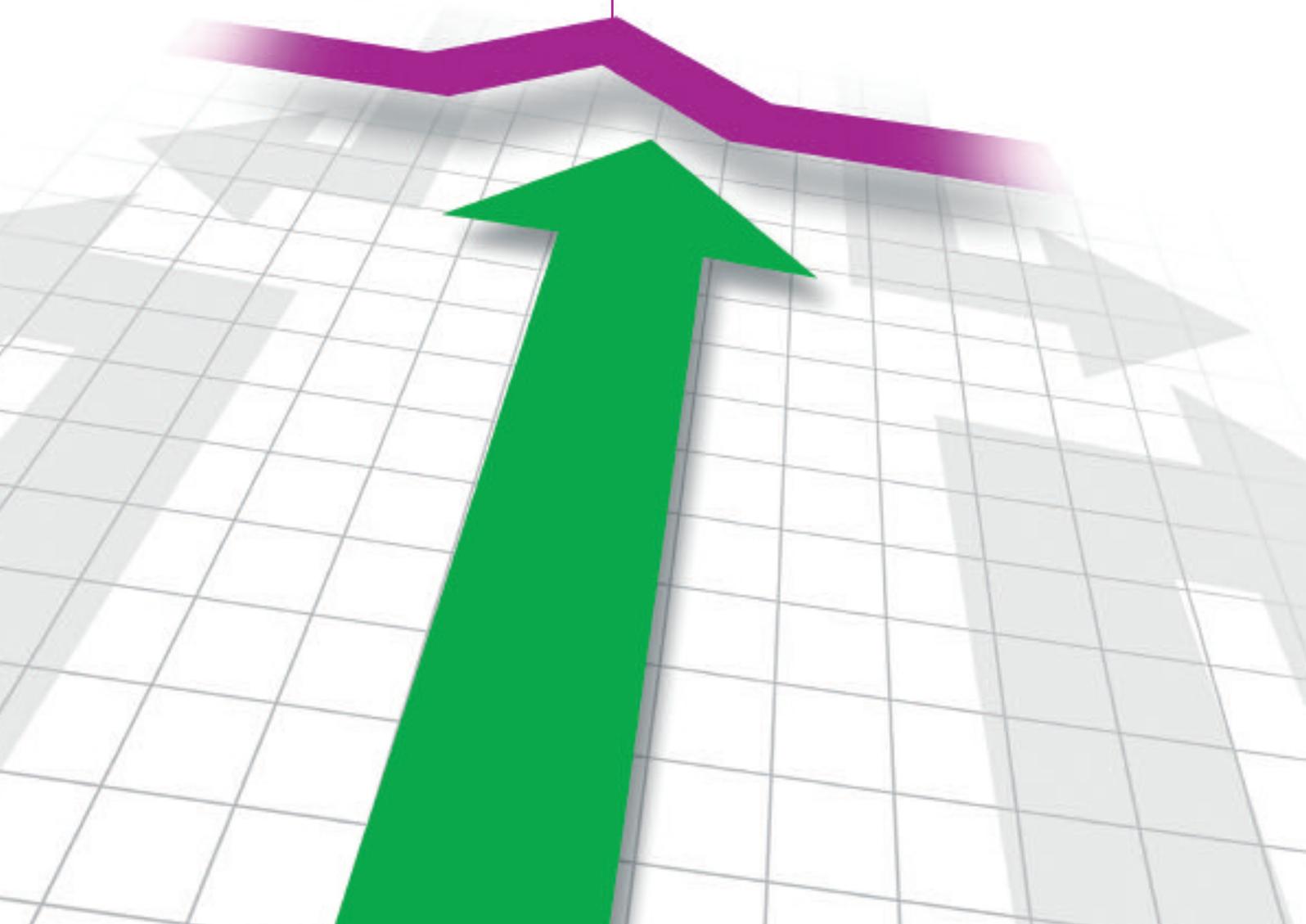


9 chapitre

Réseaux industriels

Présentation :

- *Besoins et offre existante*
- *Technologies*
- *Politique Schneider Electric*



9. Réseaux industriels Sommaire

9.1	Introduction	Page
9.2	Historique	Page
9.3	Les besoins et les réponses du marché	Page
9.4	Technologies des réseaux	Page
9.5	Les réseaux préconisés par Schneider Electric	Page
9.6	Ethernet TCP/IP	Page
9.7	Services Web et Transparent Ready	Page
9.8	Bus Can Open	Page
9.9	Synergie Ethernet et Can Open	Page
9.10	Bus AS-Interface (AS-I)	Page
9.11	Conclusion	Page

Nous abordons ici les liaisons électriques nécessaires au fonctionnement d'un équipement d'automatisme. L'habitude est de considérer deux catégories :

- Les liaisons **courants forts** destinées à assurer la connexion des constituants de puissance depuis le réseau d'alimentation jusqu'à la charge. Ce sujet ne sera pas traité dans ce chapitre, nous renvoyons le lecteur à ceux traitant de l'alimentation et de la mise en œuvre.
- Les liaisons **courants faibles** connectant l'ensemble des constituants d'acquisition, de dialogue, de traitement et de commande de puissance avec l'environnement de la machine et du processus.

