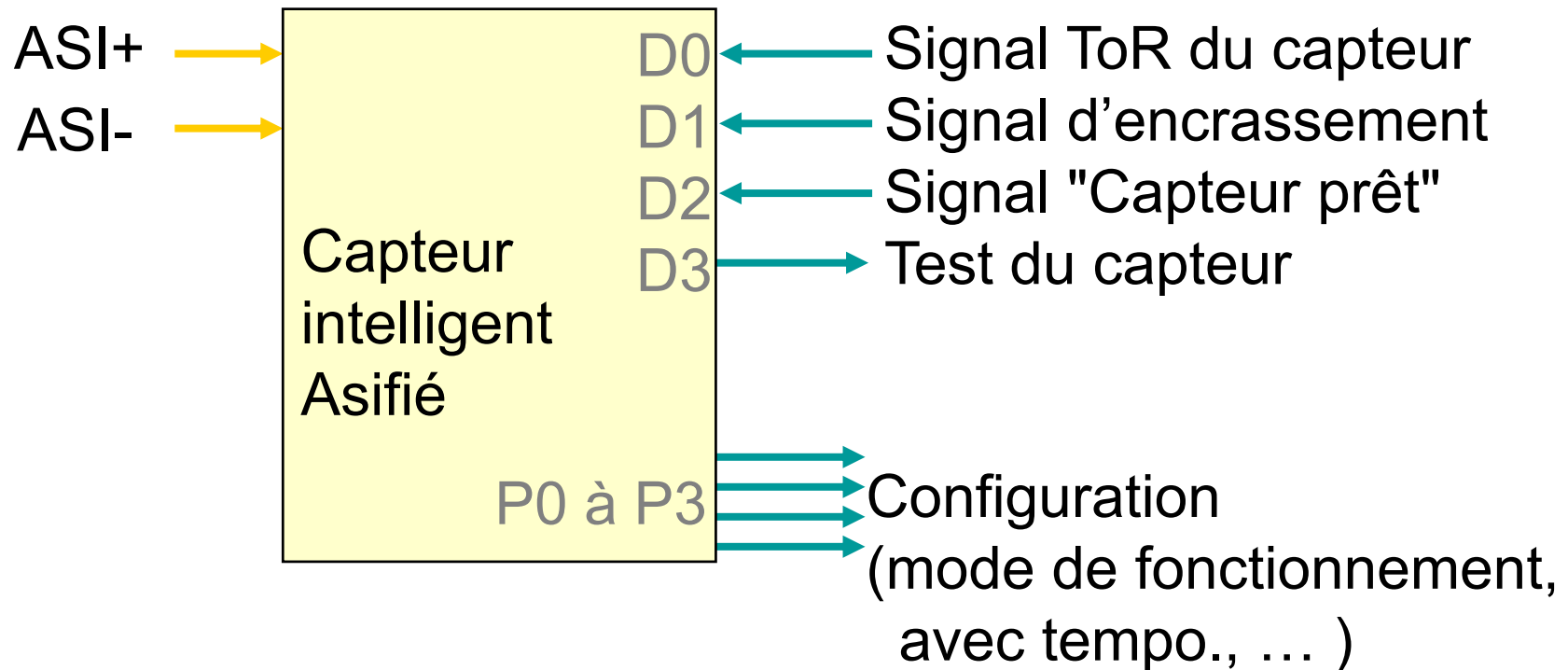


AS-I : Les esclaves

- Registres des esclaves :
 - Adresse actuelle 5 bits
 - Reg. de configuration E/S et id. 4 bits
 - Reg. de données de sorties 4 bits
 - Reg. de paramètres 4 bits
 - Reg. de réception 12 bits
 - Reg. d'émission 5 bits
 - Reg. de statuts et d'erreurs 4 bits
-
- 38 bits

AS-I : Esclave intelligent

- Utilisation des 4 bits de communication



Profils

- Identification de chaque esclave par un profil X.Y :

Y: Identification Code
(0 à F)

X:
(I/O Code)

Profils normalisés :

- 0.1: 2 entrées capt.
- 1.1: capt. avec contrôle
- B.1: 2 action. avec retour
- D.1: action. avec contrôle

	D0	D1	D2	D3
0	IN	IN	IN	IN
1	IN	IN	IN	OUT
2	IN	IN	IN	IN/OUT
3	IN	IN	OUT	OUT
4	IN	IN	IN/OUT	IN/OUT
5	IN	OUT	OUT	OUT
6	IN	IN/OUT	IN/OUT	IN/OUT
7	IN/OUT	IN/OUT	IN/OUT	IN/OUT
8	OUT	OUT	OUT	OUT
9	OUT	OUT	OUT	IN
A	OUT	OUT	OUT	IN/OUT
B	OUT	OUT	IN	IN
C	OUT	OUT	IN/OUT	IN/OUT
D	OUT	IN	IN	IN
E	OUT	IN/OUT	IN/OUT	IN/OUT
F	I/O/NUL	I/O/NUL	I/O/NUL	I/O/NUL

AS-I : Un succès

- Pourquoi le succès d'AS-Interface ?

Certes :

- Boîtiers plus coûteux,
- Nécessite une "petite" formation

Mais :

- Gain en main-d'œuvre "cablage"
- Économie en bureau d'études
(Simplification de la représentation)

AS-I : Passerelles / Composants

- Composants disponibles :
 - AMS (Austria Micro System), circuit ASI3+
 - Composants Siemens
- Passerelles pour :
 - FipI/O
 - Modbus
 - Interbus-S
 - CAN (Device Net)
 - Profibus
 - ...

AS-Interface

- Assoc. "AS-International Association e.V." :
 - promotion, standardisation, certification
 - 65 membres internationaux
 - 8 groupes nationaux

- Membres :

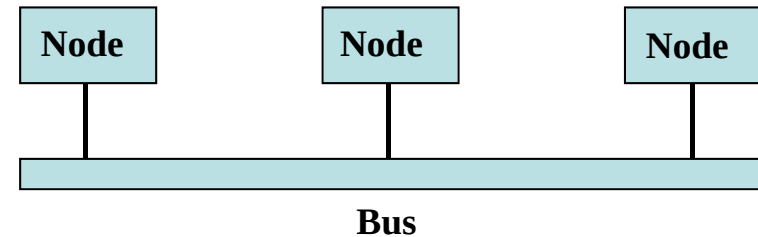
Allen-Bradley	(USA)	EMC	(DK)	Kuhnke	(D)
Allen-Bradley D	(D)	Endress + Hauser	(D)	Lanny	(D)
Amphenol - Tuchel	(D)	Eurotherm	(GB)	Leuze electronic	(D)
Andras	(D)	Festo	(D, GB)	Lumberg	(D, GB)
AUCOTEC	(D)	Fuji	(JP)	Lütze	(D)
Balluff	(D, GB)	FZI Karlsruhe	(D)	Melhardt	(D)
Banner	(USA)	Gavazzi	(CH)	Mitel	(D)
Baumer electric (CH, GB)		Groupe Schneider	(F)	Murrelektronik	(D)
Bernstein	(D)	Gebauer & Griller	(A)	Nixdorf Institut	(D)
Bihl + Wiedemann	(D)	Harting	(D)	Norgren	(GB)
Binder	(D)	Hengstler	(D)	Omron	(NL)
Bosch	(D)	HERION	(D)	Pepperl+Fuchs	(D, GB)
Brad Harrison	(GB)	Hirschmann	(D, GB)	Pepperl+Fuchs NL	(NL)
Bürkert	(D)	Honeywell	(CH)	Phoenix Contact	(D)
Carinthian Tech Res.	(A)	HTL Oensingen(CH)		Puls	(D)
Crouzet Autom.	(F)	ifm electronic	(D, GB)		
Datalogic	(I)	Klöckner-Moeller	(D)	...	
Egemin	(B)	Kostal	(D)		

CAN

CAN : Introduction

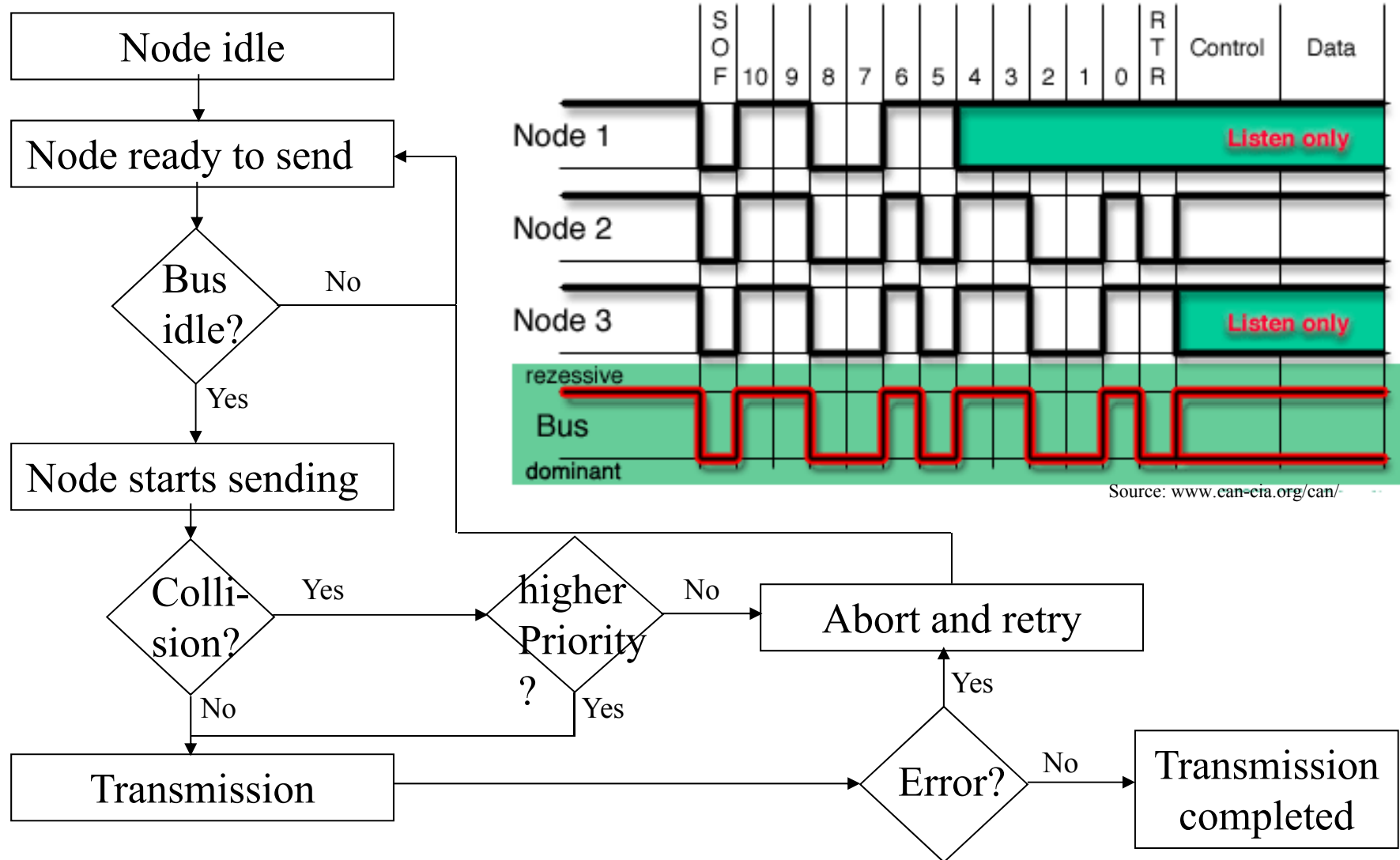
- Historique et généralités :
 - Acronyme de "Control Area Network"
 - Développé par Robert Bosch GmbH et Intel en 1985
 - Destiné à l'automobile mais repris par l'automatisme et le contrôle/commande
 - Respecte le modèle OSI (couches 1 & 2), mais plusieurs couches applicatives possibles
 - Normes :
 - ISO 11898 (haut débit $\geq 125\text{kbit/s}$)
 - ISO 11519 (faible débit $<125\text{kbit/s}$)

The CAN protocol



- Developed in 1983 for the use in motor vehicles
- **Serial multi-master bus:** every node has the same rights, nodes can be added or removed on the fly
- **Data rate:** up to 1 Mbit/s, depending on the bus length (1Mbit/s on 40m)
- **Message-oriented:** every message has an **identifier** that describes its content
- **Broadcast:** messages are sent to every node
- **Static priorities:** message priority defined by the identifier
- **Arbitration:** bitwise using the identifier
- **Error detection:** every node observes the bus
undetected error probability $< 4.6 * 10^{-11}$
- **Reaction on error:** retransmission of the message, defective nodes are excluded from the network
- **Node synchronisation:** at the beginning of each message, bit stuffing for resynchronisation

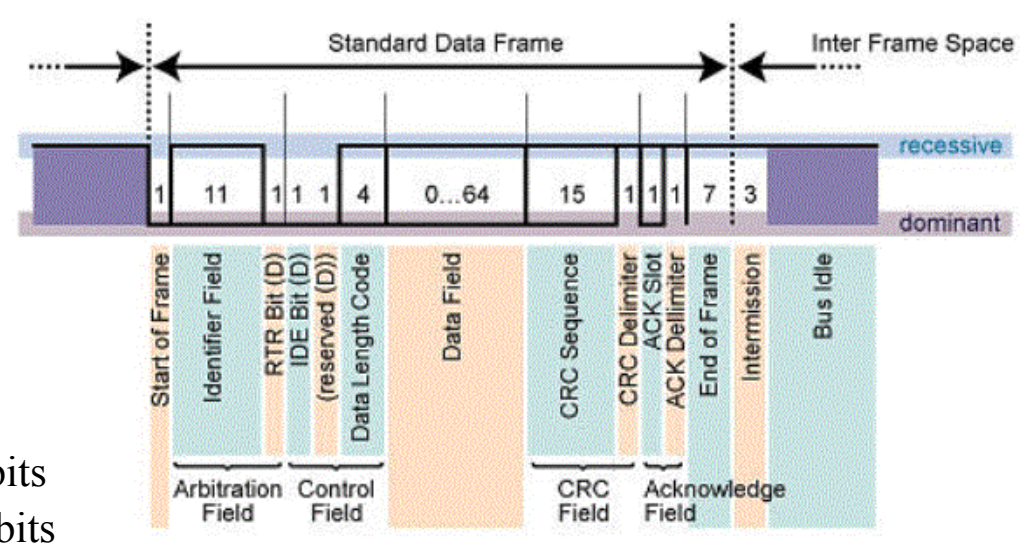
The CAN protocol: Arbitration process



The CAN protocol: frame types

■ Data frame:

- ❑ Fixed format messages of different length
- ❑ Up to **8 bytes user data**
- ❑ Two frame formats: standard (11 bit identifier), extended (29 bit identifier)
- ❑ Frame length:
 - standard: up to **108 bit** + stuffing bits
 - extended: up to **126 bit** + stuffing bits



Source: www.microcontroller.com/learn-embedded/CAN1_sie/CAN1big.htm

■ Remote frame:

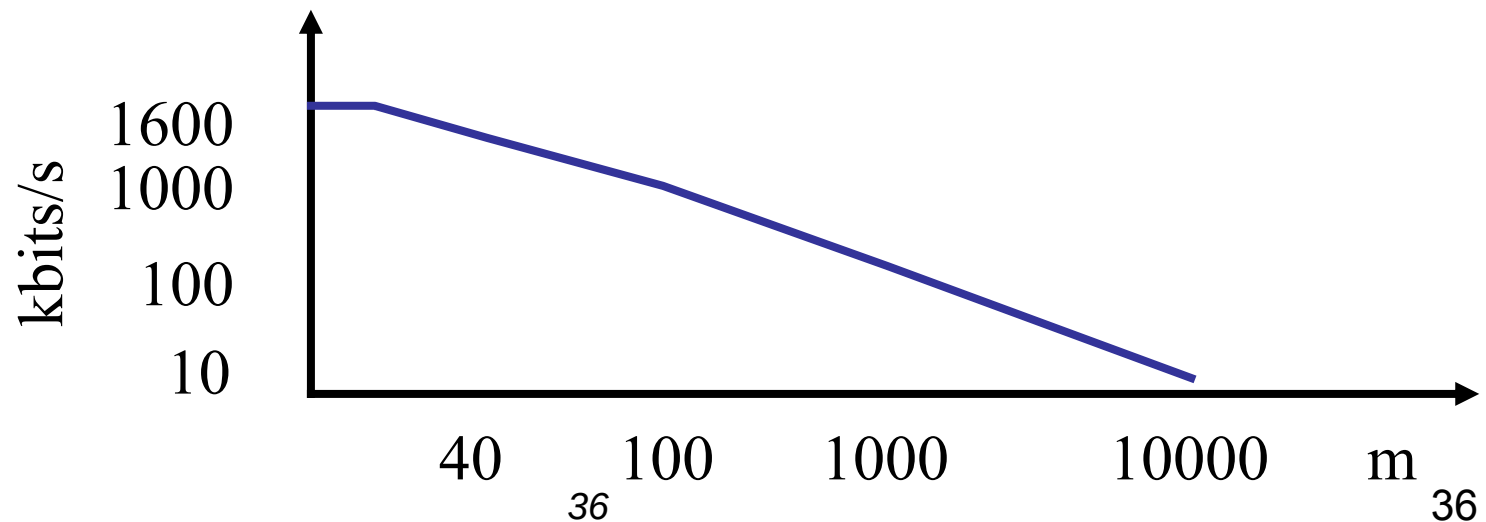
- ❑ Used when a node requests data
- ❑ Send identifier that matches the identifier of the requested data frame

The CAN protocol: frame types

- **Error frame:**
 - Generated when an error is detected
 - Overwrites data on bus
 - **Leads to a retransmission** of the actual frame on the bus
- **Overload frame:**
 - Sent when a receiver wants a delay of the next data frame
- **Interframe space:**
 - Separates data or remote frames
 - Consists of at least 3 recessive bits
 - Shows that the **bus is free**
- **Example:** 31 messages, period 0.01s, each 32 bit user data, standard format
72 bit per data frame + stuffing bits + 3 bit interframe space $\approx$ 80 bit
 $31 * 80 \text{ bit} / 0.01 \text{ s} = 248 \text{ Kbit/s}$

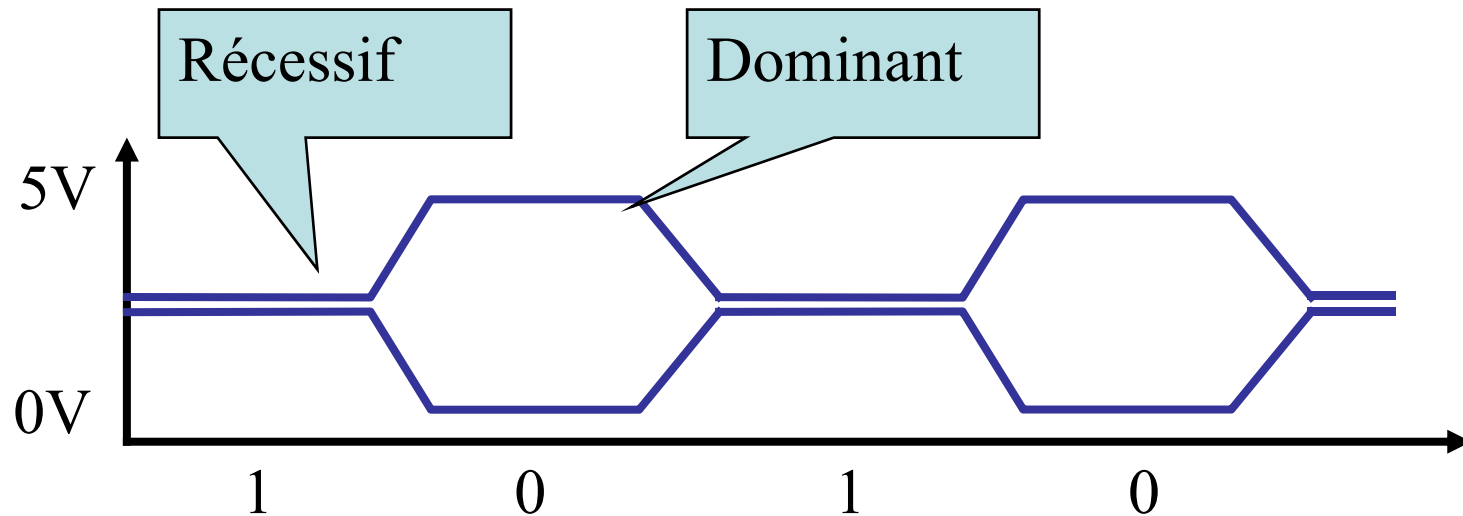
CAN : Couche physique

- Caractéristiques générales :
 - Paire torsadée (120Ω)
 - Codage NRZ, émis en différentiel sur la paire
 - Nombre de nœuds max. env. 100
 - Topologie : bus
 - Contrainte entre débit et couverture :

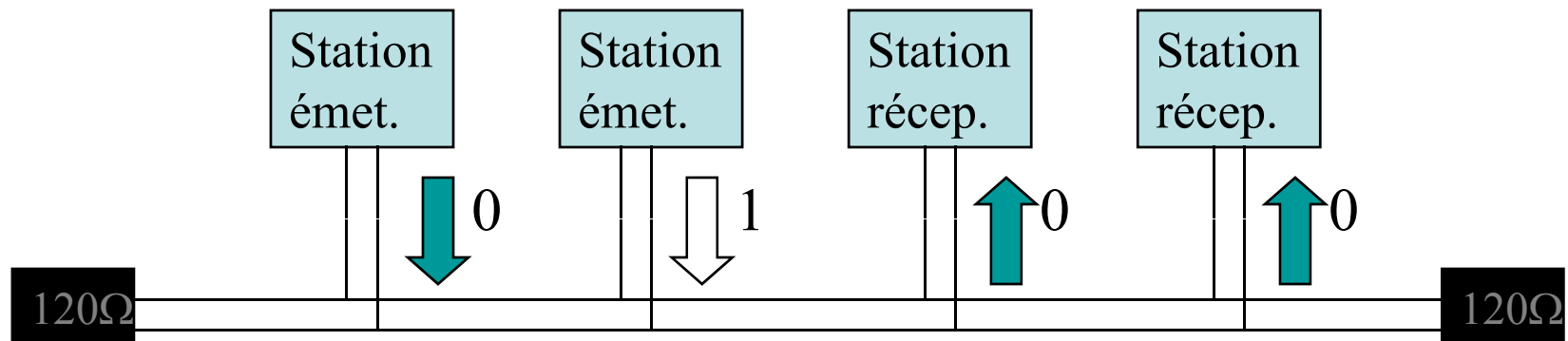


CAN : Couche physique

- Emission sur paire en différentiel



- Principe d'un "ET câblé" pour l'émission :



CAN : Couche de liaison

- Bit de stuffing
 - Obj. : Re-synchroniser les horloges
 - Après 5 bits consécutifs de même valeur, ajout d'un bit de valeur complémentaire

valeurs à émettre 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 0 1 1

valeurs transmises 0 0 0 0 0 1 0 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1

valeurs traitées 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 0 1 1

CAN : Couche liaison

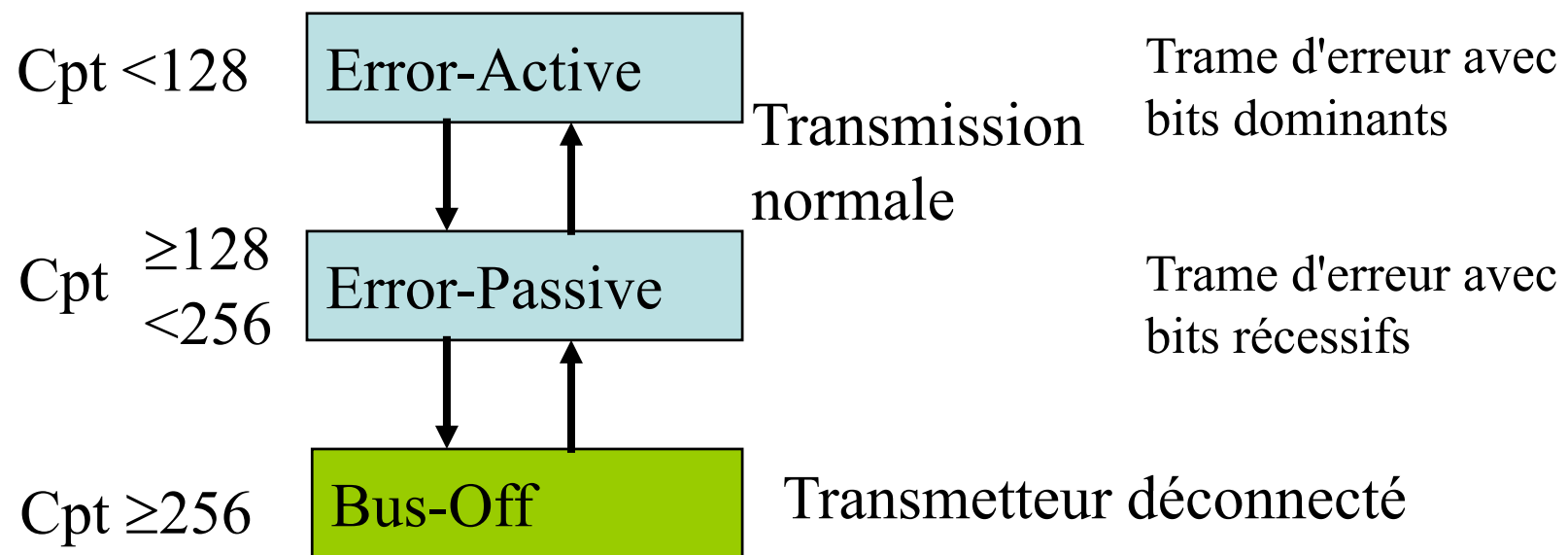
- Les différentes trames :
 - Data frame
Diffusion d'une donnée (ou d'un événement) associée à un identifieur et nécessitant un accusé de réception
 - Remote frame :
Demande de diffusion d'une donnée par l'émission de l'identifieur souhaité
 - Error frame :
Message "sabordé" suite à la détection d'une erreur par l'un des abonnés.