9.1 Introduction

Traditionnellement le câblage des équipements électriques est assuré par des liaisons fils à fils.

La norme internationale machines IEC 60 204-1 et celle d'installations - propres à chaque pays - définissent des règles précises sur les sections, la qualité de l'isolant et le repérage par des couleurs normalisées. La plupart de ces liaisons sont réalisées par des câbles unitaires souples de section comprises entre 1.5 et 2.5mm² (AWG 16 et 14) protégés aux extrémités par des embouts.

Ces solutions ont couvert, jusqu'à la précédente décennie, l'ensemble des besoins, que ce soit pour les signaux en tout ou rien ou les signaux analogiques nécessaires aux asservissements, ces derniers exigeants parfois des câblages blindés pour éviter les perturbations électromagnétiques.

L'arrivée des technologies numériques dans l'industrie a eu un impact considérable sur la conception et la réalisation des équipements électriques. Elle s'est faite sous l'influence des standards issus de l'informatique et de l'automobile.

L'échange d'informations numériques a imposé des liaisons par réseaux de communication entraînant l'usage de connecteurs et de connections préfabriquées. Le travail de réalisation d'un équipement électrique devient alors beaucoup plus simple, les erreurs de câblage sont réduites et la maintenance simplifiée.

Les technologies de liaisons conventionnelles étant bien connues, nous consacrerons ce chapitre aux réseaux de communications utilisés dans l'industrie.

9.2 Historique

En 1968, la société Modicon invente le concept d'automate programmable. Un matériel unique répond à une grande multiplicité de besoins et apporte une économie d'échelle. De sa grande souplesse d'utilisation découle de nombreux gains dans toutes les phases de vie de l'installation. Les réseaux apparaissent également peu à peu, d'abord sous forme de liaisons séries. Des protocoles viennent formaliser les échanges. Ainsi Modbus (1979), contraction de MODicon BUS, devenu depuis un standard de fait.

Depuis quelques années, de nombreuses applications ont adopté le bus de terrain. Cette épine dorsale de l'architecture d'automatisme apparaît comme un moyen extrêmement puissant d'échanges, de visibilité et de souplesse pour les équipements qui y sont raccordés. Le bus de terrain conduit à un bouleversement progressif des architectures :

- suppression des câbles d'entrées/sorties,
- disparition ou décentralisation des interfaces d'entrées/sorties,
- décentralisation et la répartition de l'intelligence,
- interconnexion avec Internet.

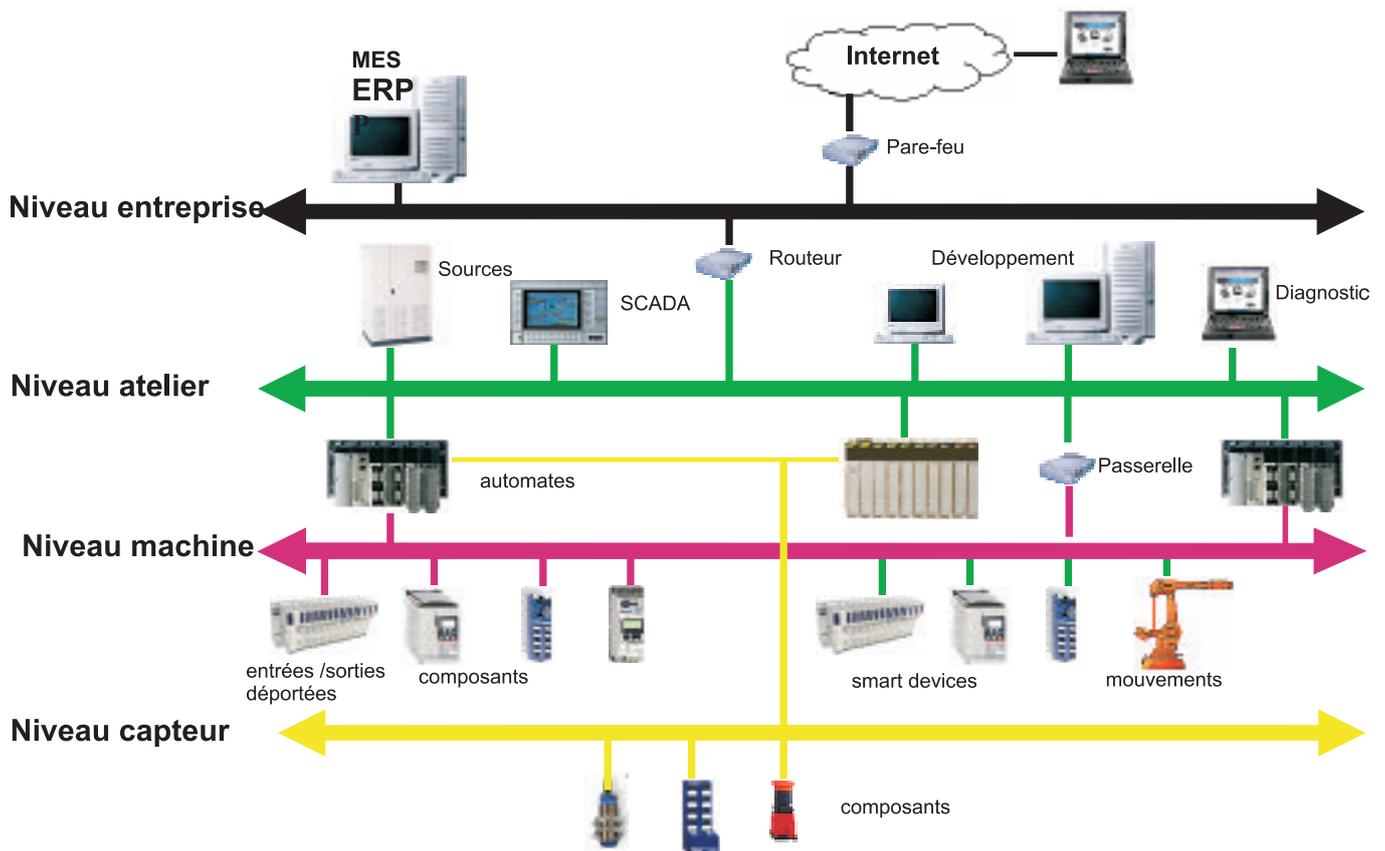
Les années 70 voient naître dans Xerox PARC le réseau Ethernet (contraction d'éther et de net). 10 ans plus tard, il devient le standard international que nous connaissons et équipe en natif pratiquement tous les ordinateurs. Les premières applications ont été de transférer des fichiers, des messages et de transmettre des pages WEB. La généralisation de l'informatique dans tous les métiers de l'entreprise a fait émerger le besoin de connecter l'ensemble des domaines industriels dans les années 90.

Le World Wide Web inventé par le CERN en 1989 - a été développé à l'origine pour permettre le partage d'informations entre les différentes équipes de travail implantées internationalement. Le monde du WWW consiste à partager des documents et des liens. Un protocole simple : HTTP est utilisé par un navigateur (browser) pour accéder aux pages web stockées sur un serveur. Ces pages sont programmées à l'aide de langages, tels que HTML ou XML. Le consortium World Wide Web Consortium (W3C), créé en 1994 gère l'évolution technique du web (voir le site <http://www.w3.org/>)

En 1996, Schneider Electric fait la promotion du réseau Ethernet industriel pour connecter les niveaux "entreprise" et "atelier" avec les automates puis développe le concept de "Transparent Ready". Ce concept est basé sur l'ajout d'outils et de protocoles industriels -dont Modbus- aux éléments standards existants d'Ethernet.

9.3 Les besoins et les réponses du marché

Sous l'effet conjugué des contraintes des utilisateurs, des technologies et des standards, les architectures actuelles se structurent en quatre niveaux distincts et interconnectés par des réseaux (⇒ Fig. 1).



↑ Fig. 1 Exemple de niveaux d'architecture

Avant d'analyser les technologies des réseaux de communication, il est nécessaire de présenter une synthèse des principaux besoins auxquels ces niveaux apportent une réponse pertinente. Les caractéristiques citées dans le tableau de la *figure 2* seront détaillées dans les paragraphes suivants.