CAN : la détection d'erreur

- Les mécanismes de détection d'erreur
 - Bit error : Valeur du bit émis différent de celui écouté
(inactif pour ID=Arbitrage, et ACK Slot)
 - Stuff error : Absence de bit de stuffing après 5 bits consécutifs de même valeur.
 - CRC error : Non-correspondance entre CRC reçu et CRC évalué
 - Form error : Valeur d'un bit différente de celle attendue
 - ACK error : Absence d'accusé de réception dans ACK Slot
- Taux de couverture :
 - dû au CRC : 3.10^{-5} globalement : 10^{-11}

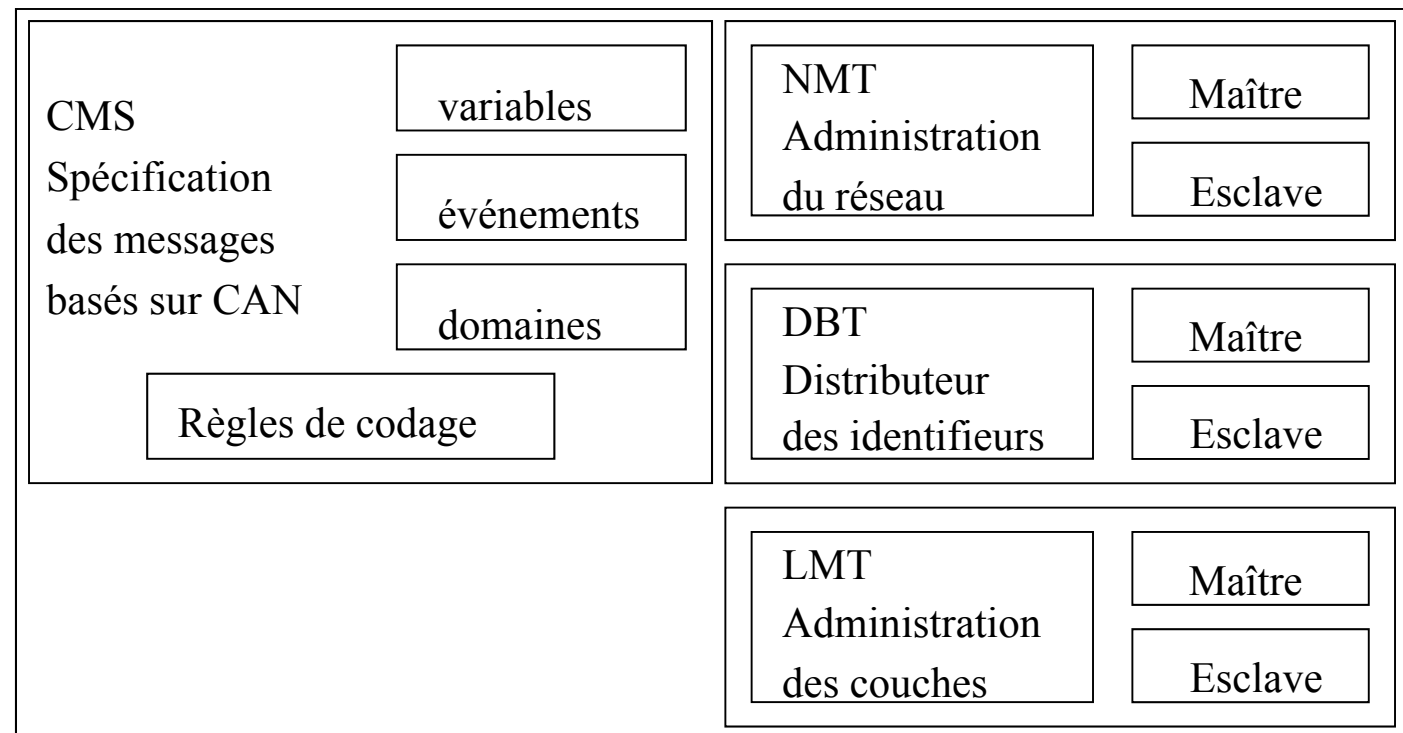
CAN : Confinement d'erreur

- Mécanisme destiné à distinguer les erreurs fugitives de celles permanentes
 - 2 compteurs (1 pour la réception, 1 pour l'émission)
 - incrémentation de 8 à chaque erreur détectée
 - décrémentation de 1 à chaque échange sans erreur



CAL : CAN Application Layers

- Développé au sein du CiA (Can in Automation)
- Destiné à l'administrer le réseau, les objets échangés, les identifiants...



Les éléments de CAL

- CMS : CAN based Message Specification
 - décrit les objets de communication dans un langage standard
 - . CMS_variables : permettent de lire et d'écrire des données
 - . CMS_events : signalent des événements
 - . CMS_domains : permettent le transfert de blocs de données de plus de 8 octets de longueur
 - les communications s'effectuent selon le modèle client-serveur
- DBT : (Identifier) DistriBuTor
 - distribue dynamiquement les identifiants en fonction de la priorité des objets définie par CMS

Les éléments de CAL

- NMT : Network Management
 - spécifie les services généraux de contrôle et d'administration du réseau
 - réalise l'initialisation globale du réseau
 - initialise si besoin , la distribution dynamique des identifiants
 - assure la supervision du réseau pendant son fonctionnement
- LMT : Layer Management
 - définit des services permettant d 'effectuer sur l'étendue du réseau une configuration de certains paramètres de la couche CAL tel que les numéros individuels d'identifiant de nœuds, les paramètres temporels du CAN, etc.

CANopen

- Décrit un concept de réseau basé sur CAN et la couche applicative CAL

CAL fournit les éléments permettant de concevoir une application utilisant CAN comme protocole mais n'indique pas comment ces éléments sont utilisés.

- objectif de CANopen

définir des profils d'instruments pour assurer l'interopérabilité.

=> Device Profiles : offre un standard permettant à chaque fabricant de spécifier son instrument avec le même formalisme.

DEVICE NET

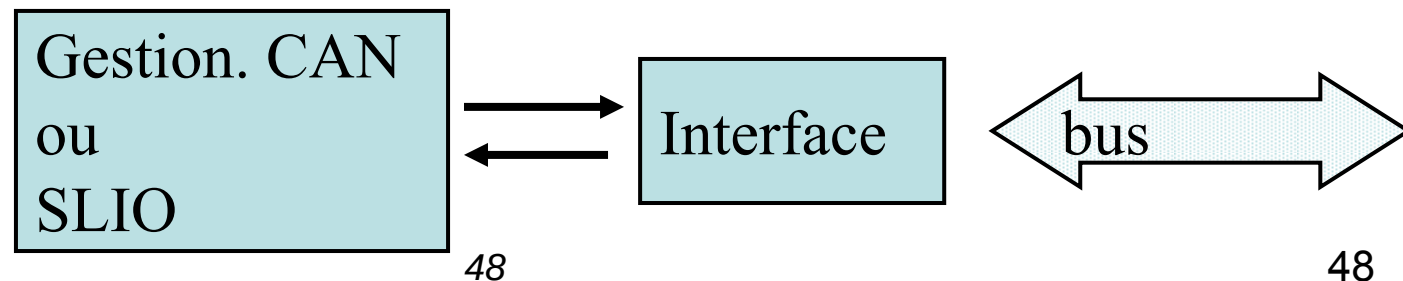
- Conçu et développé par Allen Bradley filiale de Rockwell Automation
- Deux types de messagerie :
 - messagerie implicite ou de haute priorité pour des usages temps réel
 - basée sur le modèle producteur / consommateurs
 - traitement des entrées / sorties
 - messagerie explicite ou de base priorité pour des usages moins fréquents
 - basée sur le modèle client / serveurs
 - reconfiguration, diagnostic d'une station
- Définition de profils de communication

SDS : Smart Distributed Systems

- proposé par Honeywell
- quatre classes génériques de services
 - READ, WRITE : accès aux entrées sorties et à toutes les données visibles sur le réseau de moins de 7 octets
 - EVENT : permet aux entrées de faire connaître leurs états sans être interrogées.
 - ACTION : permet aux éléments d'administration du réseau de lancer des ordres
- détection automatique de débit
- cartographie automatique
- initialisation automatique d'un nouvel élément
- définition de Device Model (approche orientée objet)

Les composants CAN

- Gestionnaires de protocoles :
2 types selon leur capacité à assurer ou non le décodage et la génération du protocole.
- SLIO (Serial Linked Input Output) :
Constituant des nœuds autonomes (esclaves) assurant des fonctions d'entrées/sorties
- Interfaces de ligne :
Adaptation des signaux au niveau électrique requis par le bus



Les composants CAN

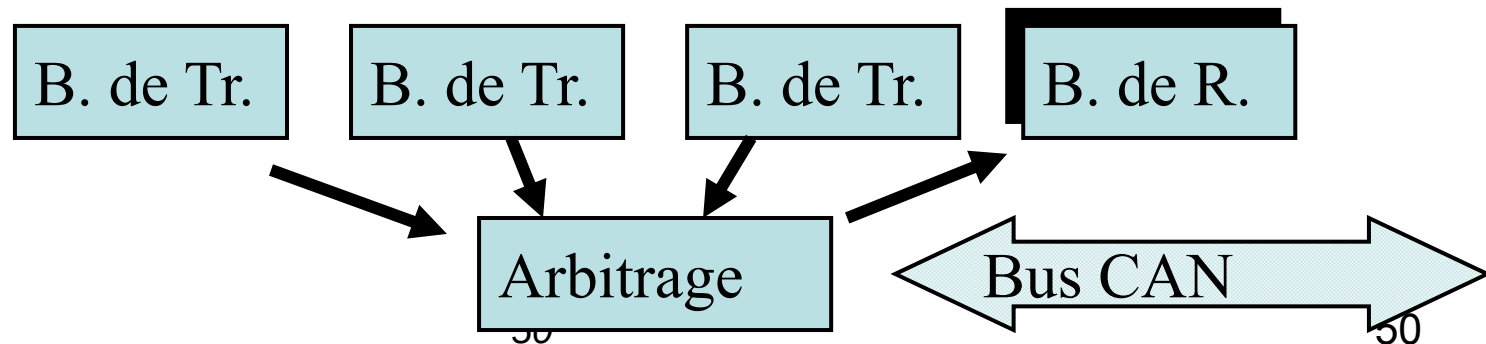
- Gestionnaire de protocole :
 - MCP2510 ($\approx 50\text{€}$ chez RS)
 - SJA1000 (9€ chez RS)
 - 82527
 - Microcontrôleur "canné" :
 - P87C592EFL/02 ($\approx 300\text{€}$ chez RS)
 - 68HC(9)12
 - SLIO :
 - 82C150
 - Interface de ligne :
 - 82C250 (4,57€ chez RS)
- à associer à un microprocesseur

Mise en oeuvre

- Exemple de Microcontrôleur "Canné" :
68HC(9)12 (B32,D60...) de Motorola, Caractéristiques :
 - 32Ko à 60Ko d'EEPROM, 1 à 2 Ko de RAM
 - Entrées : ToR (x16), Analogique (x8), Compteur
 - Sortie : PWM (x4)
 - Communication : série (x2), CAN

Interface CAN :

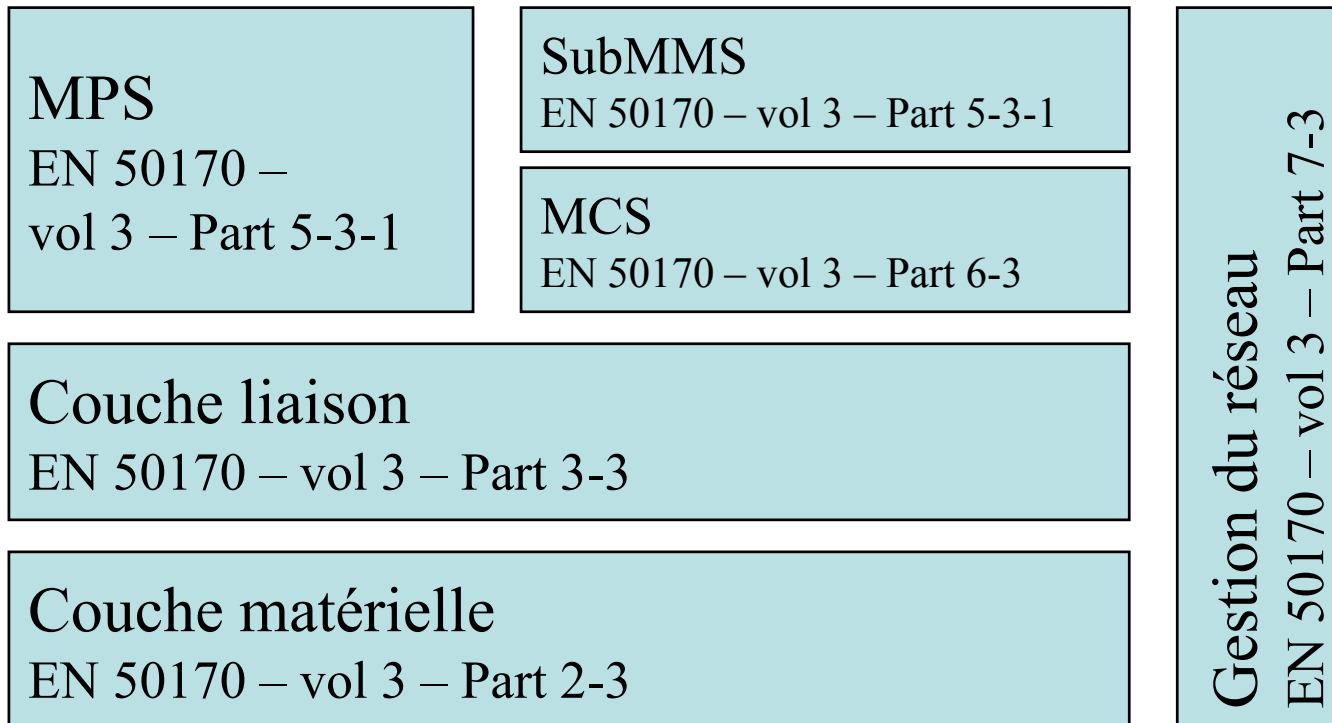
- 3 blocs de transmission, 1 de réception (+ 1 tampon)



WorldFIP

WFip : Un bus normé

- Protocole normalisé (ss-ens. de EN50170)

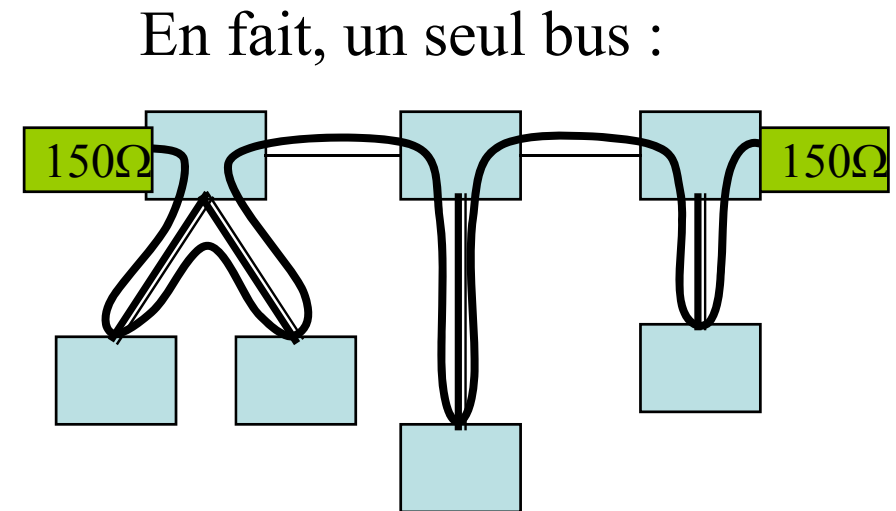
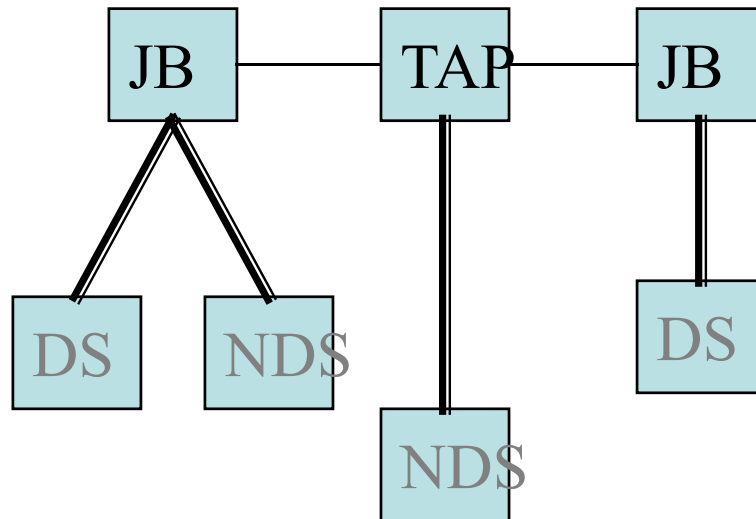


WFip : Couche physique

- Caractéristiques :
 - paire torsadée blindée (150Ω)
 - 32 nœuds max. par segment
 - 4 répéteurs au plus
 - débits :
 - 31,25 kbits/s (1900m)
 - 1 Mbits/s (750m)
 - 2,5 Mbits/s (500m)

WFip : Topologie

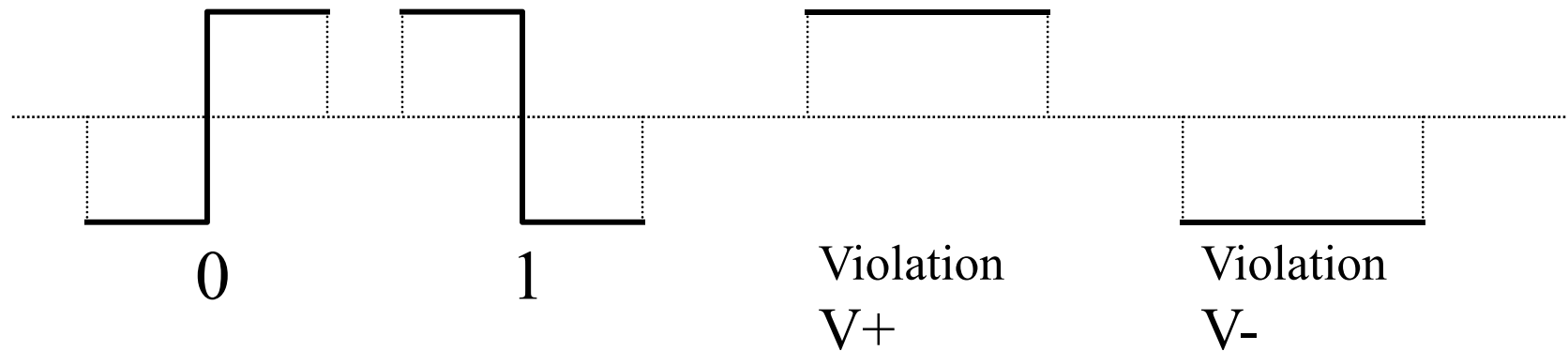
- Toutes topologies possibles (étoiles, bus,...)



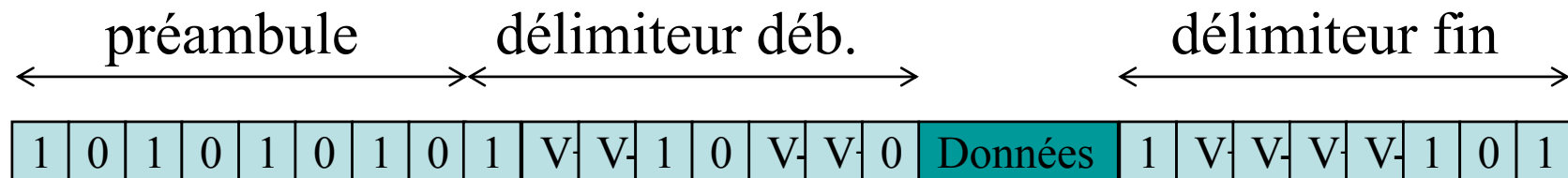
- Distinction abonnés déconnectables (DS)
ou non (NDS)

WFip : Codage

- Codage Manchester :



- Format d'un message (couche phys.)

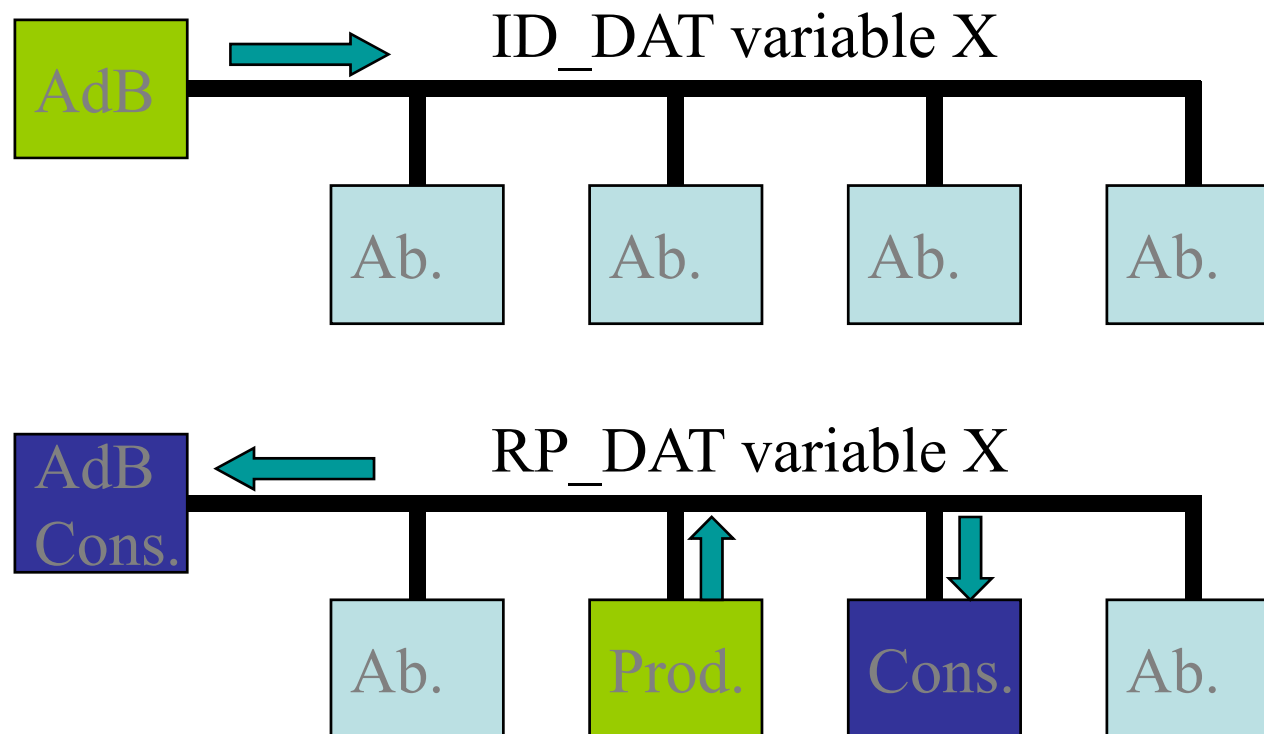


WFip : Couche liaison

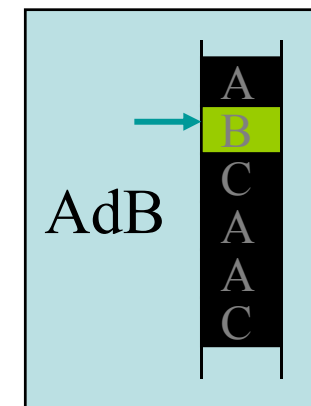
- Les différents types de trame :
 - ID_DAT : demande d'émission d'une var.
 - RP_DAT : émission d'une variable
 - RP_DAT_RQ : émission d'une variable
+ demande d'émission de var. apériodique
 - ID_RQ : demande var. apériodique
 - RP_RQ : émission des demandes apériod.
 - RP_DAT_MSG : émission d'une variable
+ demande d'émission de msg. apériodique
 - ID_MSG : demande d'émission de msg.
 - RP_MSG : émission d'un message

WFip : Mode d'accès

- Emploi d'un arbitre de bus :