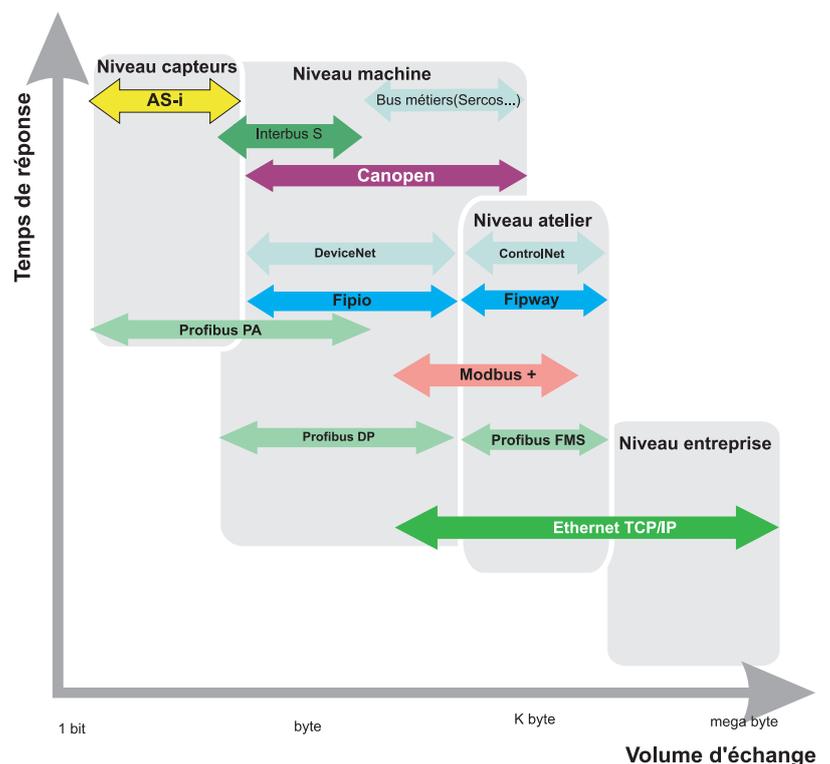
Niveau	Besoin	Volume d'informations à transmettre	Temps de réponse	Distance	Topologie réseau	Nombre d'adresses	Médium
Entreprise	Echange de données. Sécurité informatique. Standards entre progiciels.	Fichiers Mbits	1mn	Monde	Bus, étoile	Non limitée	Electrique, optique, radio
Atelier	Synchronisation des API' d'un même flot d'automatisme échanges d'information en mode client/serveur avec les outils de conduite (HMI, supervision). Performances Temps réel.	Données Kbits	50 à 500 ms	2 à 40 Km	Bus, étoile	10 à 100	Electrique, optique, radio
Machine	Architecture distribuée. Intégration fonctionnelle et transparence des échanges. Topologie et coût de connexion.	Données Kbits	5 à 100 ms (cycle de l'API)	10 m à 1 Km	Bus, étoile	10 à 100	Electrique, optique, radio
Capteur	Simplification du câblage distribution des alimentations des capteurs et actionneurs. Optimiser les coûts de câblage.	Données bits		1 à 100 m	Sans contrainte	10 à 50	Electrique radio

↑ Fig. 2 Les besoins et les contraintes de communication

Nous pouvons, en première approche, retenir les deux principaux axes de ce tableau de besoins :

- le nombre d'informations à transmettre,
- le temps de réponse nécessaire.

Ceci nous permet de positionner les principaux réseaux commercialisés (⇒ Fig.3).



↑ Fig. 3 Principaux réseaux industriels

9.4 Technologies des réseaux

Nous présentons succinctement les différents concepts, le lecteur intéressé par un approfondissement se reportera vers les nombreux ouvrages qui ont été édités sur ce sujet.

■ Topologie des réseaux

Un réseau industriel est constitué d'automates programmables, des interfaces hommes/machines, d'ordinateurs, des équipements d'entrées/sorties, reliés entre eux grâce à des lignes de communication, telles que des câbles électriques, des fibres optiques, des liaisons radio et des éléments d'interface, tels que des cartes réseaux, des gateways. L'arrangement physique du réseau est appelé **topologie physique** ou architecture du réseau.

Lorsque l'on considère la circulation des informations, on utilise la terminologie de topologie logique.

On distingue généralement les topologies suivantes :

- en bus (⇒ Fig.4),
- en étoile (⇒ Fig.5),
- en arbre,
- en anneau,
- maillées.

• Topologie en bus

Cette organisation est une des plus simples. Tous les éléments sont reliés à une même ligne de transmission par l'intermédiaire de câbles. Le mot bus désigne la ligne physique. Cette topologie est facile à mettre en œuvre, la défaillance d'un nœud ou d'un élément ne perturbe pas le fonctionnement des autres organes.

Les réseaux du niveau machine et capteurs, appelés d'ailleurs bus de terrain, utilisent cette méthode.

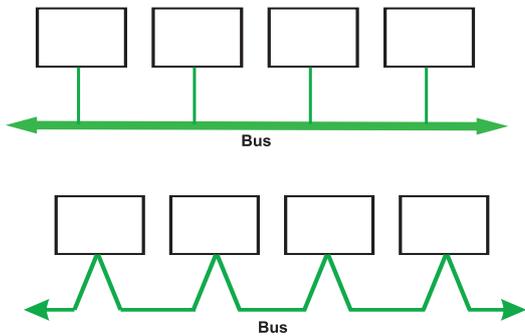
La typologie bus se met en œuvre soit par chaînage des équipements les uns avec les autres, soit par connexion via un boîtier de raccordement (TAP) au câble principal (⇒ Fig.4).

• Topologie en étoile

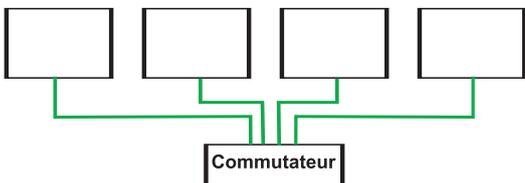
Cette typologie est la plus courante au niveau de l'entreprise et de l'atelier. Elle est celle du réseau Ethernet. Elle présente l'avantage d'être très souple en matière de gestion et de dépannage. Les stations finales sont reliées ensemble à travers un équipement intermédiaire (répéteur, commutateur). La défaillance d'un nœud ne perturbe pas le fonctionnement global du réseau, en revanche, l'équipement intermédiaire qui relie tous les nœuds constitue un point unique de défaillance.

• Autres topologies (⇒ Fig.6)

- La **typologie en anneaux** reprend la topologie physique de l'étoile en apportant une meilleure disponibilité du réseau.
- La **typologie en réseau maillé** est assez peu utilisées dans l'industrie et présente l'inconvénient d'un nombre important de liaisons.



↑ Fig. 4 Topologie des réseaux



↑ Fig. 5 Topologie des réseaux en étoile

En anneau	Maillée
<p>La typologie en anneaux reprend la topologie physique de l'étoile en apportant une meilleure disponibilité du réseau.</p>	<p>La typologie en réseau maillé est assez peu utilisée dans l'industrie et présente l'inconvénient d'un nombre important de liaisons.</p>

↑ Fig. 6 Autres topologies des réseaux

■ Protocole

Un protocole de communication est une spécification de plusieurs règles pour un type de communication particulier. Initialement, on nommait protocole, ce qui est utilisé pour communiquer sur une même couche d'abstraction entre deux équipements différents. Par extension de langage, on utilise parfois ce mot aussi aujourd'hui pour désigner les règles de communication entre deux couches sur un même équipement.

Le modèle OSI (Open System Interconnexion) a été créé par l'ISO (Organisation internationale de normalisation) qui a édité la norme ISO 7498 dans le but d'offrir une base commune à la description de tout réseau informatique. Dans ce modèle, l'ensemble des protocoles d'un réseau est décomposé en 7 parties appelées couches OSI, numérotées de 1 à 7. Les couches OSI respectent les principes suivants :

- chaque couche supporte un protocole indépendamment des autres couches,
- chaque couche procure des services à la couche immédiatement supérieure,
- chaque couche requiert les services de la couche immédiatement inférieure,
- la couche 1 décrit le médium (le support de communication),
- la couche 7 procure des services à l'utilisateur ou à une application.

Lors d'une communication, l'utilisateur d'un réseau utilise les services de la couche 7 via un programme. Cette couche met en forme et enrichit l'information qu'elle reçoit du programme en respectant son protocole. Puis, elle l'envoie à la couche inférieure lors d'une demande de service. À chaque couche, l'information subit des mises en forme et des ajouts en fonction des protocoles utilisés. Enfin, elle est envoyée sur le médium et reçue par un autre nœud du réseau. Elle parcourt toutes les couches de ce nœud dans l'autre sens pour finir au programme du correspondant, dépouillée des différents ajouts liés aux protocoles.