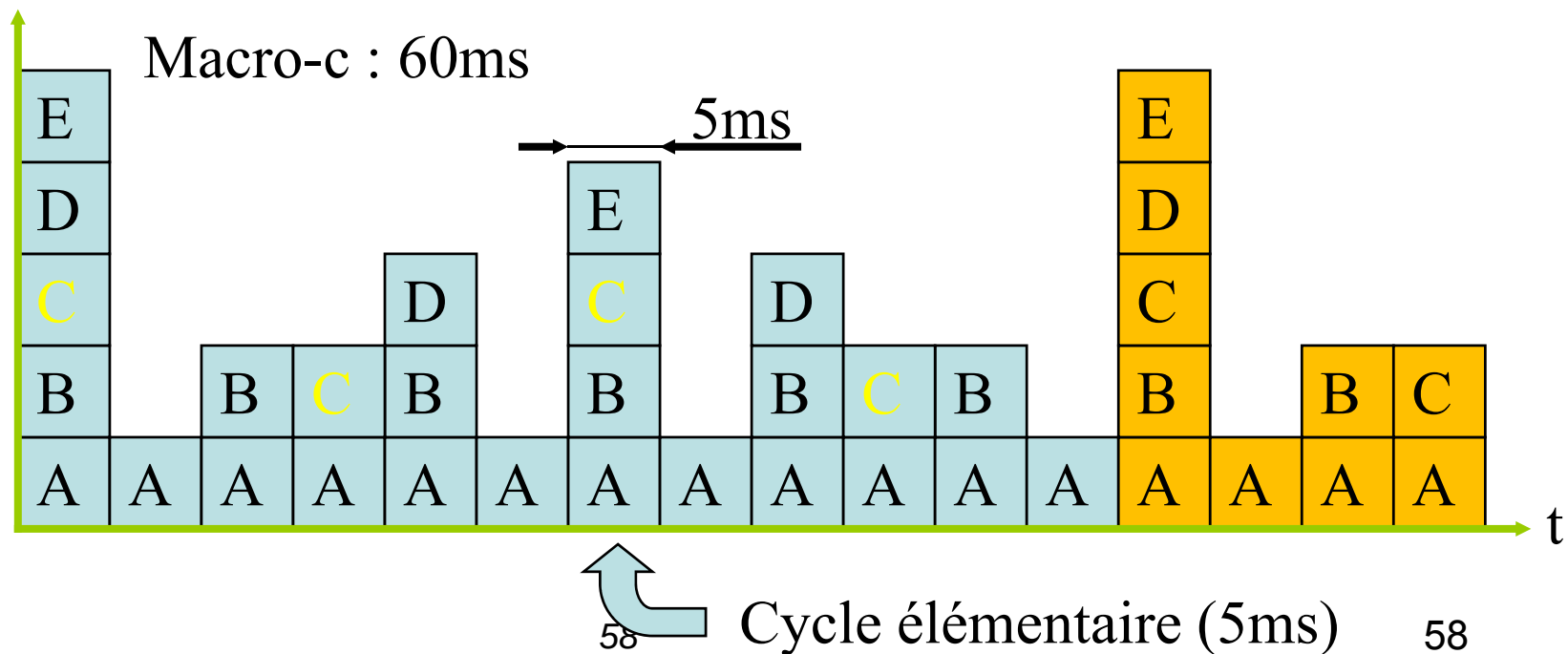


Séquence
des var. à
diffuser



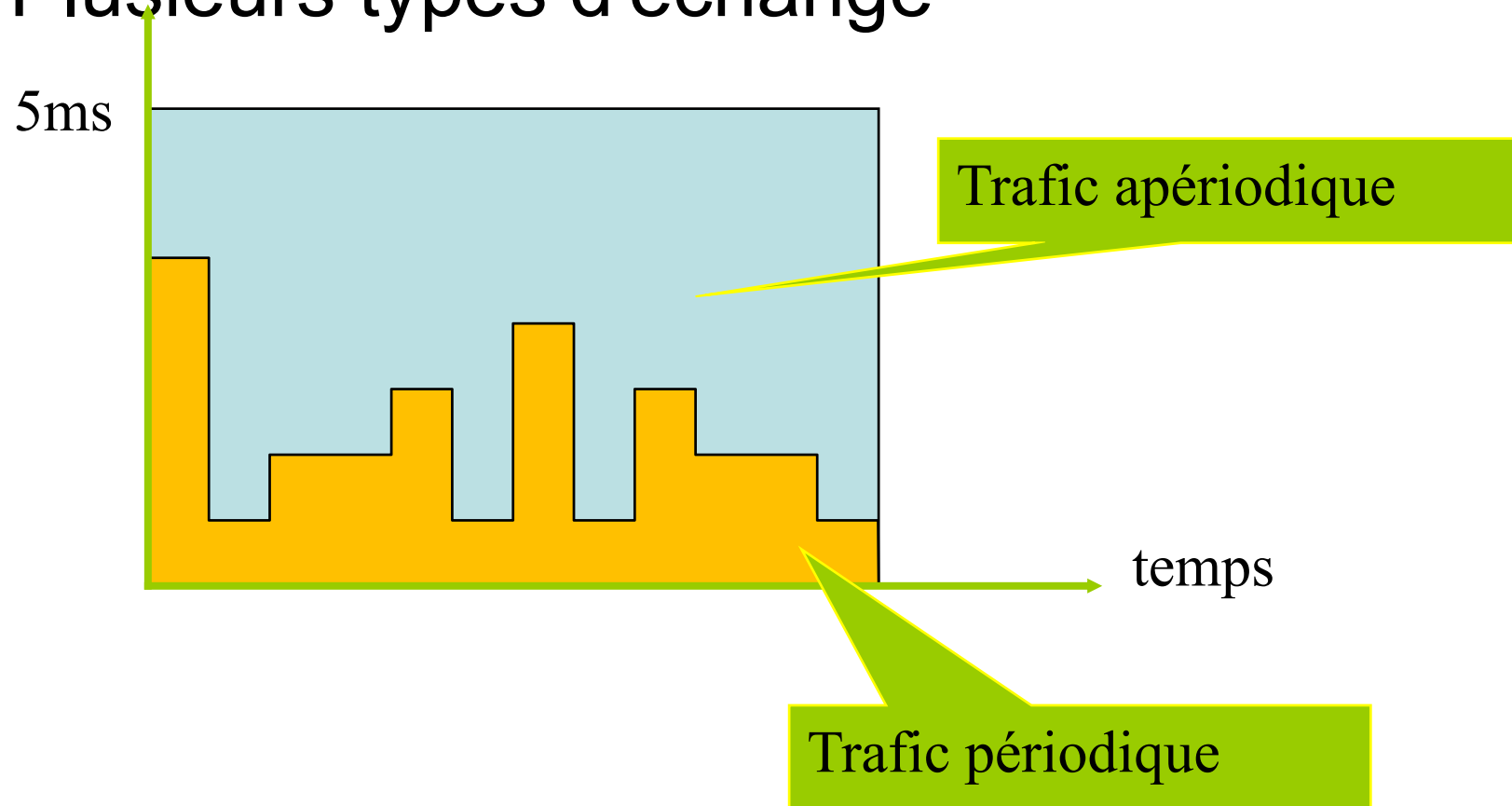
WFip : Arbitre de bus

- Séquence organisée en macro cycle :
 - Liste des variables (exemple):
 Variable : A B **C** D E
 Période : 5 10 **15** 20 30(ms)
 - Macro cycle correspondant :



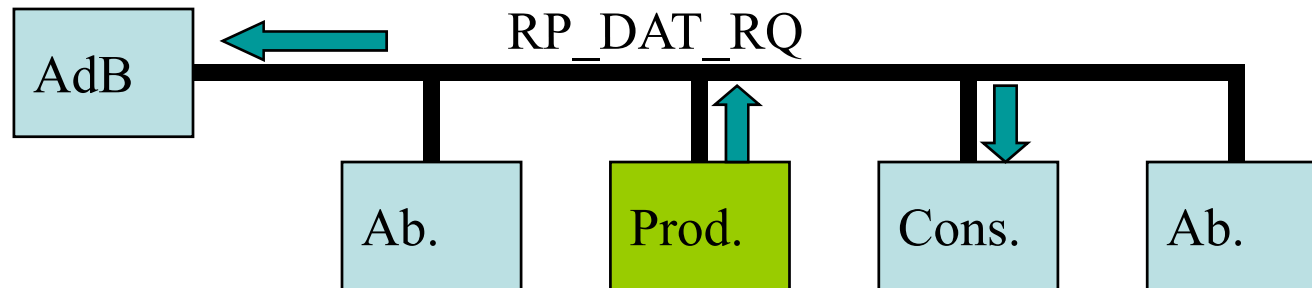
WFip : différents trafics

- Plusieurs types d'échange

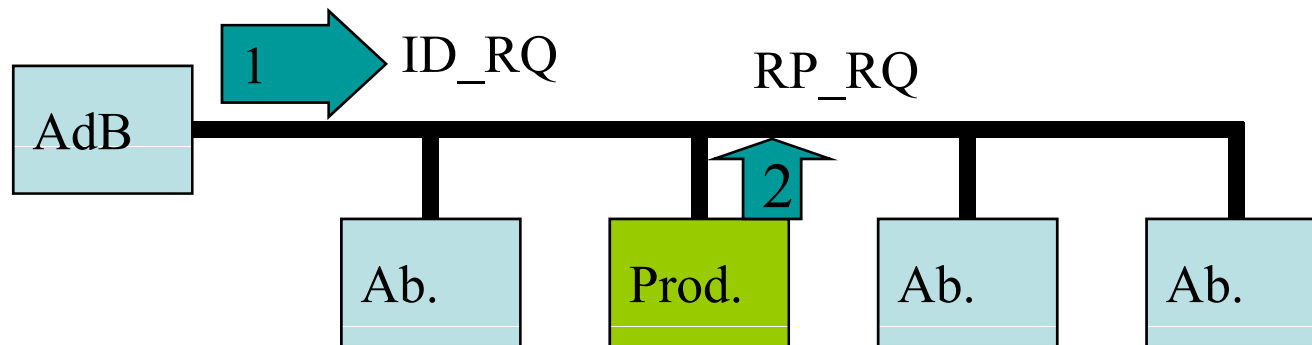


WFip : Trafic aperiodique

- Dans la fenêtre temporelle périodique :
 - émission d'un demande aperiodique de l'abonné



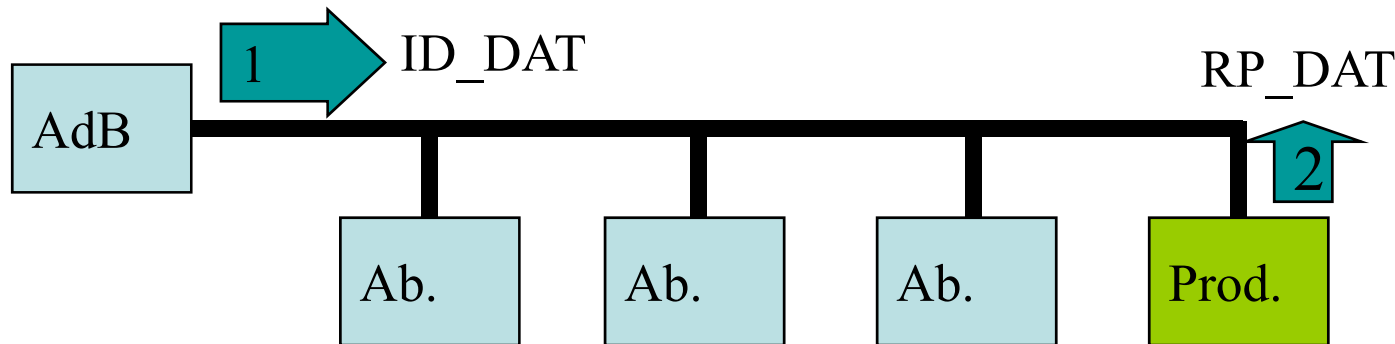
- Dans la fenêtre temporelle aperiodique :



Donne la liste des variables apér. souhaitées

WFip : Trafic aperiodique

- Dernière phase (fenêtre aperiodique)

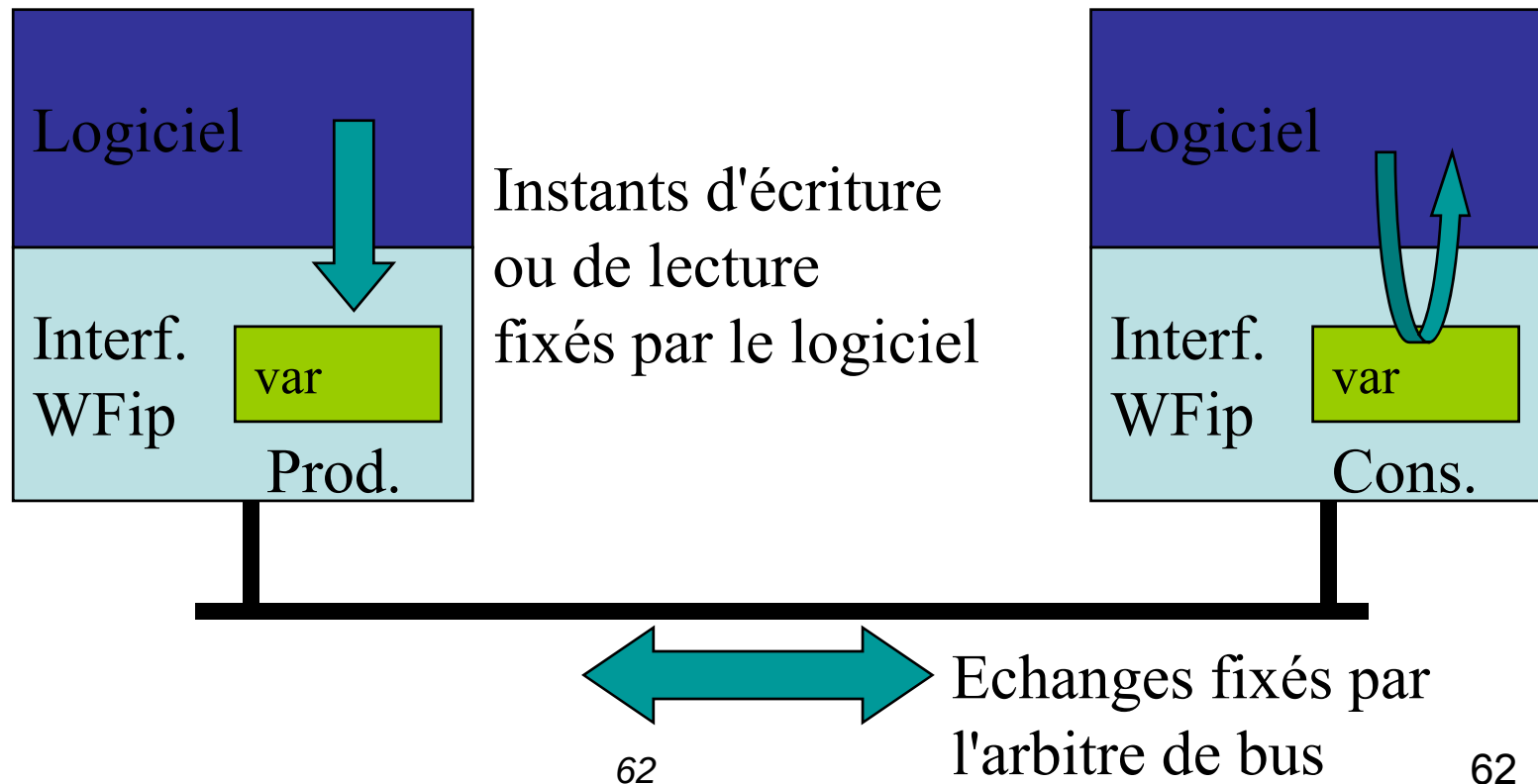


Emission des variables (sur 1 ou plusieurs cycles)
et uniquement dans les fenêtres temporelles apér.

- Demande de transmission messagerie :
Même principe que pour les variables apér. :
1- demande lors des échanges périodiques
2- transmission dans les fenêtres aperiodiques

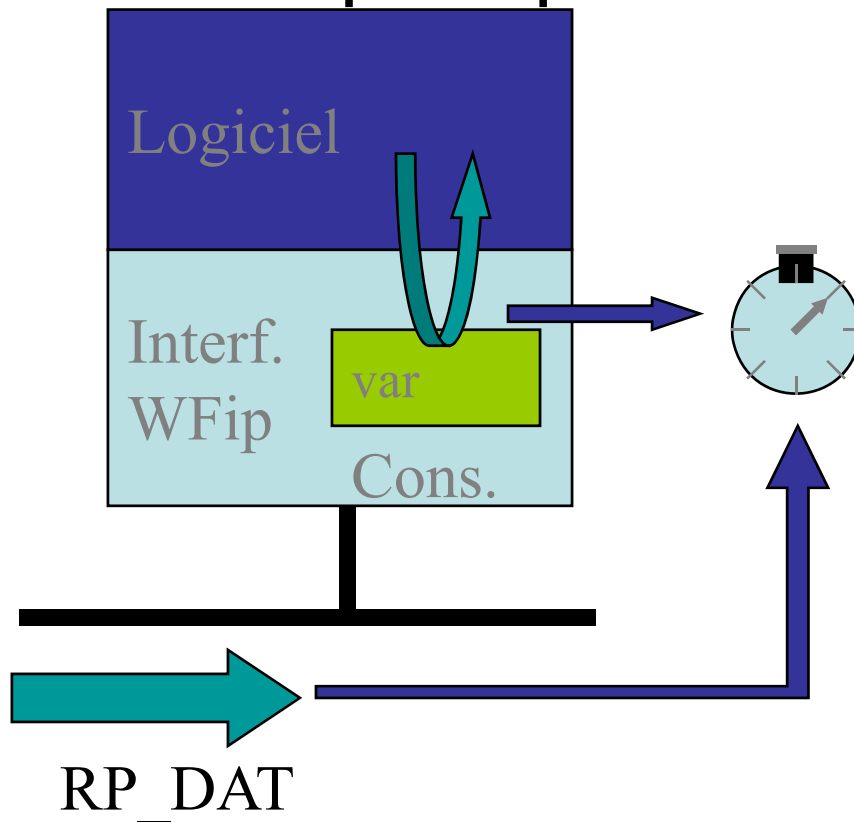
WFip : Couche application

- Statuts de validité temporelle :
 - Ecriture et lecture asynchrone des données par les programmes (→ simplification des accès)



WFip : Couche application

- Statut de promptitude :

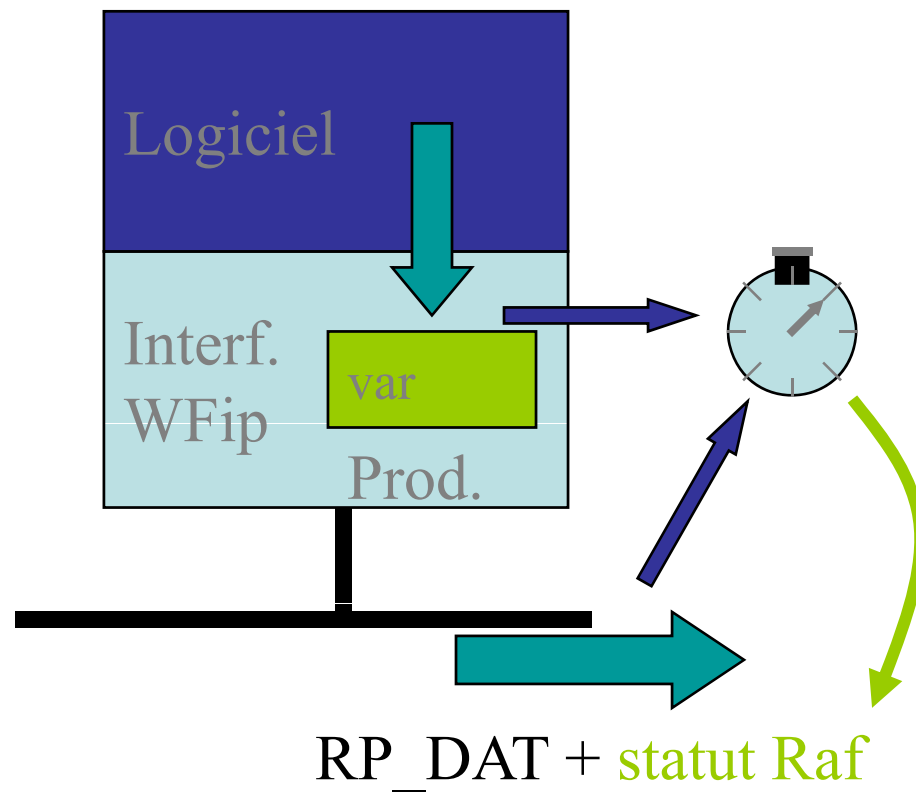


Vérification du délai entre:
-réception de la variable
-lecture de la variable
dans une fenêtre définie

Délai dépassé : FAUX
Délai respecté : VRAI

WFip : Couche application

- Statut de rafraîchissement :



Vérification du délai entre:

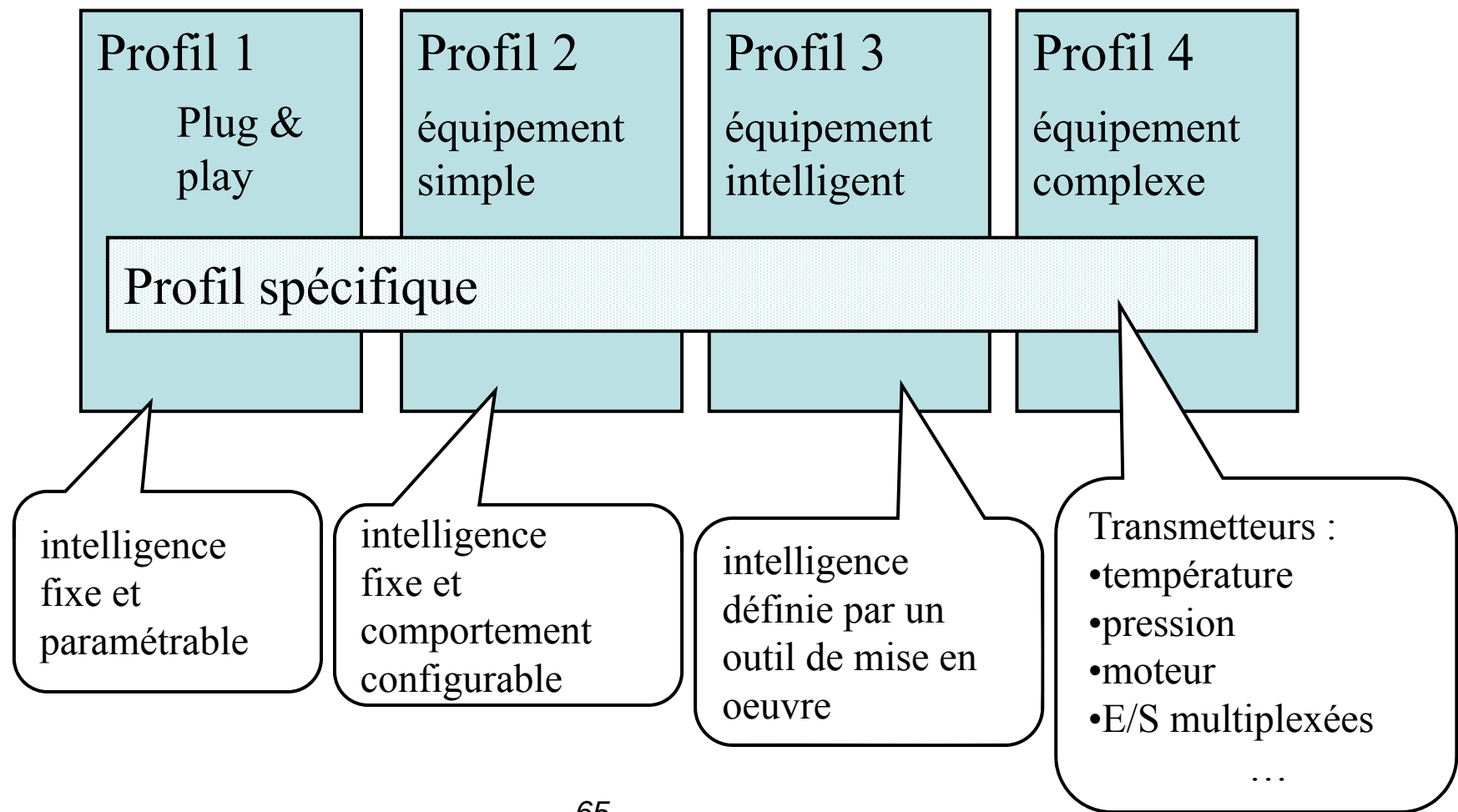
- écriture de la variable
- émission de la variable dans une fenêtre définie

Délai dépassé : FAUX

Délai respecté : VRAI

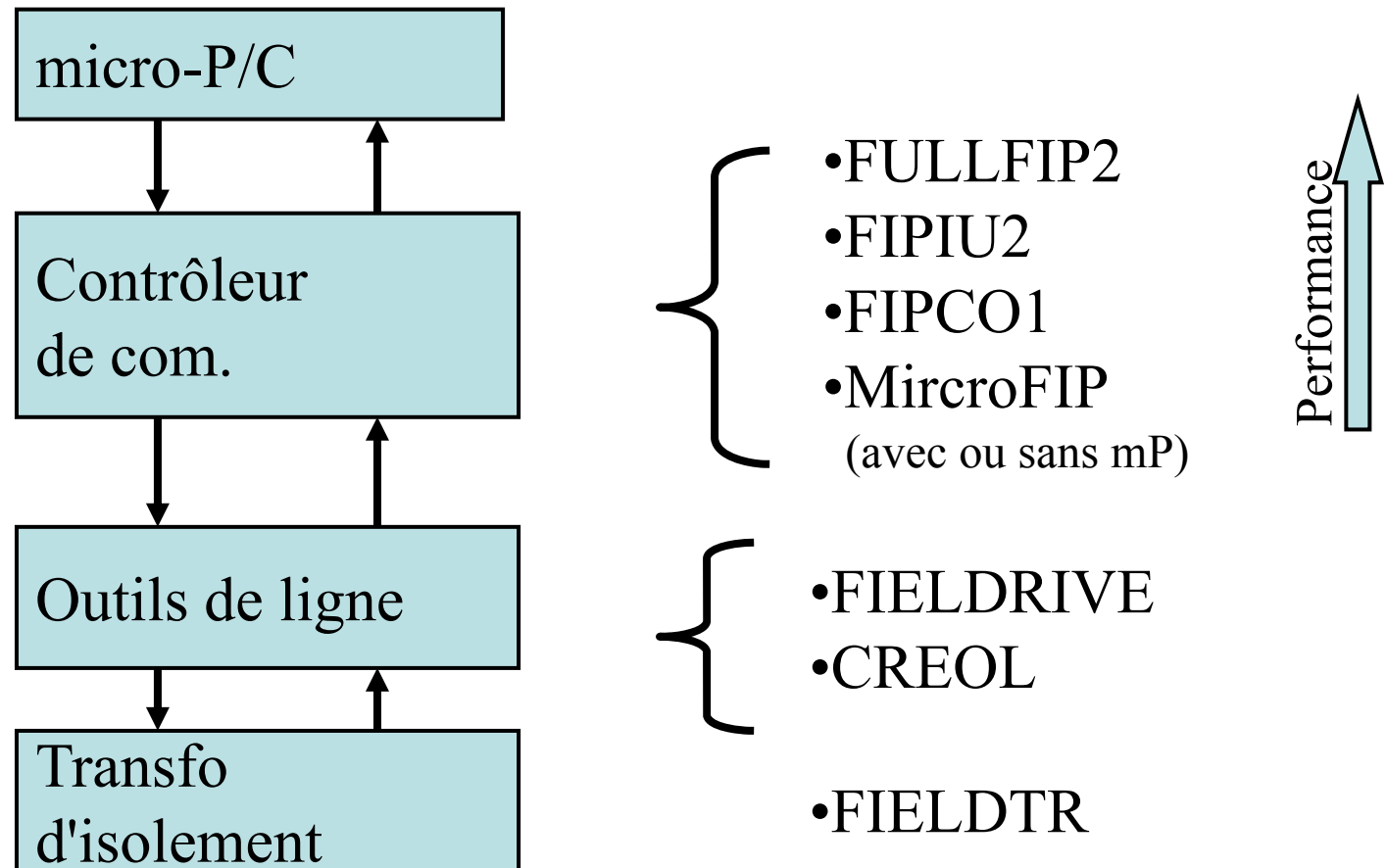
Les profils

- 4 catégories d'abonnés :



WFip : Mise en œuvre

- Architecture générique d'une interface FIP



WFip: Mise en oeuvre

- Exemple MicroFIP :
 - Caractéristiques :
 - Arbitre de bus non-sup.
 - Statuts de Raf/Pr. dispo.
 - Mode Stand-Alone
 - 2 variables
 - 8 E/S
 - pas de messagerie
 - Mode piloté par μP
 - 8 variables
 - messagerie jusqu'à 128 octets