Le modèle à 7 couches proposé par l'OSI (⇒ Fig. 7) a fait l'objet d'implémentations chez divers constructeurs, mais sans succès commercial. Le marché s'étant largement orienté vers le modèle à 4 couches TCP/IP plus facile à comprendre et à utiliser et pour lequel des implémentations portables existaient déjà. Le modèle garde toutefois un intérêt théorique, bien que les frontières des 4 couches TCP/IP ne correspondent pas à d'exacts équivalents en OSI. Nous décrivons ces différentes couches dans le paragraphe dédié à Ethernet.

N°	Couche ISO	Fonction de la couche	Exemples
7	Application	Elle est l'interface avec l'utilisateur, et fait parvenir les requêtes à la couche de présentation.	HTTP, SMTP, POP3, FTP, Modbus
6	Présentation	Elle définit la manière dont les données vont être représentées. Elle convertit les données pour assurer leur interprétation par tous les systèmes.	HTML, XML
5	Session	Elle assure les communications et les liaisons correctes entre les systèmes. Elle définit l'ouverture des sessions sur les équipements du réseau.	ISO8327, RPC, Netbios
4	Transport	Elle permet d'établir une communication de bout en bout. Elle gère la segmentation et le ré-assemblage des données, le contrôle du flux ainsi que la détection d'erreur et la reprise sur erreur.	TCP, UDP, RTP, SPX, ATP
3	Réseau	Elle s'occupe de l'acheminement de paquets (datagrammes) à travers le réseau.	IP, ICMP, IPX, WDS
2	Liaison	Elle permet d'établir, à partir du support physique, une liaison exempte d'erreurs.	ARCnet, PPP, Ethernet, Token ring
1	Physique	Elle définit les protocoles d'échange de bits et les aspects électriques, mécaniques et fonctionnels de l'accès au réseau.	CSMA, RS-232, 10Base-T, ADSL

↑ Fig. 7 Les couches ISO

■ Trame

La trame (⇒ Fig.8) est l'ensemble des informations transmises en un seul bloc via un réseau. Elle est également appelé paquet. Chaque trame respecte la même organisation de base et contient des informations de contrôle, telles que les caractères de synchronisation, les adresses de station, une valeur de contrôle d'erreur, ainsi qu'une quantité variable de données.

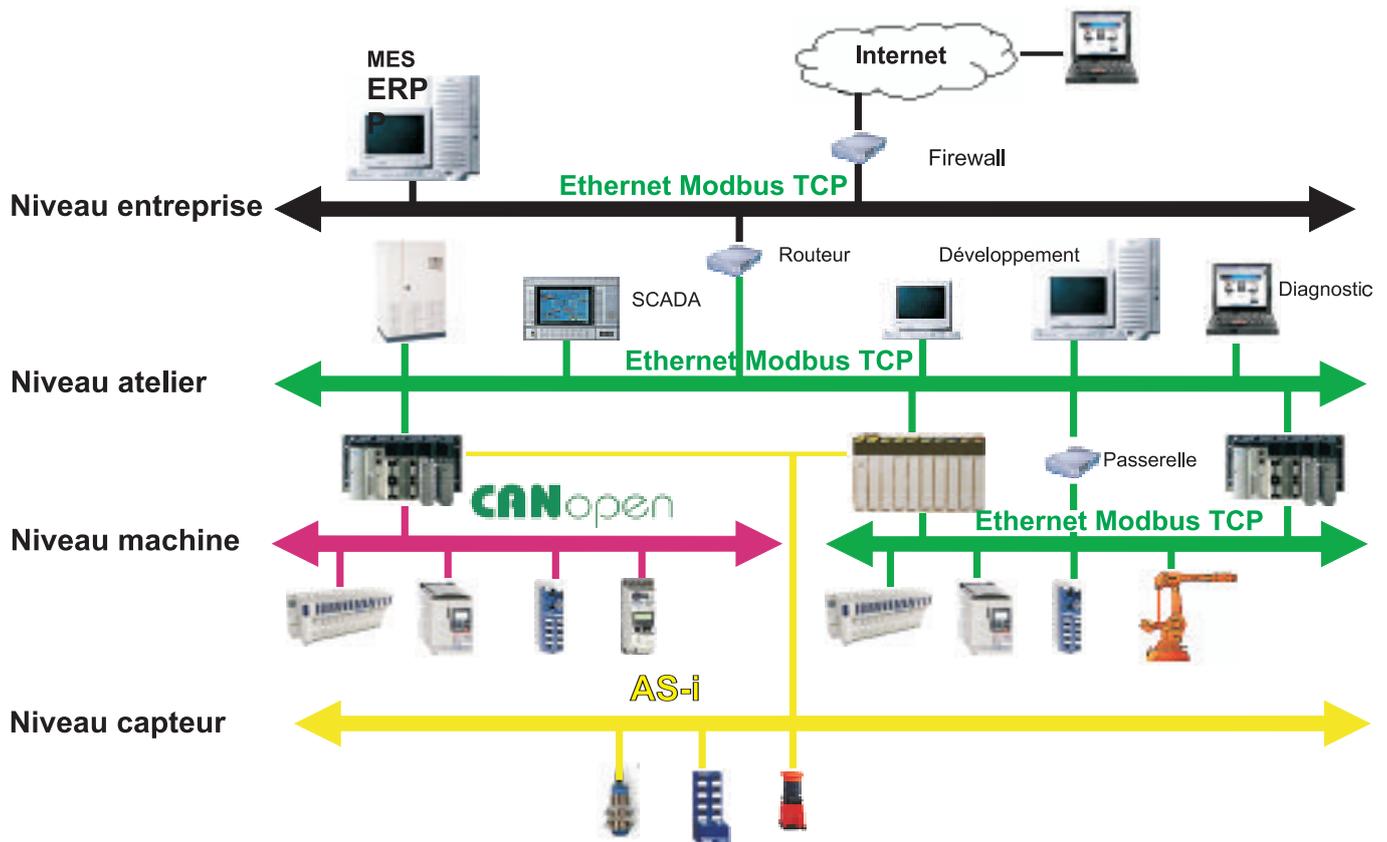
Préambule	Délimiteur trame	Adresse destination	Adresse origine	taille données	Données	Contrôle séquence trame
-----------	------------------	---------------------	-----------------	----------------	---------	-------------------------