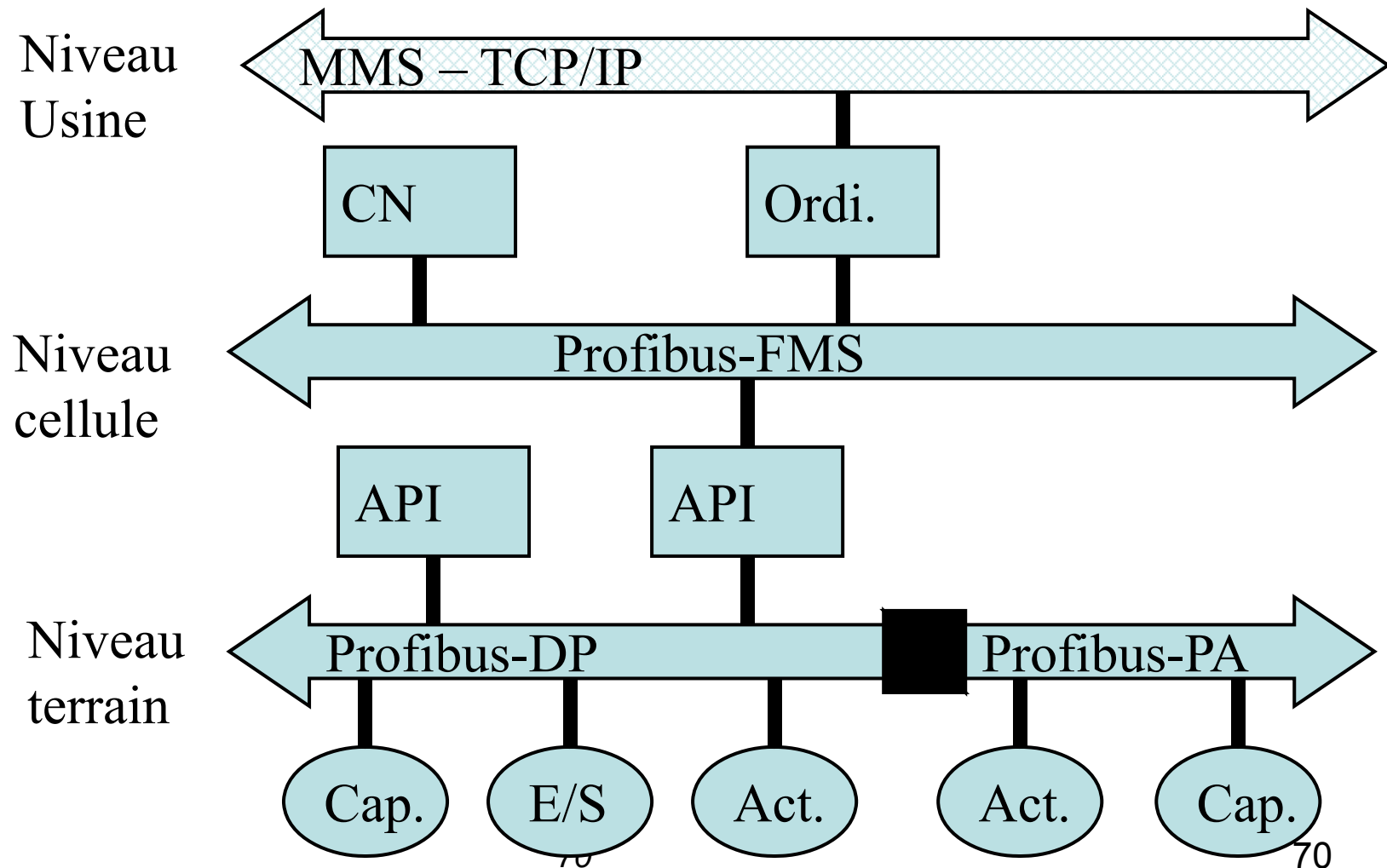
Profibus

Profibus : généralités

- Développé par Siemens, Bosh Knöchner, Müller
- Objectif : fournir un réseau pour l'interconnexion :
 - des automates
 - d'un automates avec les capteurs/actionneurs
- Trois versions disponibles :
 - Profibus-DP : destiné au manufacturier
 - Profibus-PA : destiné au process
 - Profibus-FMS : communication entre maitres

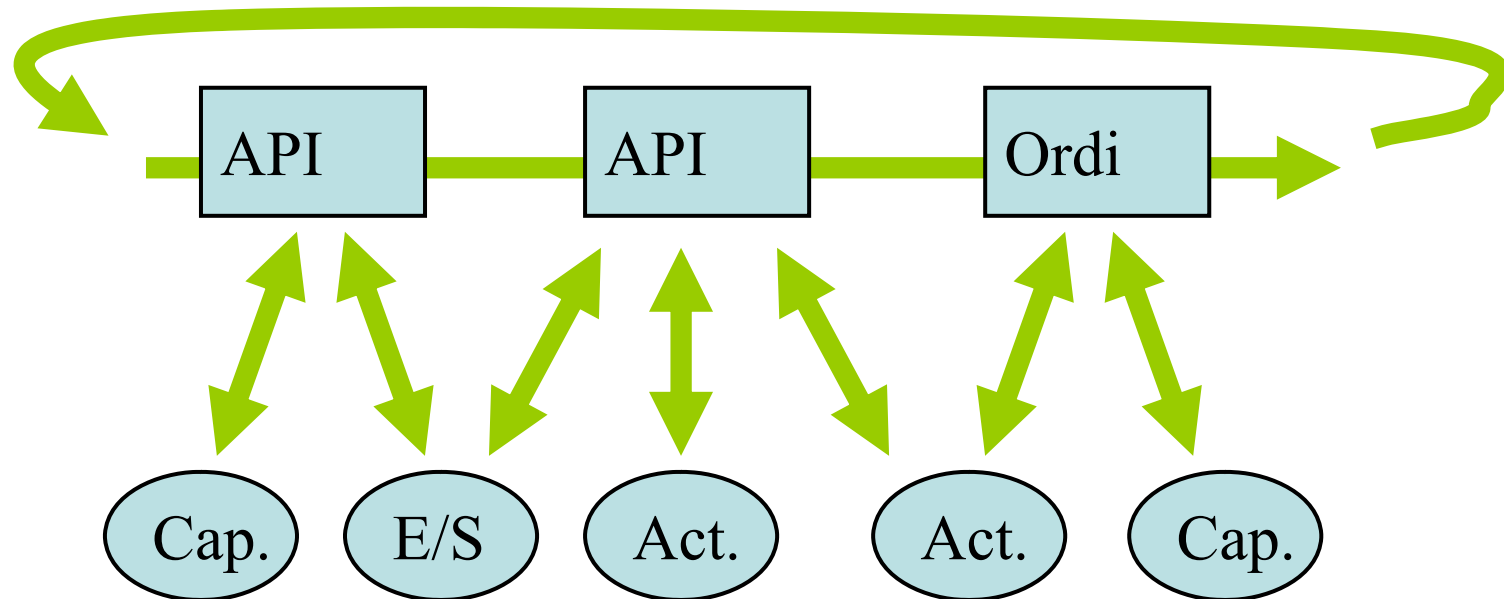
Profibus : un ensemble

- Fournir une architecture complète :



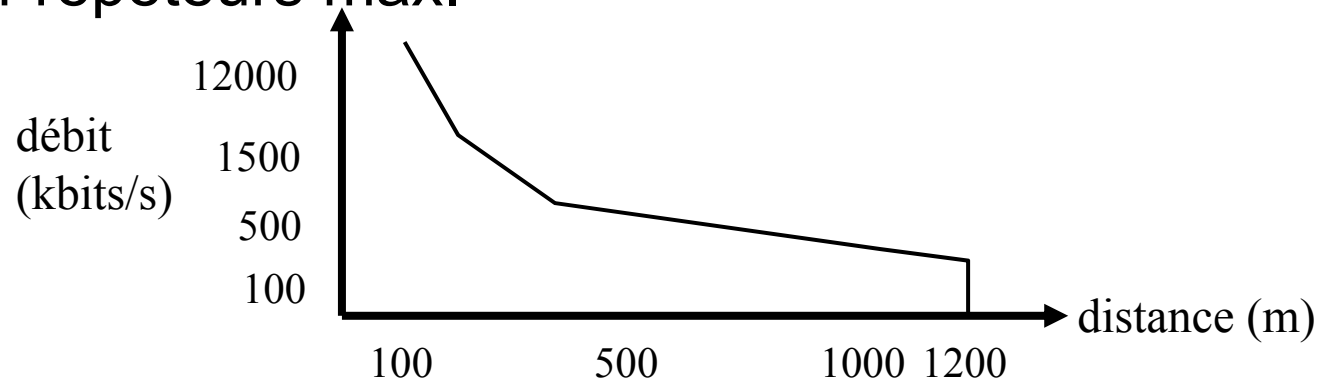
Profibus : principes

- Association de deux méthodes :
 - méthode du jeton
 - communication maître/esclaves



Profibus : couche physique

- Transmission :
 - RS485 : Profibus-DP et FMS
32 stations par segment
4 répéteurs max.



- CEI 1158-2 : Profibus-PA
vitesse : 31,25kbit/s
consommation par stations : 10mA
modulation : ± 9 mA

Profibus : couche liaison

- Méthode d'accès au réseau :
 - Uniforme pour les 3 versions
 - Temps de parole limité pour chaque maître
 - Communication maître-esclaves :
 - Emission avec acq. (FMS)
 - Emission et demande de données (DP, PA FMS)
 - Emission de données ss acq. (DP, PA, FMS)
 - Emission de données cyclique avec réponse (FMS)
 - Communication maître-maître :
par passage du jeton
 - Mécanisme de sécurité :
contrôle de l'intégrité (HD=4)
surveillance du jeton et du retrait/ajout de maître

Profibus (DP) : couche application

- Type d'abonnés :
 - Maître DP de classe 1 = API, PC...
 - Maître DP de classe 2 :
pour la configuration et surveillance du réseau
 - Esclave DP : Bloc d'E/S, Capteurs, Actionneurs
max. : 246 octets en entrées ou en sorties
en lecture : accessible à tous les maîtres
en écriture : 1 seul maître autorisé à la conf.
chien de garde en cas de déf. du maître
- Mode Synchro et Freeze
- Profil :
Esclaves plug&play grâce à des fichiers GSD

Profibus (FMS) : couche application

- Destiné a l'interconnexion d'instruments intelligents (API, PC, IHM)
- Communication maître à maître, Broadcast et Mutlicast
- Transfert de données cycliques et acycliques
- Protocole orienté objet :
 - Dictionnaire d'objets configurés individuellement par équipement
 - Caractéristiques définis pour chaque objet (lecture, écriture...)

Mise en oeuvre

- Implantation de Profibus :
 - en principe relativement simple (UART)
 - ASIC conseillé pour débit élevé ou CEI 1158-2
- Composants proposés :

IAM	PBS	Esclave FMS,DP
	PBM	Maître FMS,DP
Motorola	68302	mP16, Maître/esclave FMS,DP
	68360	mP32, Maître/esclave FMS,DP
Siemens	SIM1	modem pour PA
	SPC4	Esclave FMS, DP, PA
	ASPC2	Maître FMS, DP, PA

Interbus-S

Interbus : Généralités

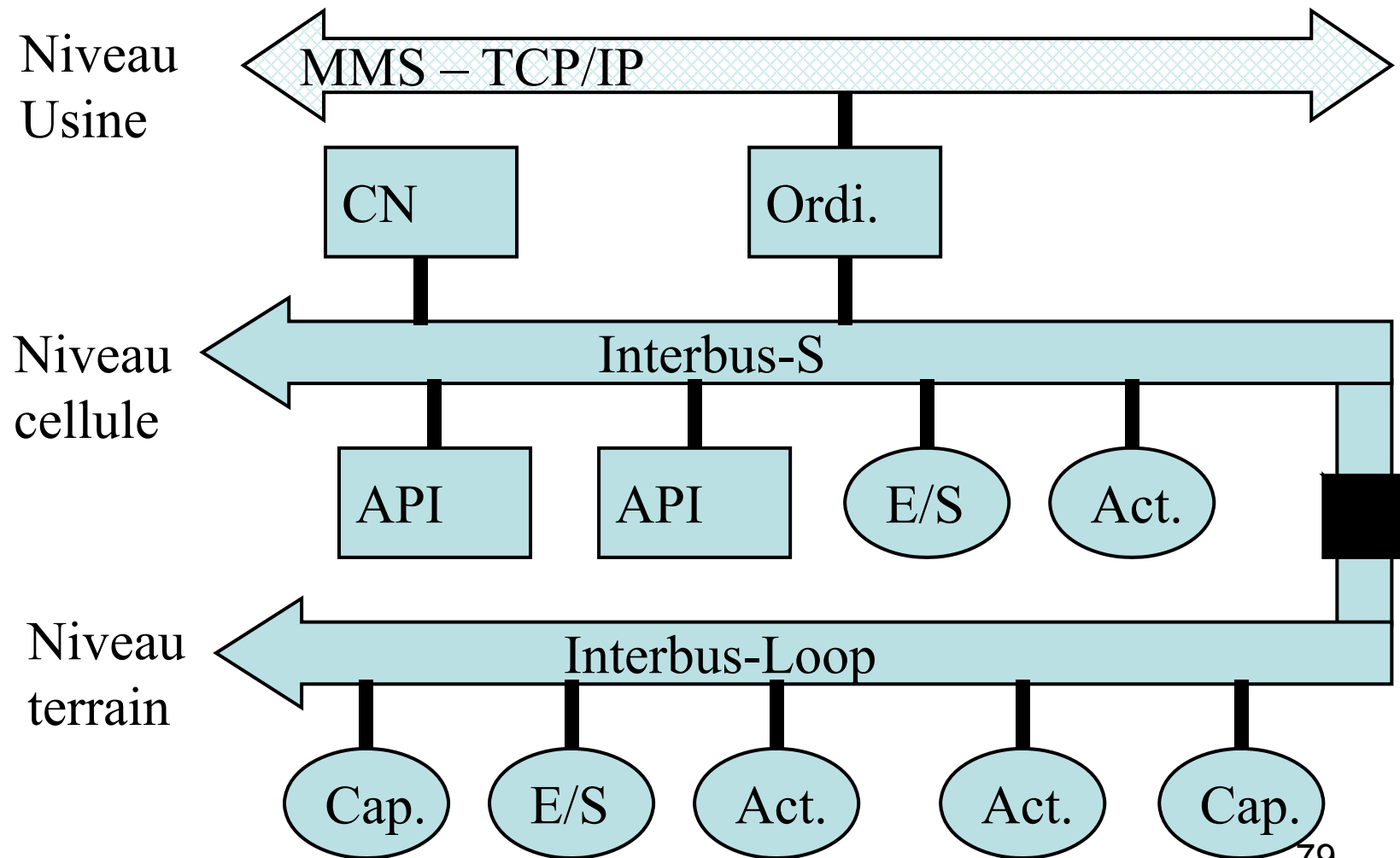
- Standard de fait développé par Phoenix Contact
- Norme : DIN E 19258
- Club Interbus (Assoc 1901)

Promouvoir Interbus en France et assurer un soutien technique

Membres : AEG Schneider Automation, Atermation, Balogh, Festo, Lutze, HD Technology, IBM, Jahnisch & Klass, Joucomatic, Klockner Moeller, Lenze, Murrelektronik, Parker, Phoenix Contact, Wizcon

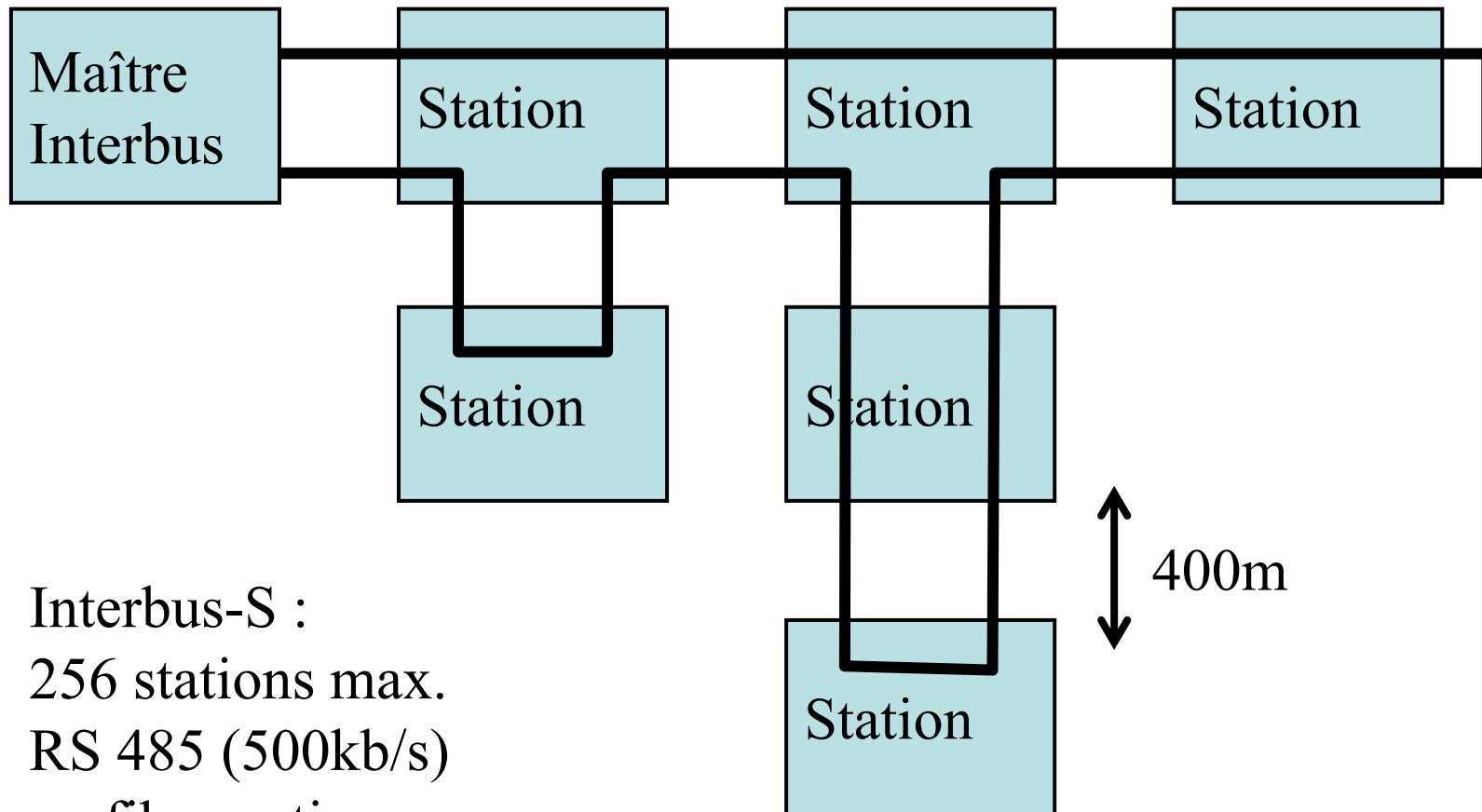
Interbus : solution complète

- Plusieurs niveaux



Interbus : Couche physique

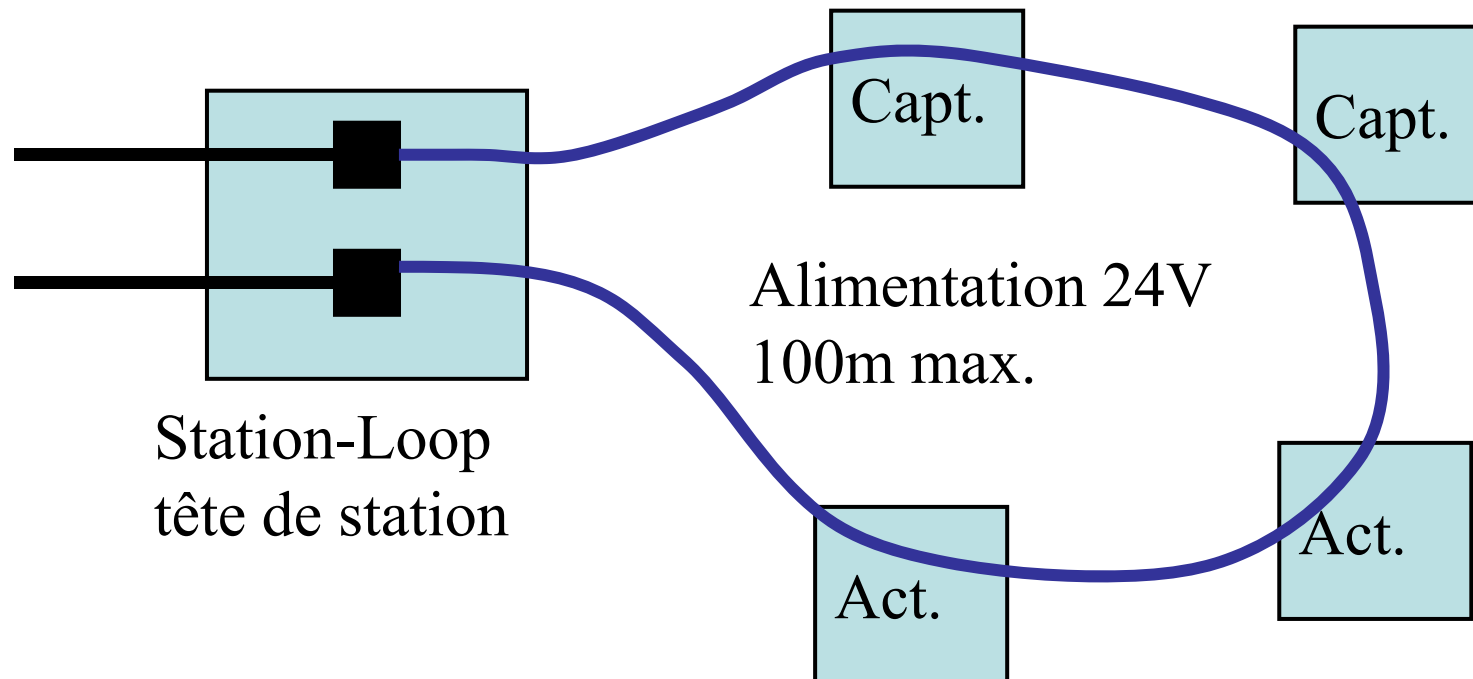
- Topologie : un anneau



Interbus-S :
256 stations max.
RS 485 (500kb/s)
ou fibre optique

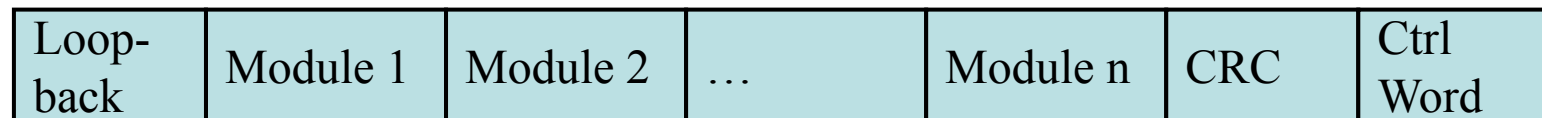
Interbus : Couche physique

- Interbus-Loop : Prolongement d'Interbus-S pour les capteurs et actionneurs :

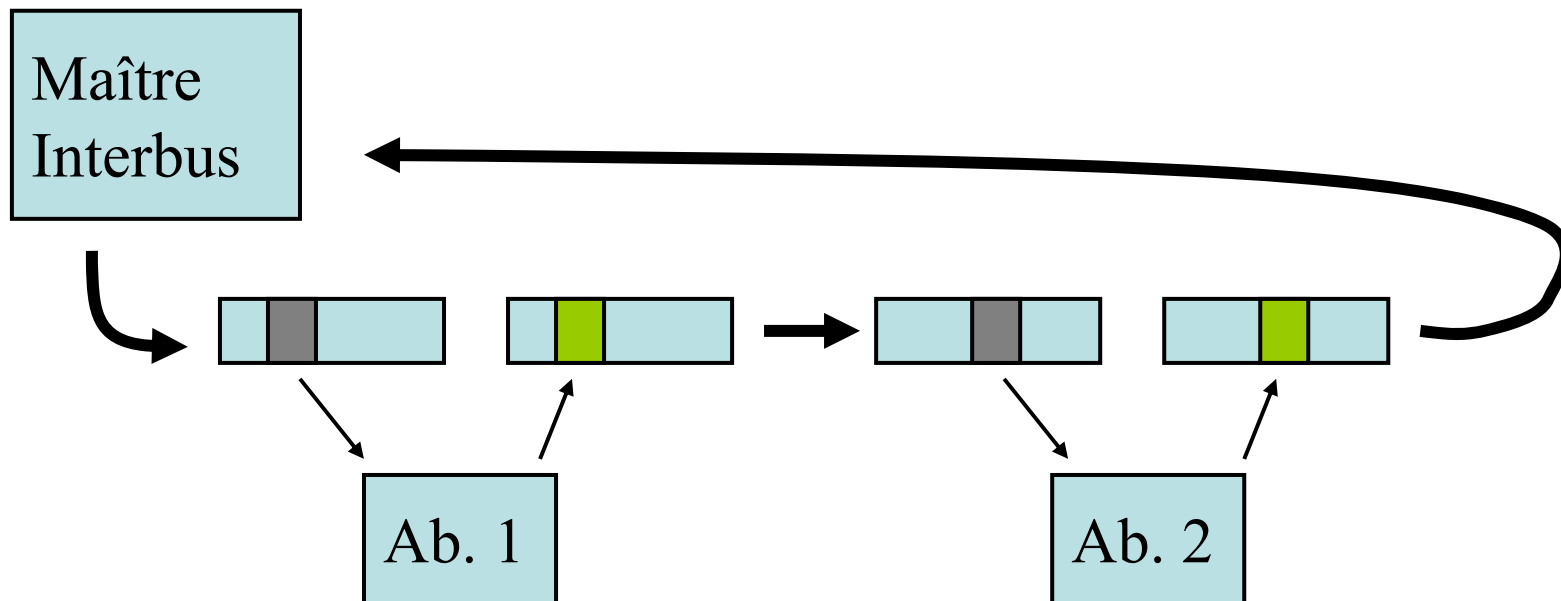


Interbus : couche liaison

- Une seule et unique trame :

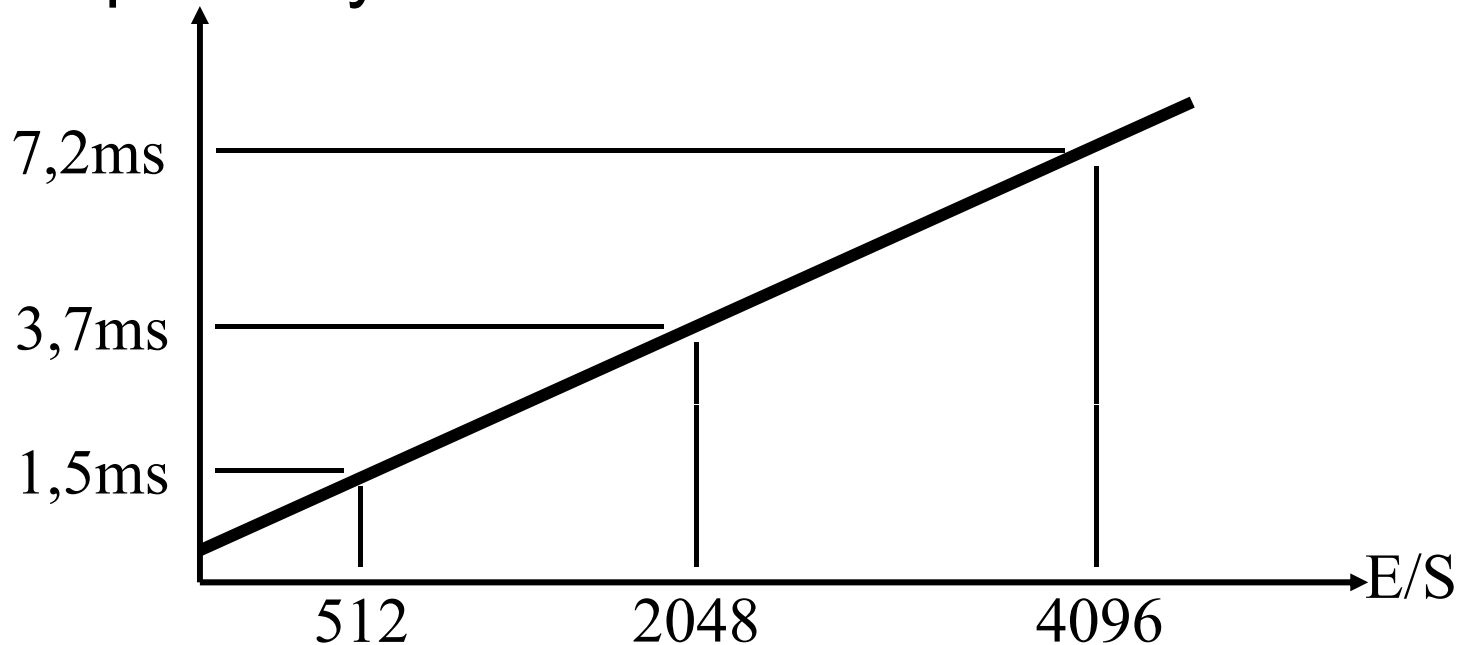


- Un champ par abonné :



Interbus : couche liaison

- Communication type maître/esclave
- Efficacité $\approx 60\%$
Débit utile = 300 kb/s
- Temps de cycle déterministe



Interbus : Composants

- Commercialisés par Phoenix Contact :
 - Composants :
 - SUPI 2 ou 3 (8 E et 8 S)
 - SRE 1 (extension SUPI)
 - Cartes maître :
 - IBS MA/B-T (mémoire double accès)
 - IBS MA/5-T / IBS MA/5-T (pour automate)
 - IBS MA/EVA-I (MA/B-T pour PC)
 - Kit :
 1. d'implémentation InterBus
 2. d'évaluation esclave Interbus

Les réseaux de sécurité

La sécurité

- 2 aspects à la sûreté de fonctionnement

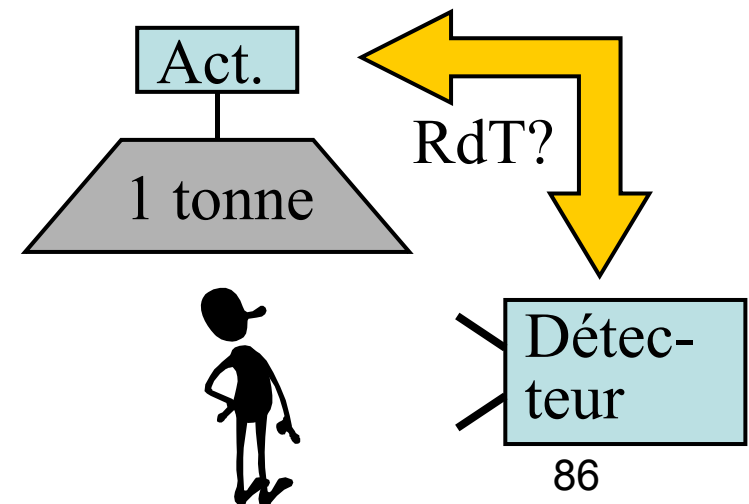
- Fiabilité, Maintenabilité, Disponibilité

Pour les réseaux :

- Offrir des services de surveillance et d'administration du réseau
 - Permettre la mise en place de mécanismes de redondance (maître, médium...), chien de garde...

- Sécurité

Assurer la non-occurrence d'événement dangereux



La sécurité & Réseau

- Objectif :
Extension des réseaux de la fonction "conduite" à la fonction "sécurité"
- Intérêts :
 - Gain de mise en œuvre
 - Facilité la détection et la localisation des défauts
- Obstacles :
 - Technique : temps de réponse requis souvent plus réduit que pour la conduite
 - Contrainte : mise en sécurité pour tout défaut
 - Réglementaire : respect des aspects normatifs, besoin d'une certification

La sécurité par niveau

- Classification par niveau (EN 954)

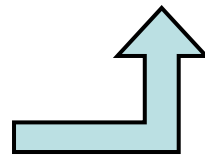
Cat.	Prescriptions / Comportement
B	un défaut peut conduire à la perte de la fonction de sécurité
1	idem mais avec une probabilité moindre grâce à des principes éprouvés
2	un défaut → perte de la fonction de sécurité entre intervalles de contrôle
3	pour un défaut unique, la fonction de sécurité est assurée
4	pour plusieurs défauts, la fonction de sécurité est assurée

La sécurité par niveau

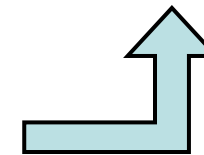
- Quantification proposée (CEI 61508)

Niveau	faible sollicitation	continu
SIL 1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$
SIL 2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$
SIL 3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$
SIL 4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$

probabilité déf.
par sollicitation

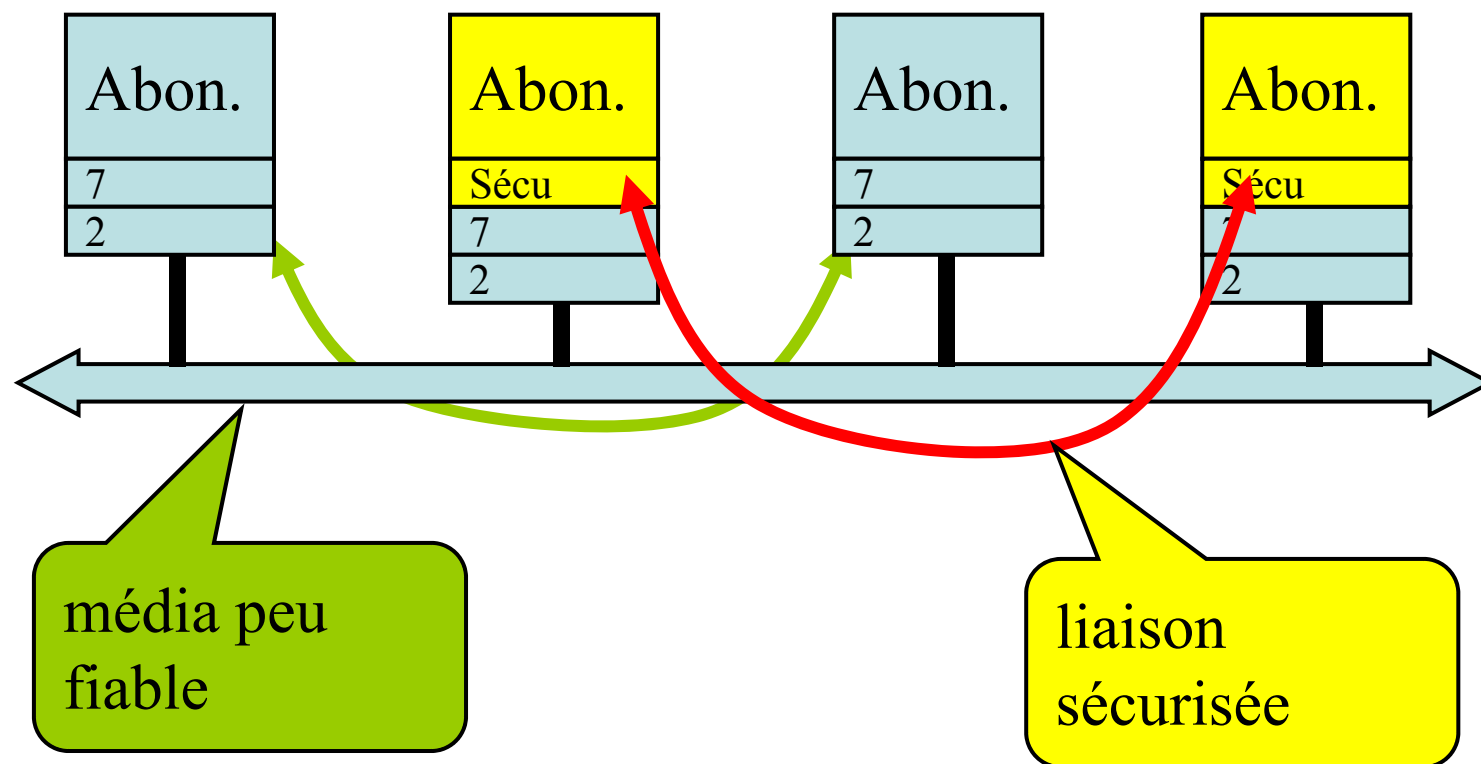


probabilité déf.
dangereuse par h.



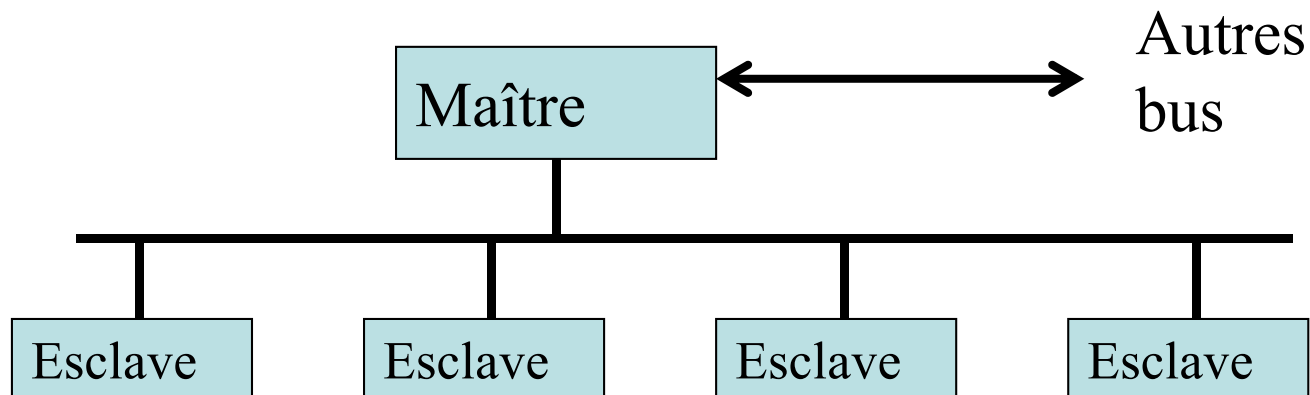
La sécurité & réseau

- Principe communément employé :
 - sur-couche sécurisée



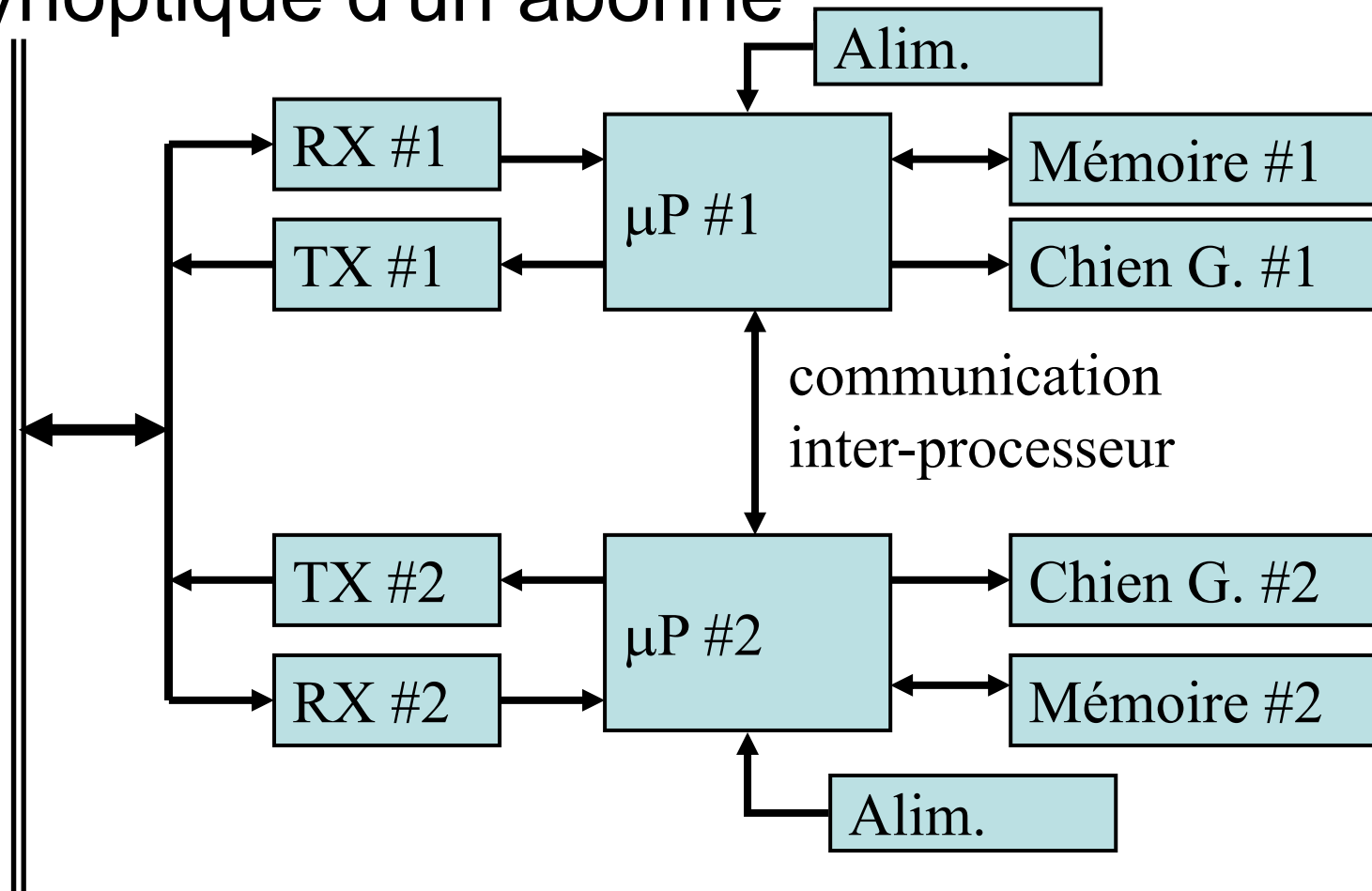
Safety Bus

- Généralités :
 - Développé par les sociétés SICK et PILZ
 - 1 maître / plusieurs esclaves (jusqu'à 60)
 - câble standard (2 conducteurs)
 - topologie arbres (500m à 125Kb, 100m à 500kb)
 - temps de réponse entre 20 et 100ms



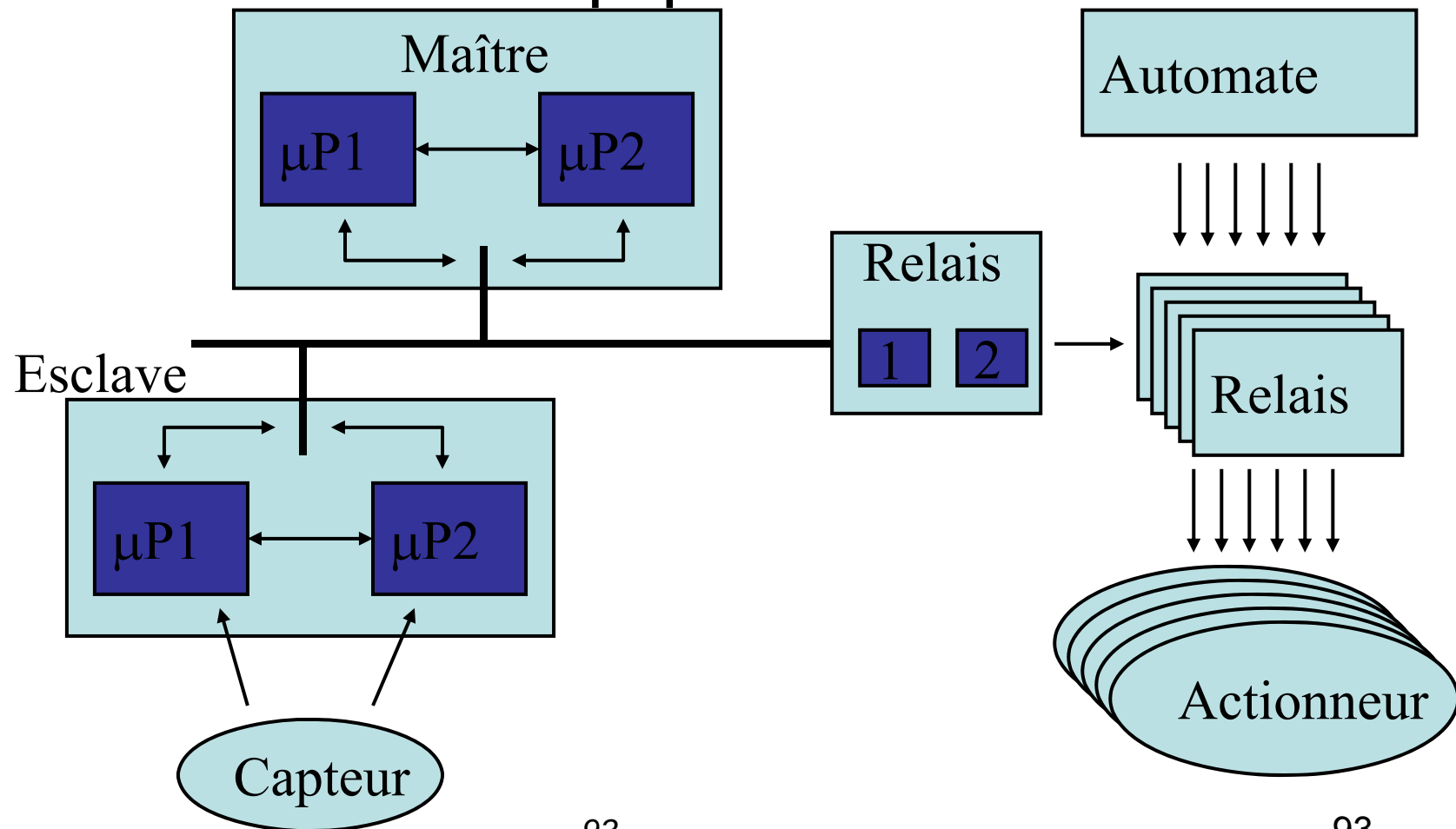
Safety Bus

- Synoptique d'un abonné :



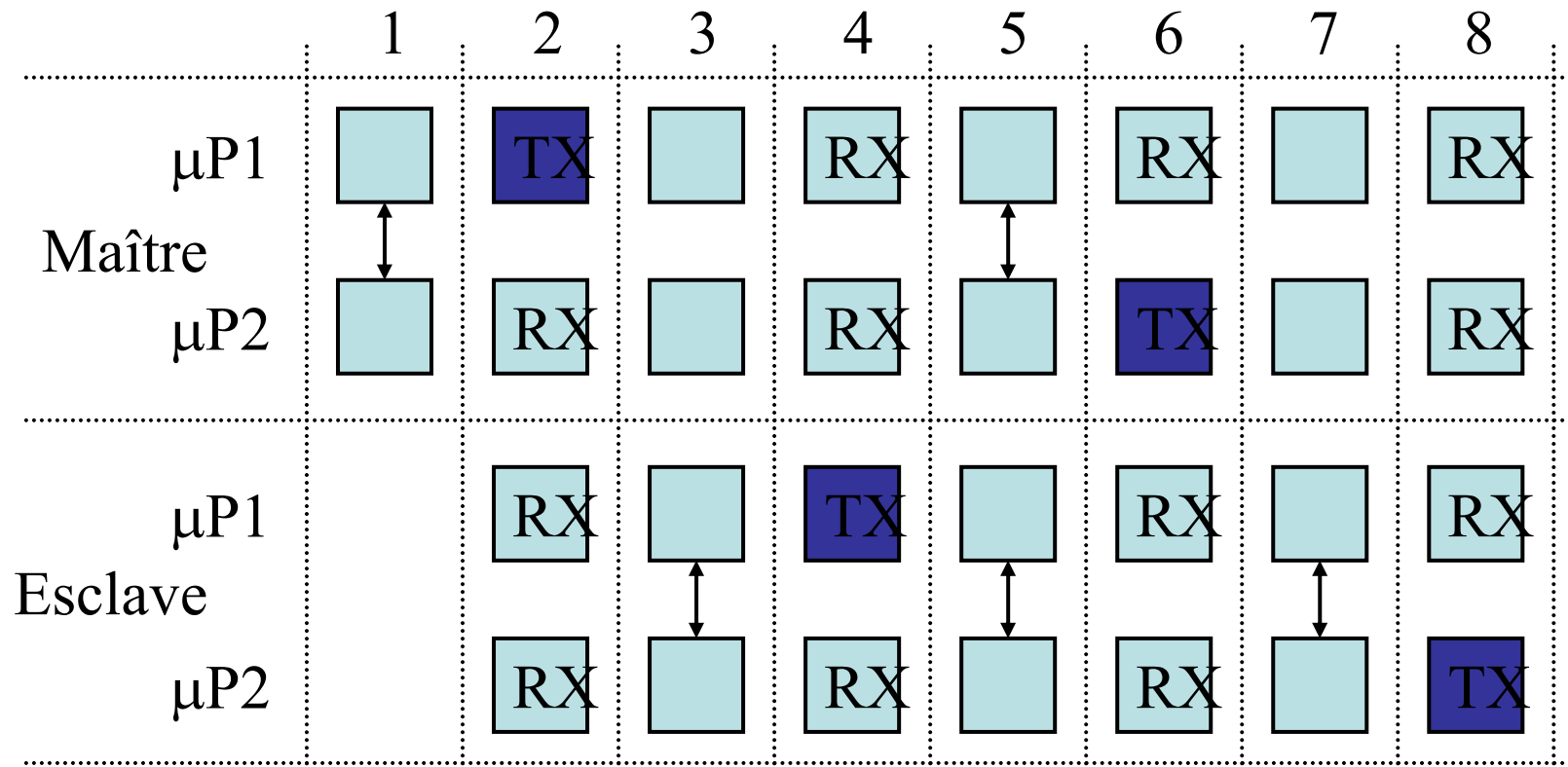
Safety Bus

- Connexion des équipements :



Safety Bus

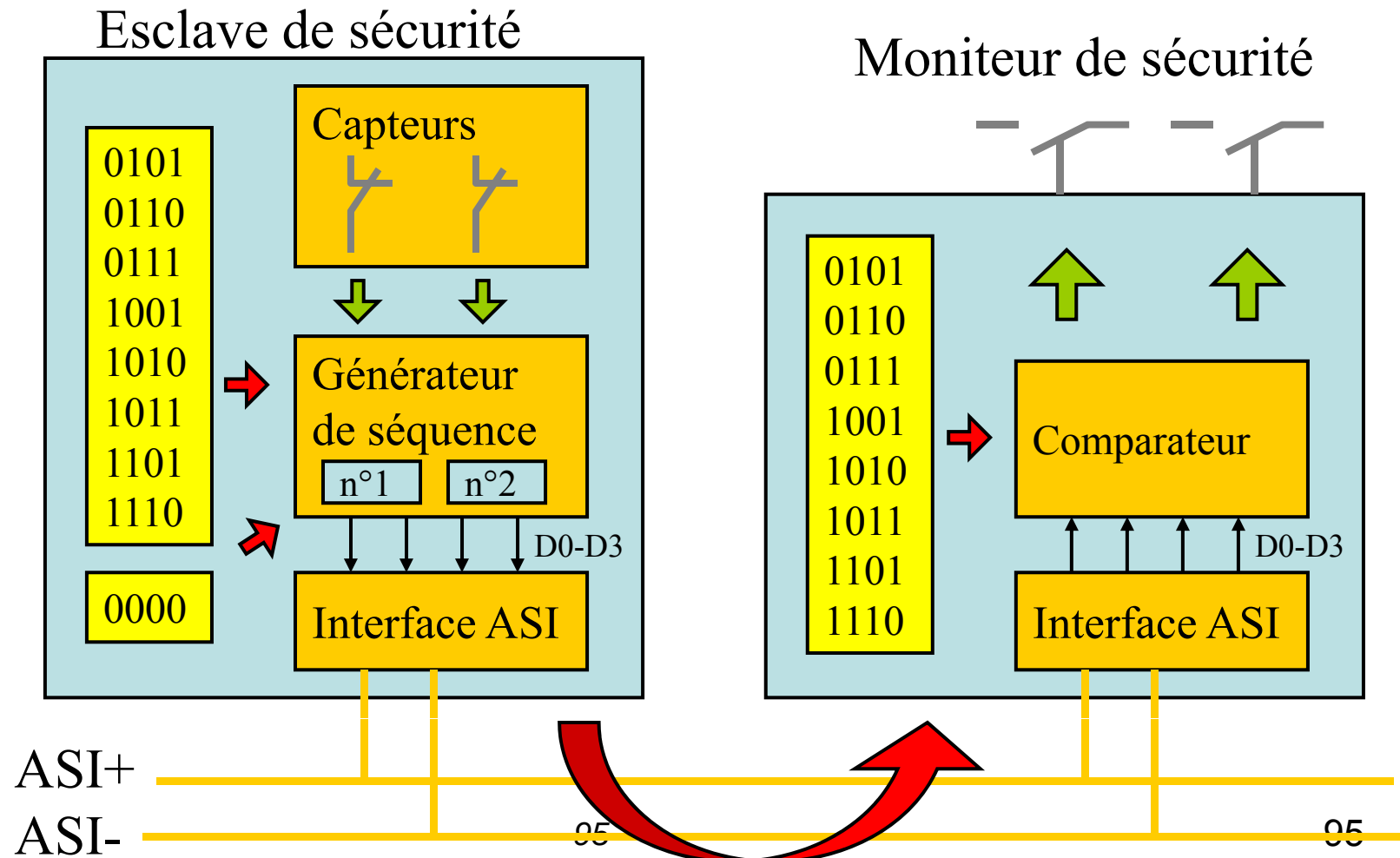
- Séquence de communication :



-Redondance des transmissions :
 un msg. acquitté suivi de son complémentaire

Les réseaux de sécurité

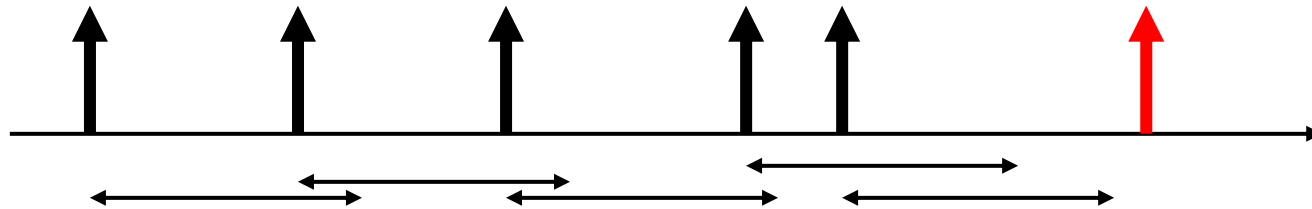
- Le cas d'ASI-Safe (séquence de transmission):



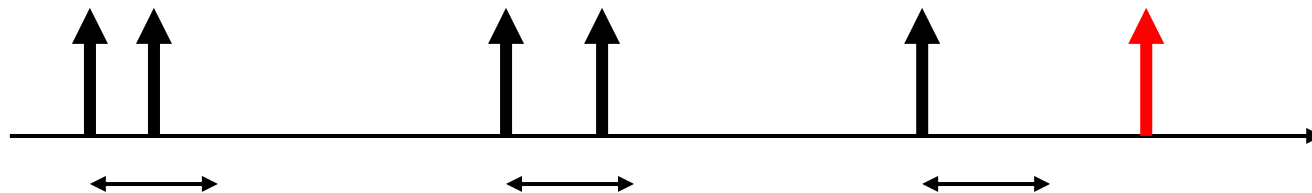
Les réseaux de sécurité

- Le CANOpen de sécurité :
 - Difficultés liées à l'accès non-déterministe, mais arbitrage → délai maximal estimable
 - Utilisation de 2 chiens de garde :

Fenêtre temporelle entre chaque trans.