↑ Fig. 8

Constitution d'une trame

9.5 Les réseaux préconisés par Schneider Electric

Dans le but de répondre à l'ensemble des besoins tout en rationalisant son offre, l'entreprise a sélectionné trois des réseaux de communications (⇒ Fig.9) pour réaliser les implémentations préférées qui ont été présentées dans l'introduction de cet ouvrage.



↑ Fig. 9

Les niveaux de communication retenus par Schneider Electric

■ Ethernet Modbus TCP

La généralisation d'Ethernet dans les entreprises et sur Internet en a fait un standard de communication incontournable. Son usage généralisé a permis de réduire les coûts de connexion, d'augmenter les performances, la fiabilité et les fonctionnalités. Sa rapidité ne limite pas les applications, son architecture permet facilement les évolutions. Les produits et les logiciels demeurent compatibles, ce qui assure la pérennité des systèmes. Le protocole "Modbus", standard de fait dans l'industrie, fournit une couche application simple et peu onéreuse à mettre en œuvre.

■ Can Open

Can Open est la version industrielle du bus CAN. Créé pour l'automobile, ce réseau a prouvé sa souplesse et sa fiabilité depuis plus de 10 ans dans de multiples applications telles que les équipements médicaux, les trains, les ascenseurs, ainsi que dans de multiples machines et installations. La forte diffusion de ce réseau a confirmé Schneider Electric dans son choix.

■ As-Interface

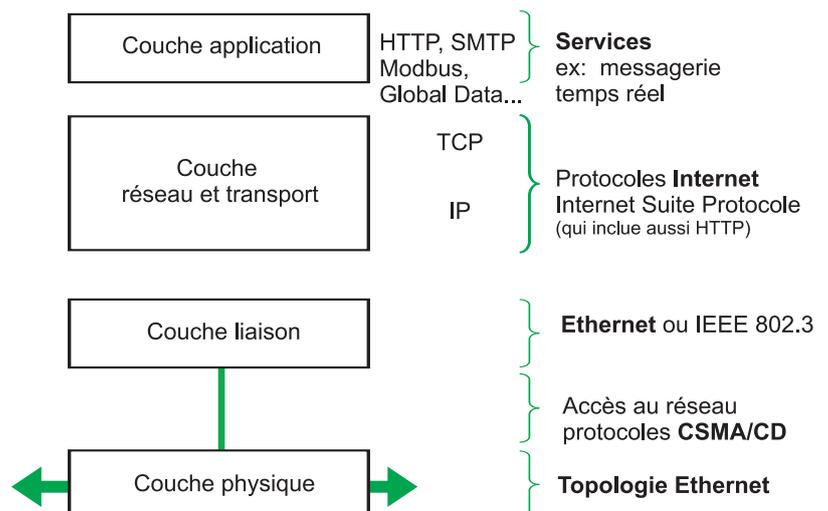
Les machines modernes ont une grande quantité d'actionneurs et de capteurs et souvent des contraintes de sécurité. AS-Interface est le réseau niveau capteur conforme aux exigences des automatismes industriels. Il présente l'avantage d'offrir une connectique rapide et un seul câble pour véhiculer les informations et l'alimentation.