Emission doublée



Communication Protocol Verification for Dependable Systems

Pavol BARGER

Jean-Marc THIRIET

Jean-François AUBRY

Philippe CHARPENTIER

Plan

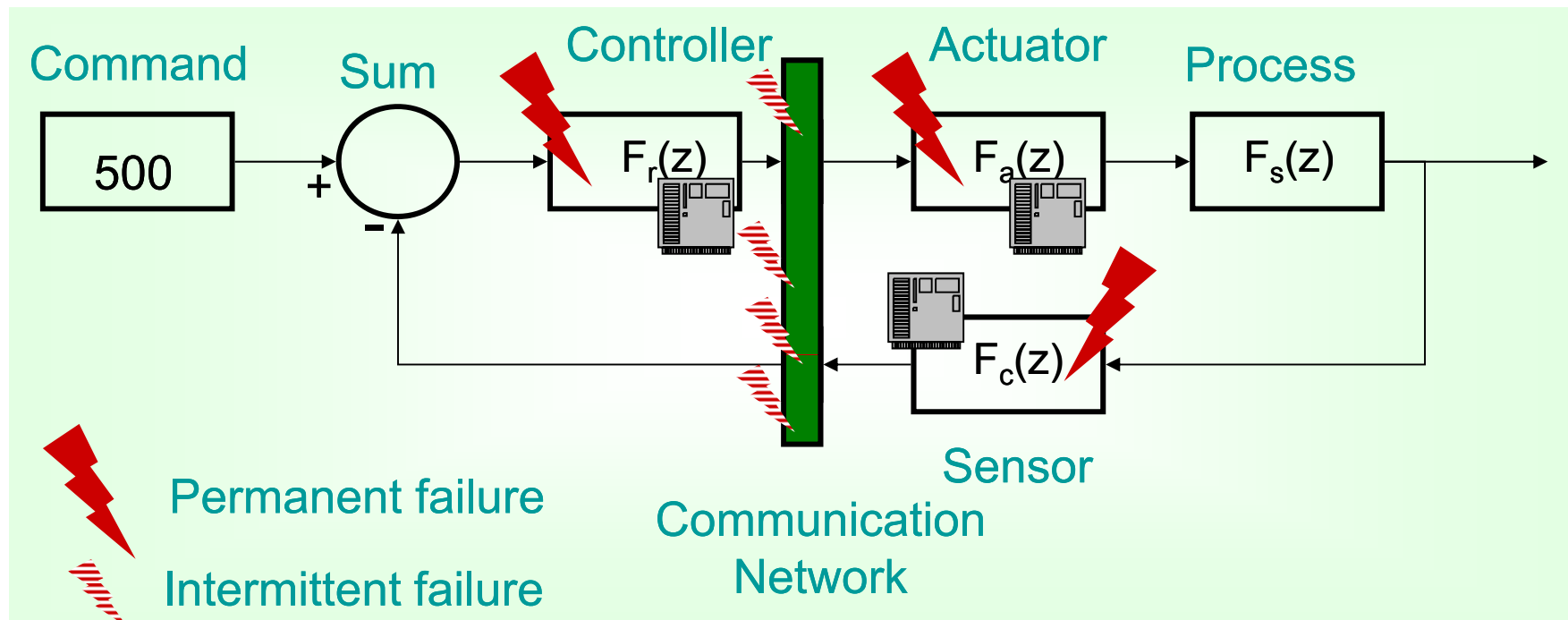
- Introduction
 - Interest in networks
- System presentation
 - Networked Control Systems
 - AS-i Safety at Work and Profisafe
- Modeling
 - Colored Petri Nets
- Our study
 - AS-i & Profisafe
- Conclusion

Introduction

- Networks – ever increasing temptation
 - Communication capacity
 - Cabling reduction
 - Modularity
 - Success of data computer networks
 - New technologies in automation
- Desire to integrate the network in control systems

Networked Control Systems

- A network is a part of the control loop



Safety Systems

- Interest in Networks
 - Identical to classic systems
- Additional constraints
 - Dependability evaluation
 - security
 - availability

→ Networks for Safety Applications

Networks and Safety

- Safety extensions of existing networks
 - AS-i Safety at Work
 - Can-safe
 - Ethernet-safe
 - Profisafe
- Safety dedicated networks
 - Safety-Bus p
 - FlexRay
 - TTP/C

AS-i

norme européenne

NF EN 50295

juillet 1999

norme française

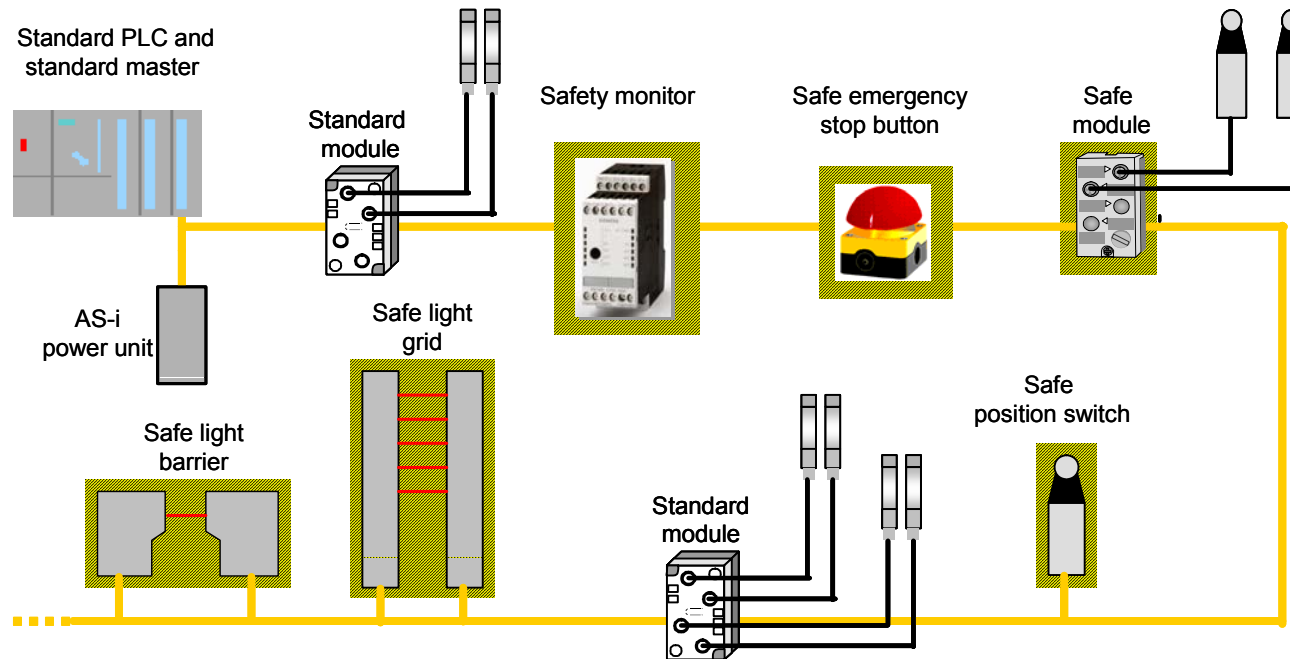
Indice de classement : **C 63-195**

ICS 29.120.60

**appareillage à basse tension
systèmes d'interface appareil de commande -
appareils. Interface capteur-actionneur (AS-i)**

E: Low-voltage switchgear and controlgear- Controller and
device- interface systems – Actuator Sensor interface (AS-i)

AS-i Safety at Work



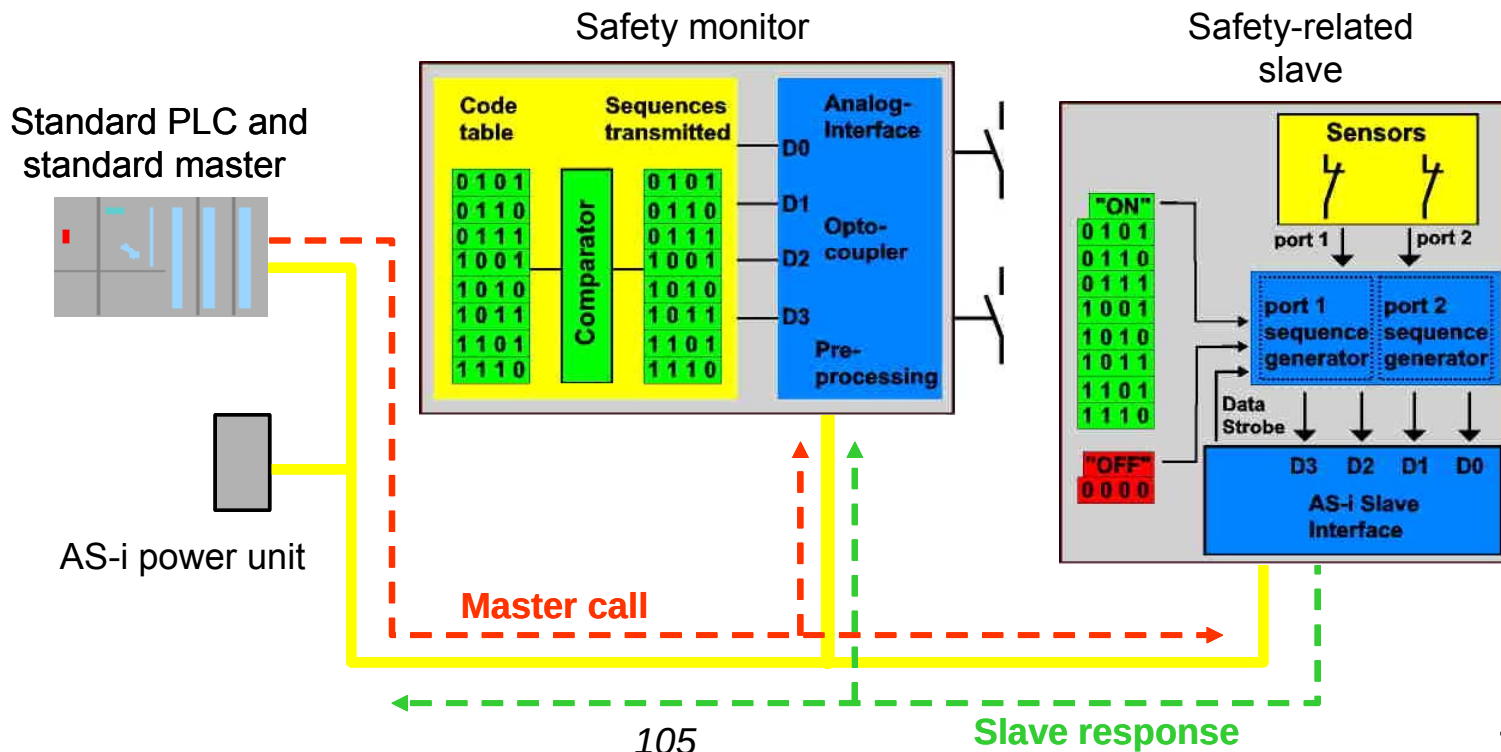
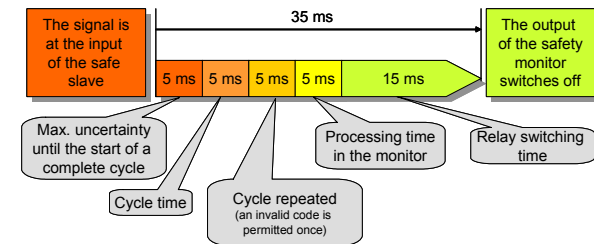
Advantages

- cabling reduction
- Safety and non-safety on one bus
- Groups of safety signals
- EN 954 – 1 category 4 compliant
- Certified: TUV and BIA
- No AS-i wiring changes needed

AS-i Safety at Work

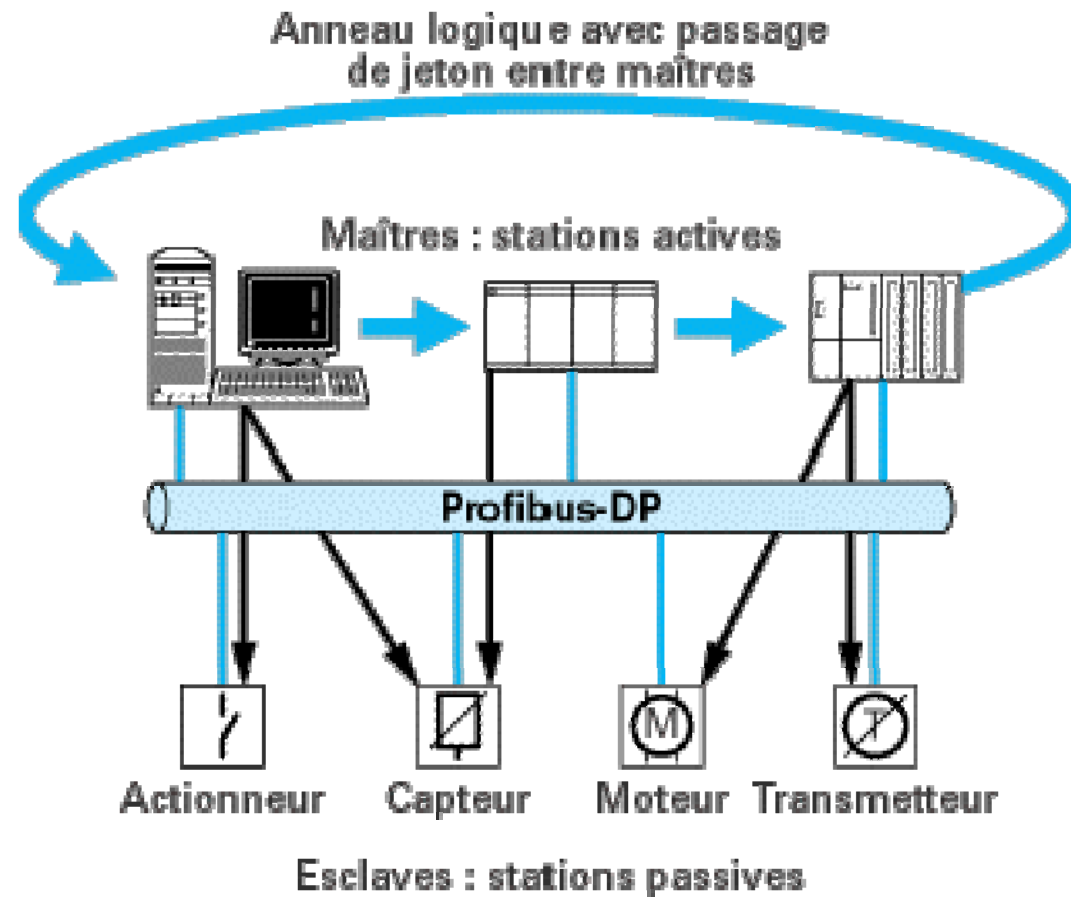
Principle

extension to the classical AS-i protocol
 A safety monitor added – continuous monitoring
 Specific safety code table for each slave
 Power supply stop by the monitor (safety relay)
 (stop, com. interruption, mess. corrupt, response delay)

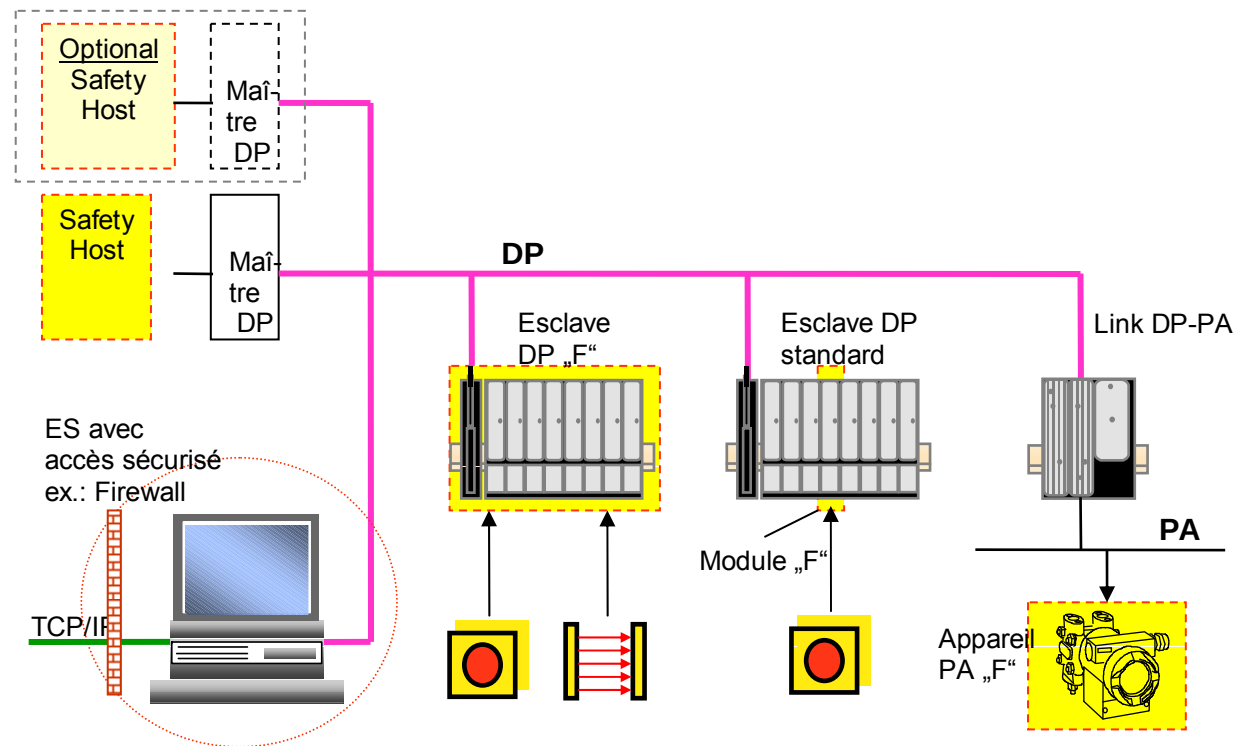


- ASI est un bus de communication standard avec des temps de réponse finis et rapides, dédié capteurs-actionneurs : il contient des mécanismes de détection et reconnaissance d'erreurs (cf. chap. 5) [SCH 01], [LET 02]. L'idée de "*ASI Safety at work*" est d'étendre les capacités de ASI afin de lui adjoindre des propriétés permettant de le rendre sûr et de mixer les trafics d'opération aux trafics de sécurité sur le même bus ; les utilisateurs peuvent de ce fait étendre leur installation existante avec des composants de sécurité.
- Pour cela, le principe est basé sur la co-existence, sur le même réseau, de composants classiques et de composants de sécurité. Un moniteur permet d'évaluer à la fois les signaux véhiculant des informations de sécurité et les systèmes de sécurité tels que les arrêts d'urgence et les barrières immatérielles.
- Ce moniteur est passif, il n'émet aucune communication. Le rôle du moniteur est d'écouter tous les trafics de sécurité et de détecter des séquences consécutives de quatre bits à zéro. Quatre zéros consécutifs indiquent que quelque chose s'est mal passé, soit un utilisateur a déclenché un système de sécurité et pressé un arrêt d'urgence, soit des défauts ont été détectés sur le bus de communication ou sur l'un des composants. Sans se préoccuper de la cause de l'erreur, dès la détection de quatre bits consécutifs à zéro, le moniteur met le système dans la position de repli qui a été programmée. Il est possible d'avoir plusieurs moniteurs sur le réseau, chacun pilotant une partie du système d'automatisation.
- Les composants de sécurité peuvent être connectés sur le réseau *ASI Safety at work* grâce à un esclave de sécurité. Le réseau *ASI Safety at work* a été certifié par le TÜV et le BIA comme étant de catégorie 4, conformément à la norme EN 954-1 [Std 954].

Profibus DP



Profisafe



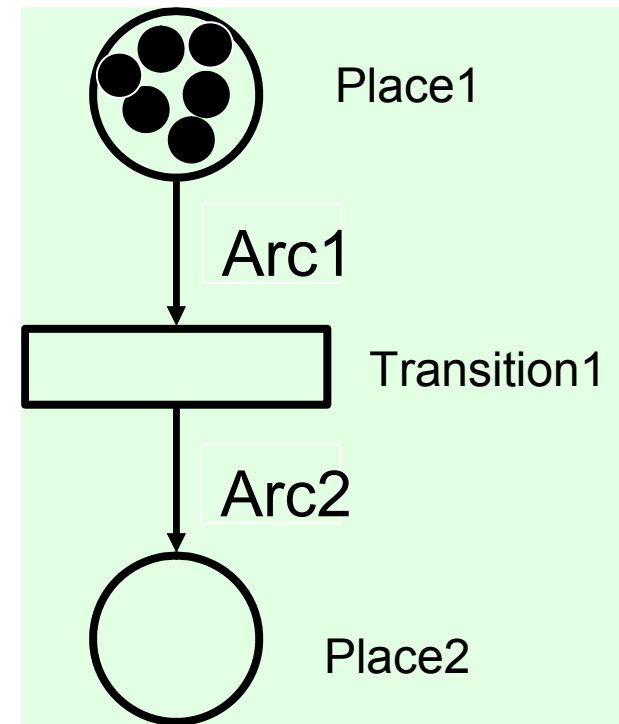
Petri Nets

Static part

- places
- transitions
- arcs

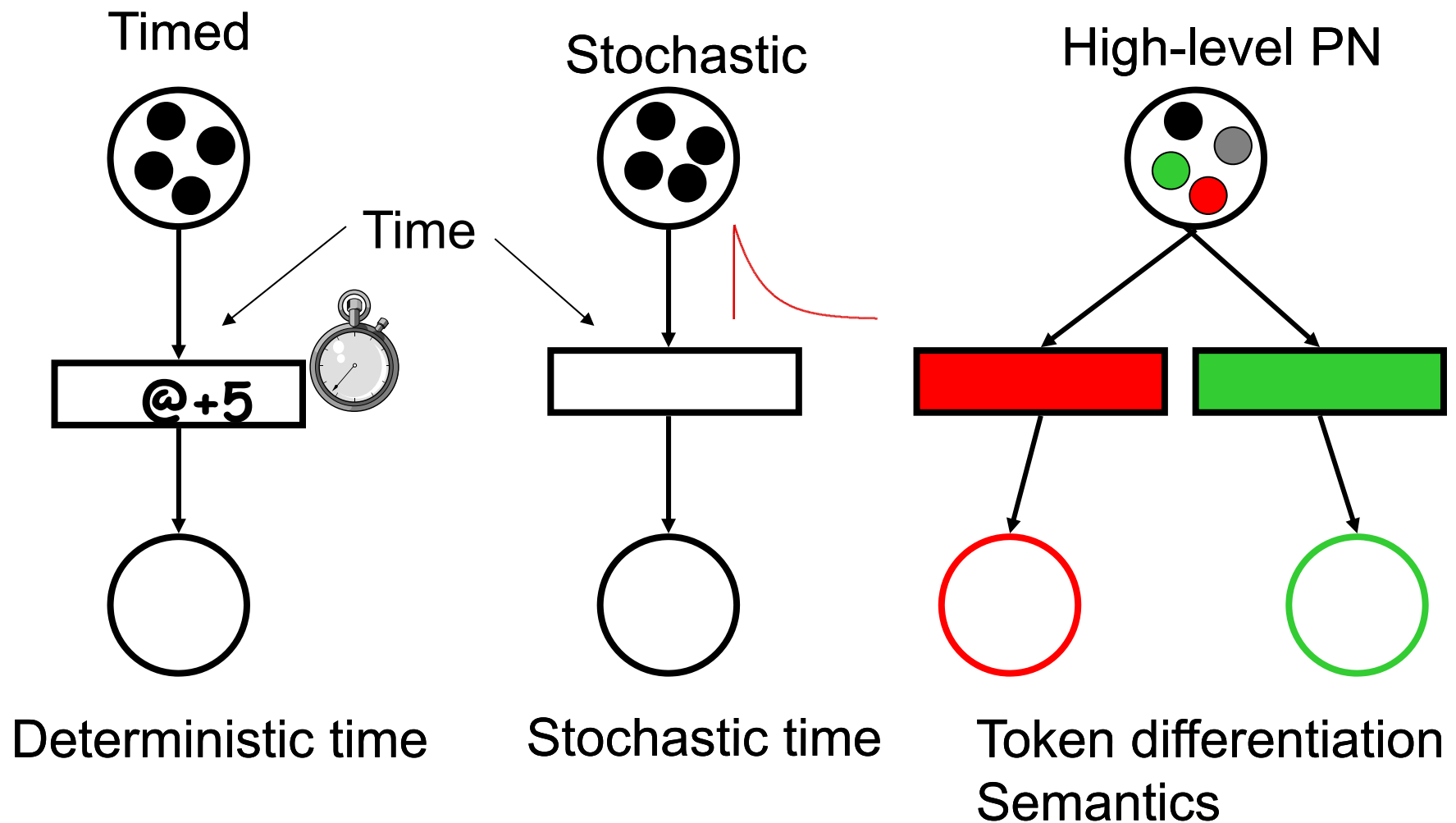
Dynamic part

- tokens ●



Wide-spread tool

PN modifications



Design/CPN and CPN tools

Constants

TRUE, 314, "Error"
empty

Variables

var my_variable: INT;
var still_one: STRING;

Data structures

tuples, domaines
Lists [1,3,5,7,9]

Functions

+, hd
if then else

Time association

@+45, @+delay

Random number generations

measure ('56')

Functional states ("Ok")

frame ('Sender', 'Receiver')

Scheduling [4,7]

Transition firing time

Stochastic aspects

Design/CPN and CPN tools

Constants

TRUE, 314, "Error"
empty

Variables

var my_variable: INT;
var still_one: STRING;

Data structures

tuples, domaines
Lists [1,3,5,7,9]

Functions

+, hd
if then else

Time association

@+45, @+delay

Random number generations

measure ('56')

Functional states ("Ok")

frame ('Sender', 'Receiver')

Scheduling [4,7]

Transition firing time

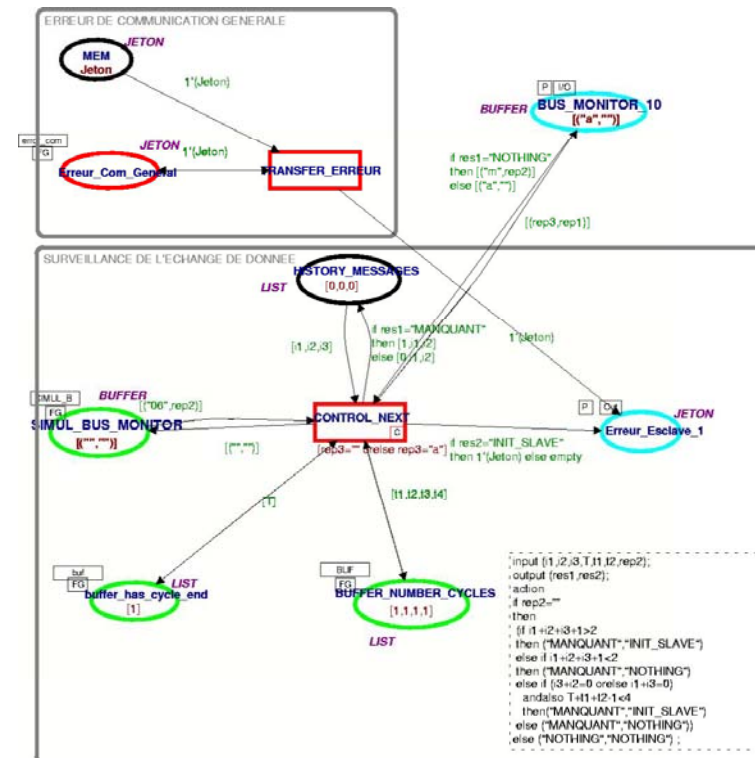
Stochastic aspects

Realized models

For AS-i Safety at Work and Profibus

- Master
- Slaves (identical copies)
- Bus (perfect, error free)

For Profisafe incremental model only.



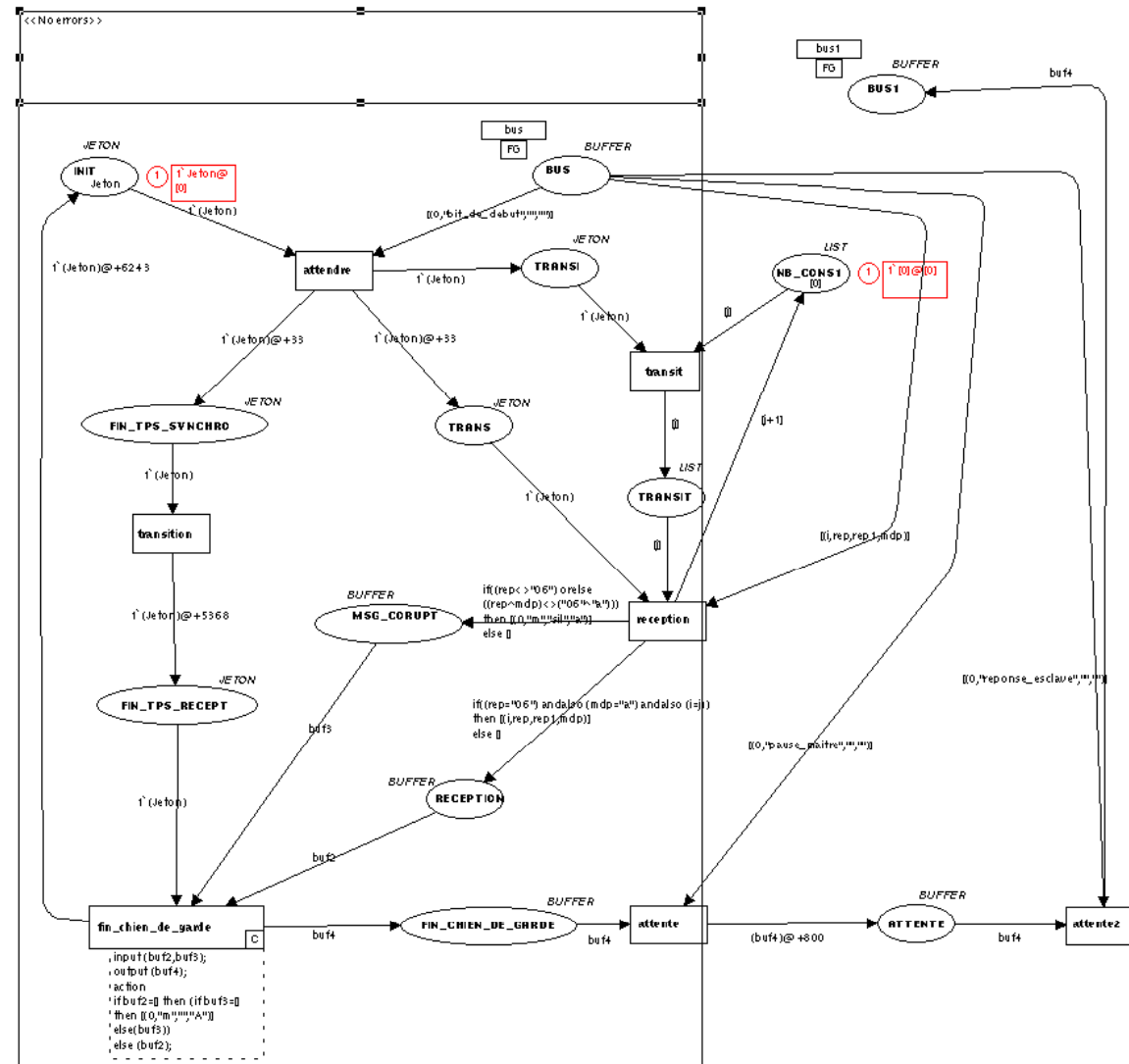
Results

- Slave internal states model
- Simulation analysis for a better understanding
- Occ graph automatic construction
- Occ graph analysis
- Non-blocking behavior verification
- Periodicity observed if stimulated with a periodic pseudo-random sequence

Conclusion

- CPN are well adapted for the modeling phase
- CPN analysis with Monte Carlo simulation is too slow
- Real formal verification impossible
- Creation of a set of potential modes
- Main result : Improvement proposal for the protocol specification

Model example

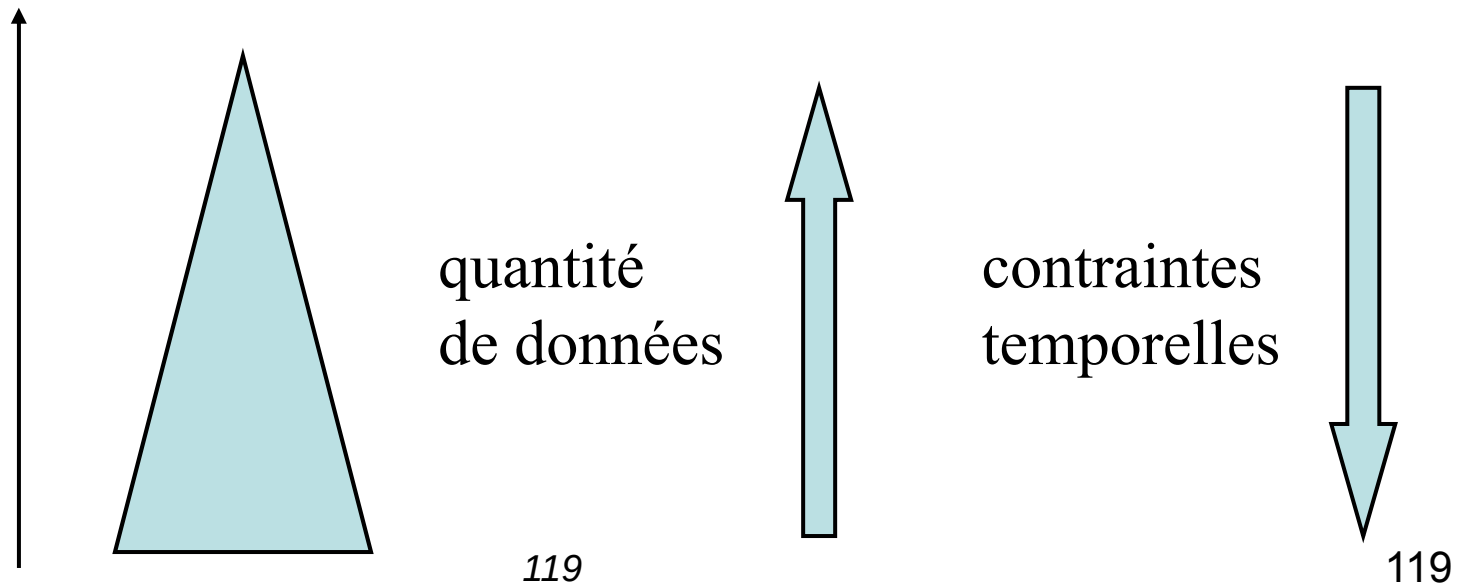




Critères de choix

Critères techniques

- Contraintes :
 - quand au format des données
 - quand aux contraintes temporelles
 - quand aux distances à couvrir
 - quand aux services à fournir
(objets ou messages, avec ou sans acquittement)



Critères commerciaux

- Réseau propriétaire :
 - avantage : pas de contraintes de standardisation, facilité de mise au point
 - limite : difficulté d'interconnexion ou de réutilisation d'équipements d'autres fabricants
- Réseau ouvert :
 - Développement plus complexe et plus long (respect des standard, certification...)
 - Marché peut-être plus large
 - Nécessité de s'inscrire (ou d'appartenir à une association) : droits d'entrée parfois élevés.

Réaliser son réseau

- Créer son réseau propriétaire :

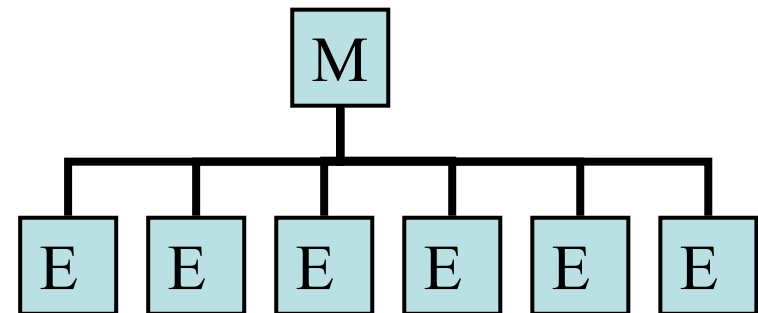
- Cas : 1 seul "chef d'orchestre"

Solution possible :

Protocole maître/esclaves

Interface : UART

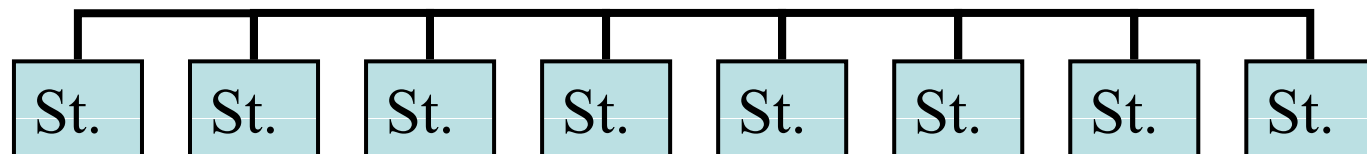
associée à RS485



- Cas : distribution du droit de parole :

Solution possible :

Protocole CAN (couche 1 et 2)



Créer son produit

- Déterminer le réseau au marché le plus favorable :
 - réseau adapté aux données à échanger
 - réseau ayant un avenir
 - nombre limité de concurrents
 - coût de développement limité concernant :
 - l'acquisition des compétences
 - le développement du produit
 - les droits d'entrée dans l'association/groupement... associé au réseau choisi
 - la certification du produit

References

- Groupe CIAME - Réseaux de terrain - Description et critères de choix – 1998 - Hermes Science Publications – ISBN : 2-86601-724-2
- Groupe CIAME - Les réseaux de terrain : Critères de sûreté de fonctionnement (Traité IC2, série systèmes automatisés) / ISBN 2-7462-1946-8 Hermes, avril-2009, 245 pages
- Transparents de Blaise Conrard, USTL, Lille
- Transparents de Sebastian ROEHL
- BARGER P., THIRIET J-M., AUBRY J-F., CHARPENTIER P. Vérification des Protocoles de Communication dans les Systèmes Sûrs de Fonctionnement . 6ème Congrès International Pluridisciplinaire, Qualité et Sûreté de Fonctionnement, Qualita'2005, Bordeaux, France, 16-18 mars 2005.
- AS-Interface : <http://www.as-interface.net/>
- CAN : <http://www.can-cia.org/>
- FIELDBUS FOUNDATION : <http://www.fieldbus.org/>
- FLEXRAY : <http://www.flexray.com/>
- Interbus : <http://www.ibsclub.com/>
- LON : <http://www.lonusers.asso.fr/>
- PILZ : <http://www.pilz.com/>
- PROFIBUS : <http://www.profibus.com/>
- TTA-Group : www.tttech.com, www.ttagroup.org
- WorldFIP : <http://www.worldfip.org>

Réseaux sans fil

Technologies in Industrial Wireless Applications

Zeashan KHAN

Introduction

- Why Wireless?
- Interference issues and coexistence
- Reliability
- Standardization
- Cost Comparison

IEEE 802.15.4 Basics

- Simple packet data protocol for lightweight wireless networks

- Released in May 2003
- O-QPSK Modulation (2.4GHz)
- DSSS Energy Spreading Scheme
- Three bands, 27 channels specified
 - 2.4 GHz: 16 channels, 250 kbps
 - 868.3 MHz : 1 channel, 20 kbps
 - 902-928 MHz: 10 channels, 40 kbps
- AES 128 Encryption and Authentication
- Communication Features
 - Simple Frame Structure
 - Reliable Data Delivery
 - CSMA-CA
 - Message Acknowledgement
 - Association/Disassociation
- Network Support
 - Employs 64-bit IEEE & 16-bit short addresses
 - Supports Mesh, Star and Point-to-Point
 - Non-Beaconed
 - Beaconed:
 - Optional super frame structure with beacons
 - Supports Guaranteed Time Slots (GTS)

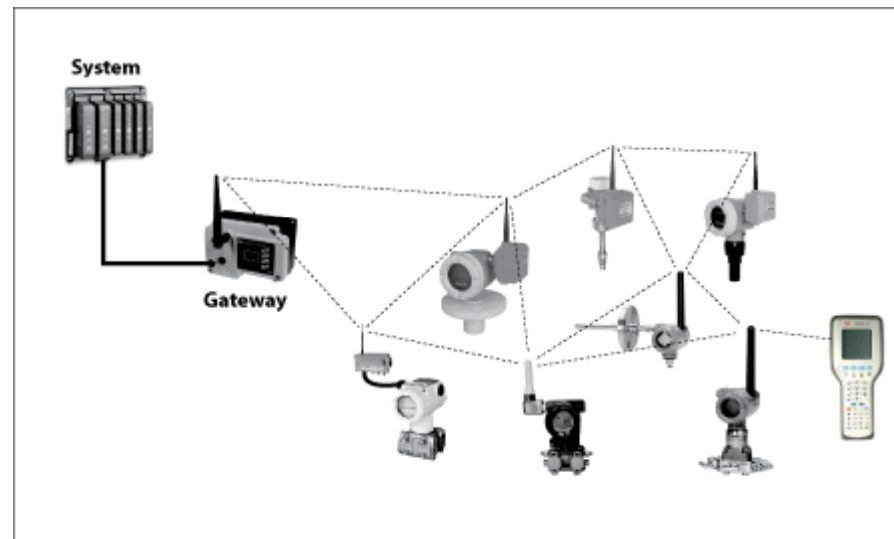
	Frequency Band	License Required?	Data Rate	Channel Number(s)	
	868.3 MHz	No	Europe	20kbps	0
	902-928 MHz	No	Americas	40kbps	1-10
	2405-2480 MHz	No	Worldwide	250kbps	11-26

Highway Addressable Remote Transducer (HART) Protocol Technology 1986

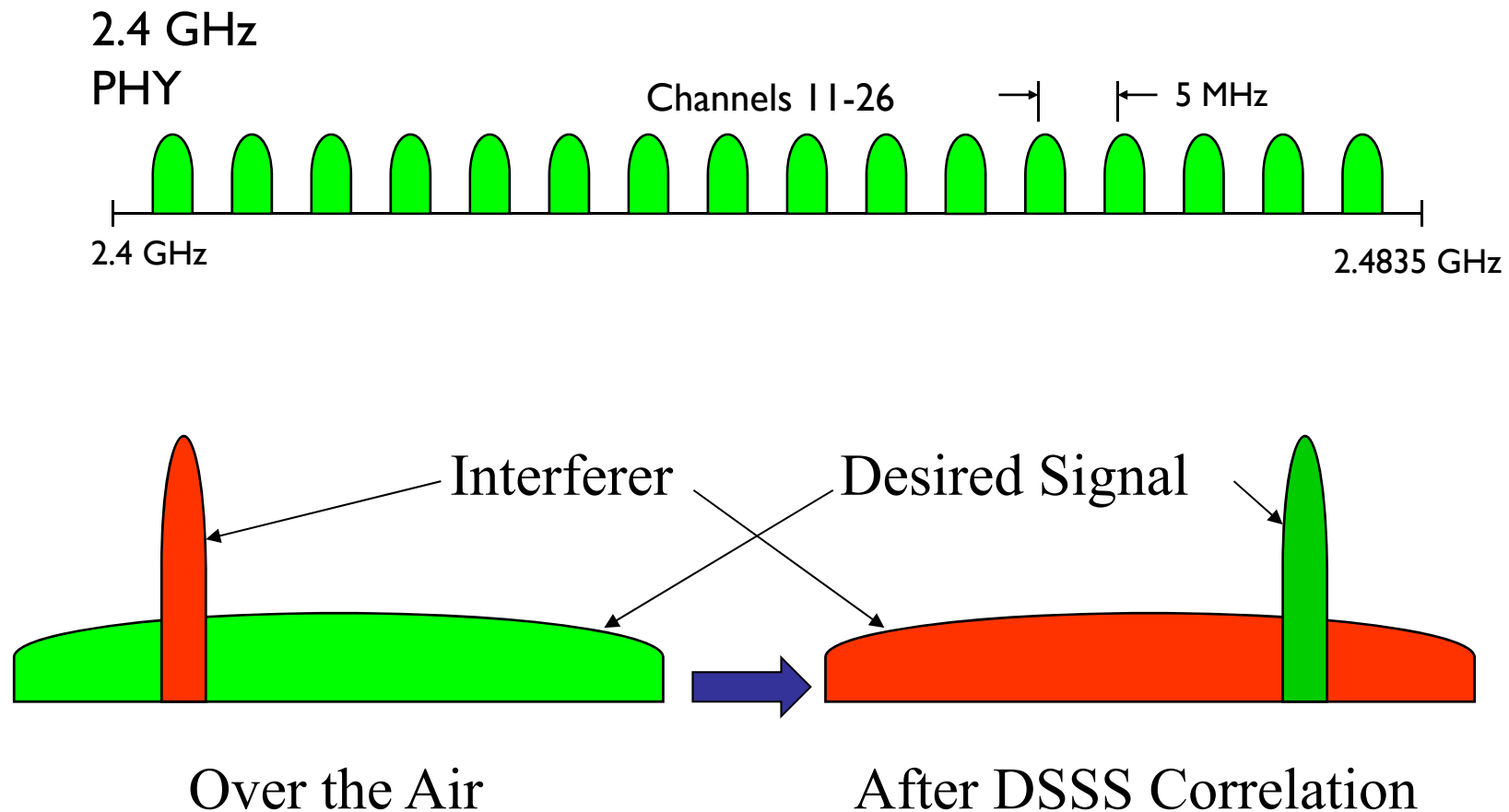
- HART is a digital protocol for two-way communication between a host application and smart field instruments, providing access to diagnostics, configuration and process data.
- Traditionally, HART specified a physical layer which used frequency-shift keying (FSK) superimposed on the analog control signal (4-20 mA).
- As of version 7, HART also incorporates an IEEE 802.15.4-based wireless mesh network as an option for the physical layer. This is commonly referred to as Wireless HART.

Wireless HART (2007)

- A *WirelessHART* Network consists of ***WirelessHART* field devices**, at least one ***WirelessHART* gateway**, and a ***WirelessHART* network manager**.
- These components are connected into a **wireless mesh network** supporting bi-directional communication from HART host to field device and back (Sensor + Actuator applications).
- WirelessHART is based on the PHY layer specified in the IEEE 802.15.4- 2006 standard, but specifies new Data-link (including MAC), Network, Transport, and Application layers.



Direct Sequence Spread Spectrum with Frequency Agility



Network Manager

- The Network Manager is an application that manages the mesh network and Network Devices. The Network Manager performs the following functions:
 - Forms the mesh network
 - Allows new devices to connect to the network
 - Sets the communication schedule of the devices
 - Establishes the redundant data paths for all communications
 - Monitors the network
- The mesh network architecture does not restrict where the Network Manager may reside in the plant automation network. It may be located on a Gateway device or on another system device.
- There is one Network Manager per mesh network. It also communicates with the Security Manager to get encryption and authentication data to secure the network.

Other Devices

Gateway

The Gateway Device connects the mesh network with a plant automation network, allowing data to flow between the two. The Gateway Device provides access to the *WirelessHART* devices by a system or other host application.

Field Devices

The Field Device may be a process connected instrument, a router or Hand Held device. The *WirelessHART* network connects these devices together.

Router Device

A device to improve network coverage (to extend a network) capable of forwarding messages from other Network Devices.

Process Connected Instrument

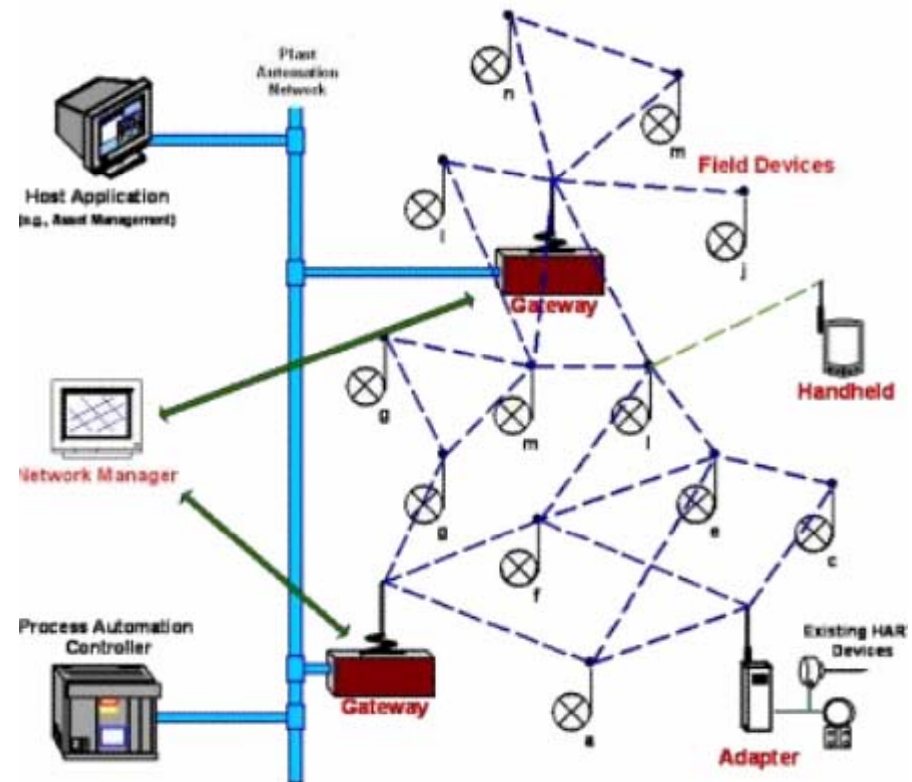
Typically a measuring or positioning device used for process monitoring and control. It is also capable of forwarding messages from other Network Devices.

***WirelessHART* Adapter**

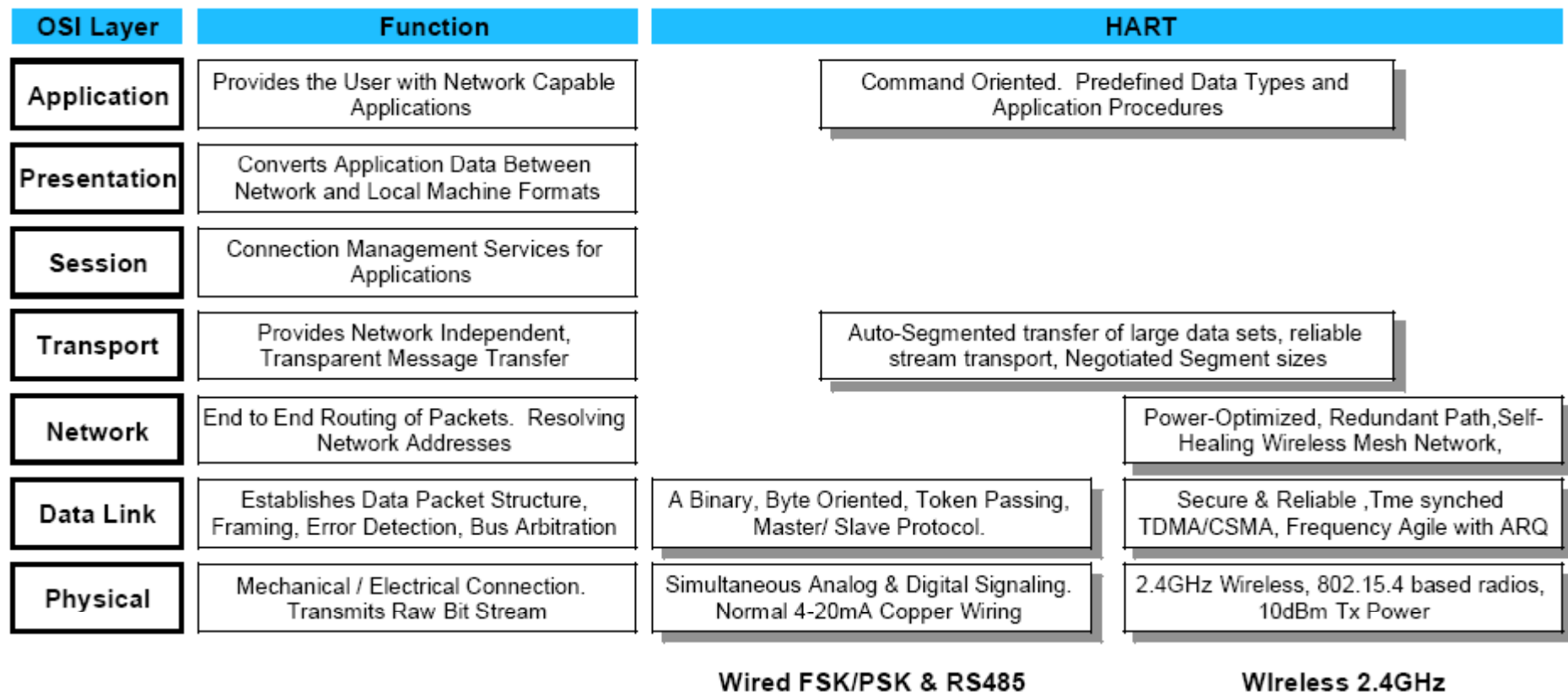
A device that allows a HART instrument without wireless capability to be connected to a *WirelessHART* network.

WirelessHART Technical Overview

- Based on IEEE 802.15.4 – 2006
- Focuses on features for reliability and co-existence
 - Adds channel hopping
 - Uses TDMA with a fixed 10ms time slot
 - *Black listing of bad channels*
 - Higher default transmit power
 - **+10 dBm**
 - Mesh network topology
 - Based on DUST Networks TSMP (Time Synchronized Mesh Protocol)
 - Provides flexible network organization
 - Provides redundant paths
 - Self organizing and self healing
 - Dynamic bandwidth allocation
 - Fixed bandwidth for prioritized data and commands
 - Supports AES-128 ciphers and key support
- Supports common HART devices
 - Wireless field devices
 - Bridges, gateways and access points provide seamless access throughout the network



WirelessHART reference model

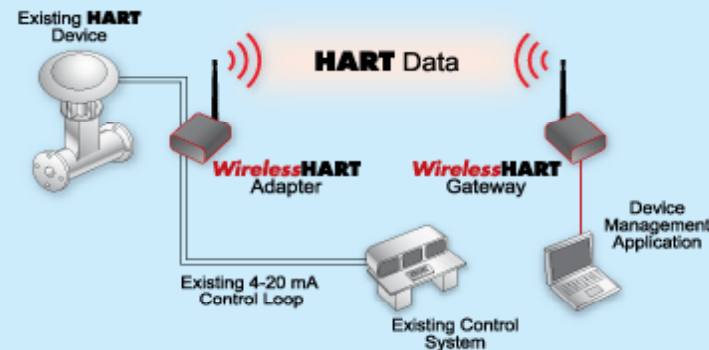


Wireless HART

Existing HART Devices with WirelessHART Adapter

Wireless Access to HART Device Information

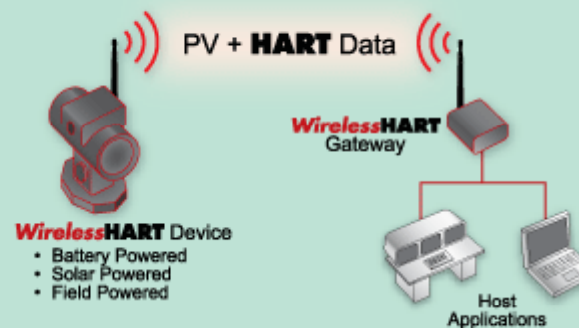
- ▶ Same **HART** device and control loop
- ▶ Utilize existing tools and experience
- ▶ Valuable device diagnostics



New WirelessHART Enabled Devices

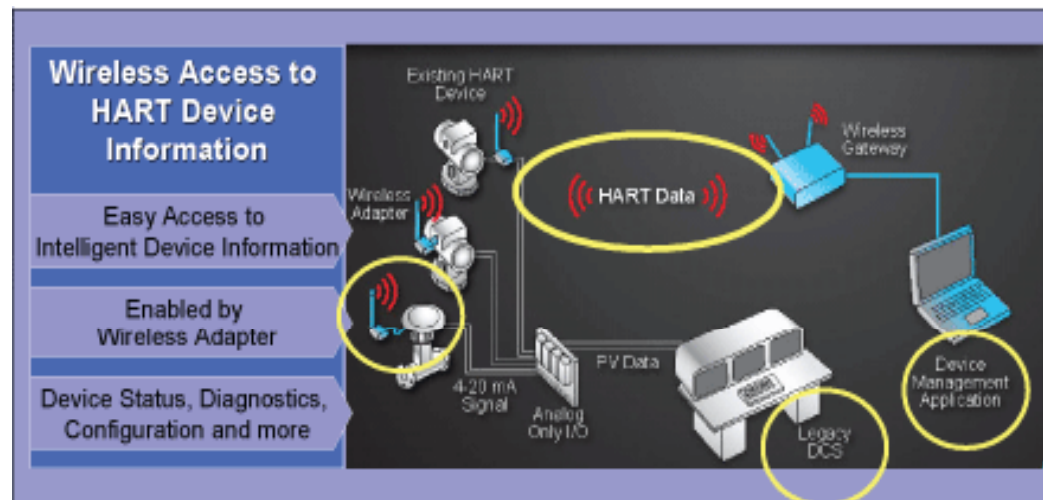
Additional Process Measurements Become Cost Effective

- ▶ Automate manual measurements
- ▶ No signal wiring costs
- ▶ Easy configuration and deployment



Wireless Access to HART Device

- This graphic shows wireless access to HART device information using existing HART-enabled devices. Here we show the traditional control loop connected to a control system. Unfortunately this legacy system is not capable of understanding the HART information.
- A system upgrade would be your first choice, but the reality is you can not afford to replace your control system.
- By adding WirelessHART adapters anywhere on the current loop, valuable device information can be communicated wirelessly to asset management application while your control signal remains intact and unaltered. Critical device diagnostics and process information can now be communicated without changing a single item in the device or in the control system.



One Wireless (Honeywell)

- The latest OneWireless release is the process industries' first mesh network with ISA100-ready hardware.
- Single network supporting both sensors and IEEE 802.11-based applications.
- Supports a broad range of both wired and wireless transmitters, including corrosion, gauge pressure, differential pressure, high-level analog input and temperature transmitters.
- Also supports mobile worker devices, such as Honeywell's IntelaTrac® PKS and Experion® Mobile Station, and can improve plant safety by helping customers quickly locate employees.
- Support the HART protocol.
- OneWireless system management software makes any XYR 6000 transmitter communicate to existing HART-enabled applications in the same manner as to a wired HART device.

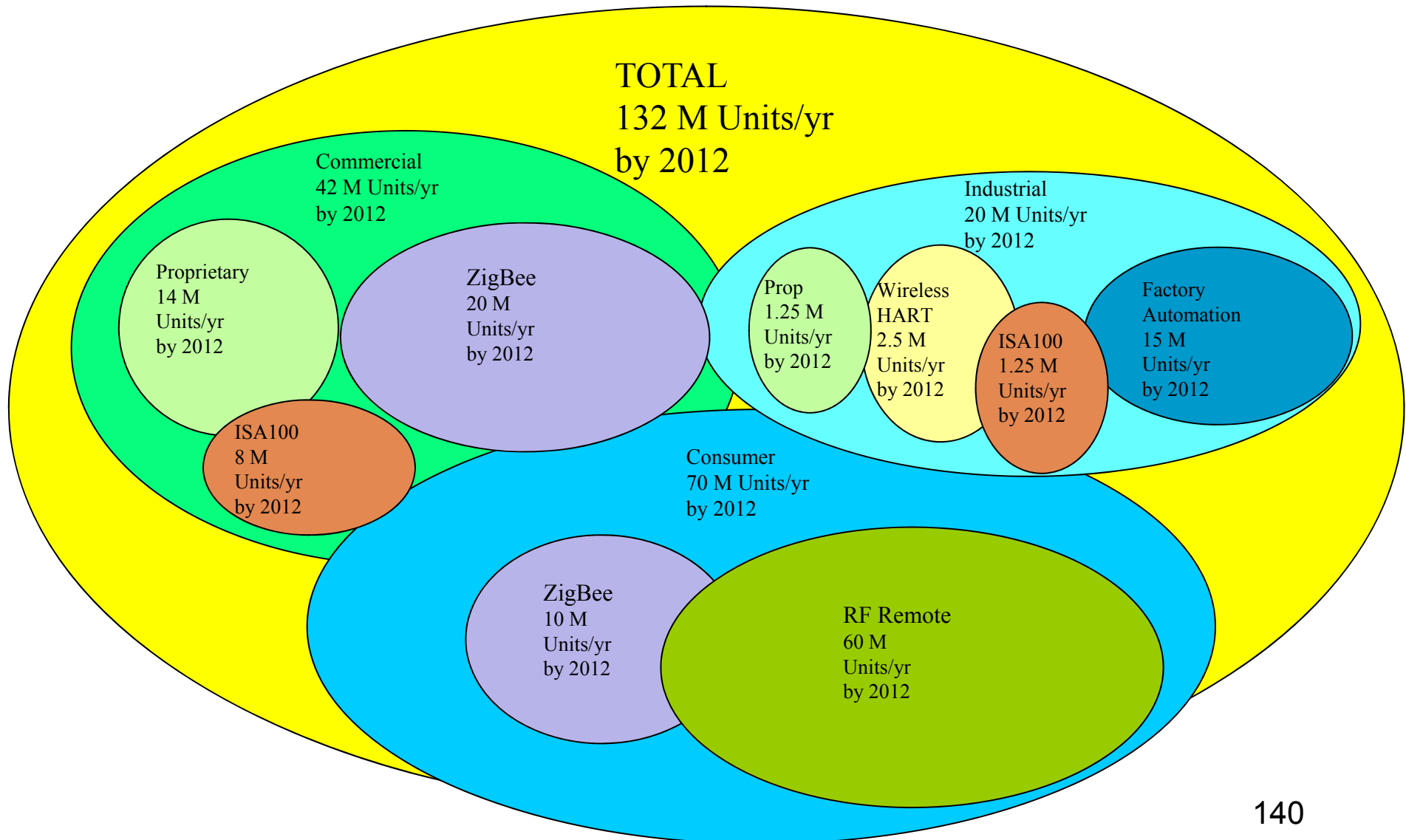
ISA and ISA100 Organization Overview

- ISA overview
 - Worldwide non profit organization founded in 1945
 - Develops standards; certifies industry professionals; provides education and training; publishes books and technical articles
- The ISA100.11a working group within ISA is defining wireless connectivity standard optimized for the unique performance of the industrial process control market
 - Addresses the needs in the industrial environment that includes sensors, actuators and other automation devices, as well as wireless workers, first responders and wireless infrastructure networks.
 - Addresses applications across the industrial industry including fluid processing, material processing, and discrete parts manufacturing environments
 - Defines the OSI layer specifications (e.g. PHY, DLL, etc.), security specifications, and management specification (including network and device configuration)
 - Key attributes are robustness to interference, low complexity, reasonable cost and low power consumption while maintaining interoperability with wired plant infrastructure networks
- Current desire is to have the specification published by November 2008
 - First draft released in December 2007

Comparison

	HART	WirelessHART	ZigBee
Layer 7 Application	Command oriented, predefined data types and application procedures		Application and security
Layer 6 Presentation			
Layer 5 Session			
Layer 4 Transport	Auto-segmented transfer of large data sets, reliable stream transport, and negotiated segment sizes		
Layer 3 Network		Power-optimized, redundant path mesh network	Ad-hoc routing mesh network
Layer 2 Data Link	A token passing master/slave protocol	Time-synchronized, frequency hopping protocol	IEEE 802.15.4-2006
Layer 1 Physical	Simultaneous analog & digital signalling (4-20mA wire)	IEEE 802.15.4-2006, 2.4GHz	IEEE 802.15.4-2006

IEEE 802.15.4 Market Forecast by 2012 (World Statistics)



Technology Comparaison

	IEEE 802.15.1 (WPAN)	Bluetooth v2.1	IEEE 802.15.4 (low rate WPAN)	Zigbee	IEEE 802.11 (WLAN)	Wireless HART
Throughput	1 Mbps (raw data rate)	3 Mbps (EDR, raw data rate)	20-250kbps (raw data rate)	20-250kbps (raw data rate)	2-54 Mbps (raw data rate)	20-250kbps (raw data rate)
(Variable) Packet length	366, 1622, and 2870 bits	366, 1622, and 2870 bits	1024 bits / MAC layer packet		34-2346 bytes	127 bytes
MAC protocol type	Dynamic TDMA	Dynamic TDMA	Slotted and unslotted CSMA/CA	Slotted and unslotted CSMA/CA	CSMA/CA	TDMA + CSMA/CA
Frequency hopping	YES	YES	Not specified	Not specified	YES	YES
Encryption	E0	E0 (improved passkey)	128-bit AES for encryption and/or integrity	Key exchange for AES encryption	WEP (802.11i: WPA)	AES-128 block ciphers with symmetric keys
Frequency band(s)	2.402-2.480 GHz	2.402-2.480 GHz	868, 902-928, 2400-2483.5 MHz	868, 902-928, 2400-2483.5 MHz	2.4-2.5 GHz 5.15-5.825 GHz	2400-2483.5 MHz
Effective range	1-100 m	1-100 m	10m nominal (1-100m based on settings)	10m nominal (1-100m based on settings)	~75 m outdoor, ~25 m indoor	1-100 m
Supported number of nodes	Protocol dependent	1 master and up to 7 active slave nodes per piconet	255 devices per network	255 devices per network	Practical limitation due to collisions	250 devices per network

Network architecture for distributed diagnosis, application to a helicopter drone



AKADEMIA GÓRNICZO-HUTNICZA
KRAKÓW

Author:

Małgorzata Sztokfisz

Faculty of Computer Science,
Department of Electrical Engineering, Automatics, Computer Science and Electronics,
University of Science and Technology AGH in Cracow,
Poland

Tutor:

Jean-Marc Thiriet

Laboratoire d'Automatique de Grenoble,
ENSIEG,
Institut National Polytechnique de Grenoble,
France



Summary

- Introduction
 - The helicopter
- Communication technology
 - ZigBee implementations
- Matlab and TrueTime
 - The TrueTime wireless network
 - The ZigBee network – roaming
- Simulation using the TrueTime library
 - Simulation with the wired network CAN
 - Simulation with the wireless network ZigBee
- Conclusions and next steps
 - The problems with ZigBee
 - The problems with TrueTime

Introduction

- Project goals:
 - Analysis of the various wireless communication medium for a distributed diagnosis system to be integrated in a helicopter drone
 - Propose model of the wireless communication in order to integrated it to a global model of a drone

Introduction: The helicopter

- the four propellers placed on the end of four branches
- the branches are arranged in a cross
- the whole electronic placed in the middle of this cross
- the helicopter flying indoors
- the diagnosis system placed in the base



- From the helicopter to the computer:
 - all data from sensors (magnetometers, gyro meters, accelerometers and also the speed of rotors).
- From the computer to the helicopter:
 - commands
 - and algorithms to control the engines.

Communication technology

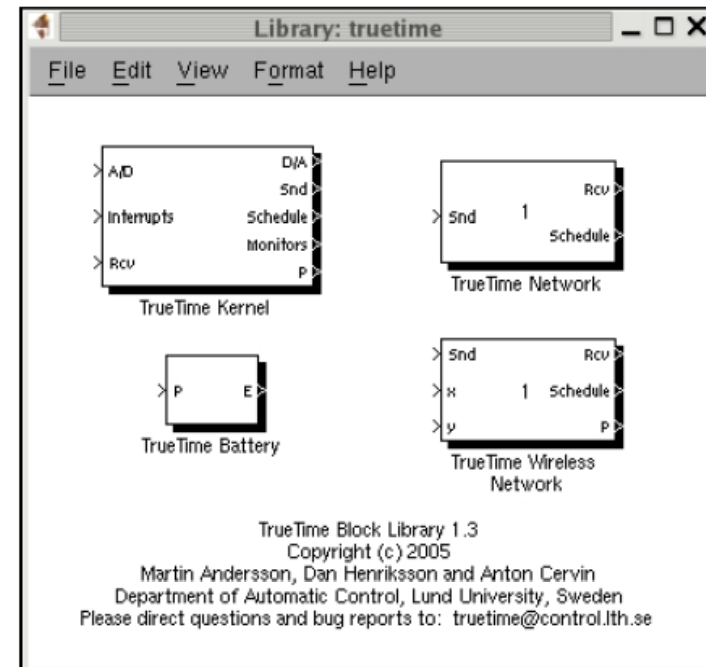
	Bluetooth	ZigBee	Wi-Fi	Wimax	Radio (The SpacePort Modem with RS232)
Standard	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.11b	IEEE 802.16	ETSI EN 300-220-3 (radio), ETSI EN 301 489-3 (EMC)
ISM band	2,44-2,48 GHz	2.4-2.4835 GHz (world), 902-928 MHz (USA) and 868-870 MHz (Europe)	2,4 GHz,	5 GHz2-11 GHz, 10-66 GHz	433.920 MHz
Transmission range	1 cm, 10 m, 100 m	from 10 to 75m	46 m indoor, 92 m outdoor	50 km, practically 5 - 8 km	50m indoor 200m outdoor
Data rate	720 Kb/s	250 kb/s (2.4 GHz), 40 kb/s (915 MHz), and 20 kb/s (868 MHz)	1, 2, 5.5, 11, 54 Mb/s	70 Mb/s, 500 kb/s and 2 Mb/s	9600bps
Number of nodes in network	7	$2^{16}=65536$	32	N/A	N/A
Battery Life (days)	1-7	100-1000+	0,5-5	N/A	N/A
Time of finding a new node in network	Up to 3s	30 ms	Up to 3s	N/A	N/A
Current market penetration	Medium	None	High	None	High
Success Metrics	Cost, Convenience	Reliability, Power, Cost	Speed, Flexibility	Wide-Range	Ease-of-use, Extended range capabilities, Speed and flexibility of installation
Application Focus	Cable replacement (for PCs, PDAs, laptops, mobile phones, printers digital cameras)	Home, building, industrial monitoring and control (for small, cheap microprocessors, low rate control networks)	Web, Email, Video. (for PCs, laptops, PDAs)	Broadband access, backhaul, "last mile" broadband connections.	Remote control, telemetry, telecontrol (for PDAs, organizers & laptops)

Communication technology - ZigBee

- protocol IEEE 802.15.4 - the global standards of communication
 - design for monitoring and control
 - cheap
 - very small
 - use in license-free radio band
 - wide range and large networks
 - low power consumption
 - possible to build low data rate wireless ad hoc mesh networking
 - coexist with IEEE 802.11/Wi-Fi and IEEE 802.15.1/Bluetooth at 2.4 GHz ISM band
-
- Unfortunately the ZigBee's support for real-time control is currently unknown

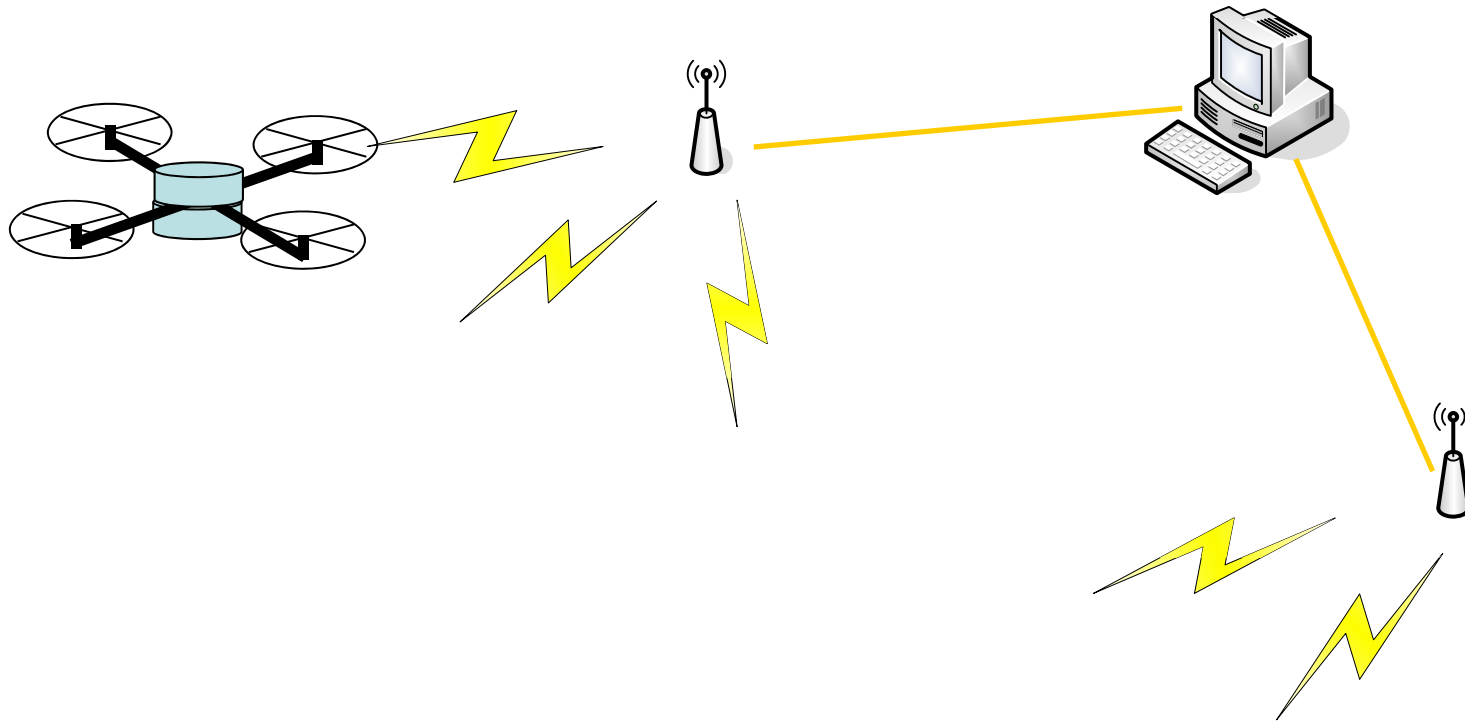
Matlab and TrueTime

- TrueTime is a Matlab/Simulink-based simulator developed at Lund University since 1999. It is possible to study more general and detailed timing models of computer-controlled systems.
- The TrueTime toolbox offers four blocks:
 - TrueTime Kernel
 - CSMA/CD (Ethernet),
 - CSMA/AMP (CAN),
 - Round Robin (Token Bus),
 - FDMA,
 - TDMA (TTP), Switched Ethernet
 - TrueTime Wireless Network
 - 802.11b/g (WLAN)
 - 802.15.4 (ZigBee)
 - TrueTime Battery



The roaming in ZigBee network

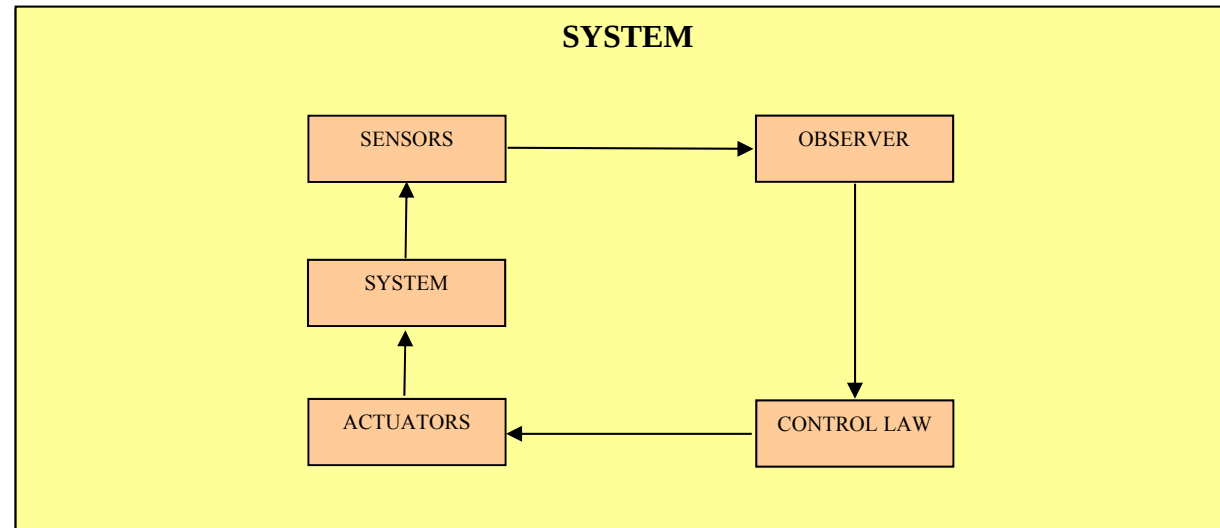
- Roaming – switching between different stations



The roaming in ZigBee network

- A large network of devices, with ongoing dynamics of devices associating, re-associating and disassociating to the network
 - Hierarchy of associations
 - Devices could reassociate elsewhere within the network
- Mobile and static nodes
- Background coverage - a grid of roughly 20-30 m.
 - Higher concentration of static nodes can improve coverage and location accuracy.

Simulation using the TrueTime library



Conclusions – Next steps

- Present simulation
 - 9 sensors – 9 transmitter
 - 4 actuators – 4 receiver
- Another simulation
 - 9 sensors – 1 transmitter
 - 4 actuators – 1 receiver
- Compare and contrast

References

- Transparents de Zeashan KHAN
- Transparents de Małgorzata Sztokfisz