9.6 Ethernet TCP/IP

■ Description générale

L'Ethernet est basé sur le principe d'accès au media régit par un mécanisme de détection de collision. Chaque station est identifiée par une clé globalement unique, appelée adresse MAC, afin de s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes. Cette technologie connue sous le nom de Carrier Sense Multiple Access with Collision Detection (Détection de porteuse avec accès multiples et détection de collision) ou CSMA/CD garantit qu'une seule station à la fois transmet un message sur le media.

Les évolutions successives d'Ethernet ont donné naissance au standard IEEE 802.3 (voir le site www.ieee.org). Il définit seulement les caractéristiques des couches physiques, la façon dont les informations accèdent au réseau (ainsi que la trame de donnée doivent être définies par des couches complémentaires). Il y a souvent confusion entre ces différentes notions, la *figure 10* les situe. Les protocoles mentionnés sont explicités dans les paragraphes suivants.



↑ Fig. 10 Les différentes couches

Ethernet a été présent dans l'industrie depuis de nombreuses années sans grand succès. Il était perçu comme non déterministe par les fournisseurs et les clients. Les besoins temps réel les ont détournés de ce standard au profit de réseaux propriétaires. Finalement, la combinaison de protocoles, issus de l'industrie à ceux d'Internet a contribué à son acceptation.

■ La couche physique

La couche physique décrit les caractéristiques physiques de la communication, comme les conventions à propos de la nature du médium utilisé pour les communications (les câbles, les liens par fibre optique ou par radio), et tous les détails associés comme les connecteurs, les types de codage ou de modulation, le niveau des signaux, les longueurs d'ondes, la synchronisation et les distances maximales.

■ La couche de liaison de données

La couche de liaison de données spécifie le contrôle d'accès au média et comment les paquets sont transportés sur la couche physique, et en particulier le tramage (les séquences de bits particulières qui marquent le début et la fin des paquets). Les en-têtes des trames Ethernet, par exemple, contiennent des champs qui indiquent à quelle machine du réseau un paquet est destiné.

■ La couche réseau

Dans sa définition d'origine, la couche de réseau résout le problème de l'acheminement de paquets à travers un seul réseau. Avec l'avènement de la notion d'interconnexion de réseaux, des fonctions additionnelles ont été ajoutées à cette couche, et plus spécialement l'acheminement de données depuis un réseau source vers un réseau destinataire. Ceci implique généralement le routage des paquets à travers un réseau de réseaux, connu sous le nom d'Internet.

Dans la suite de protocoles Internet, IP assure l'acheminement des paquets, depuis une source vers une destination quelque soit sa localisation dans le monde. Le routage IP est permis grâce à la définition d'un principe d'adressage IP qui assure et oblige l'unicité de toute adresse IP. En effet, chaque station est identifiée par une adresse IP qui lui est propre. Le protocole IP inclut aussi d'autres protocoles, comme ICMP (utilisé pour transférer des messages de diagnostic liés aux transmissions IP) et IGMP (utilisé pour gérer les données multicast). ICMP et IGMP sont situés au-dessus d'IP, mais participent aux fonctions de la couche réseau, ce qui illustre l'incompatibilité entre les modèles Internet et OSI.

La couche réseau IP peut transférer des données pour de nombreux protocoles de plus haut niveau.

■ La couche transport

Les protocoles de la couche de transport peuvent résoudre des problèmes comme la fiabilité des échanges (« Les données sont-elles arrivées à destination ? »), l'adaptation automatique à la capacité des réseaux utilisés, et le contrôle de flux. Il assure également que les données arrivent dans l'ordre correct. Dans la suite de protocoles TCP/IP, les protocoles de transport déterminent aussi à quelle application chaque paquet de données doit être délivré.

TCP est un protocole de transport, orienté connexion. Il fournit un flux d'octets fiable assurant l'arrivée des données sans altération et dans l'ordre, avec retransmission en cas de perte, et élimination des données dupliquées. Il gère aussi les données « urgentes » qui doivent être traitées dans le désordre (même si techniquement, elles ne sont pas émises hors bande). TCP essaie de délivrer toutes les données correctement et en séquence, c'est son but et son principal avantage sur UDP, même si cela peut être un désavantage pour des applications de transfert en temps réel, avec des taux de perte élevées au niveau de la couche réseau. UDP est un protocole simple, sans connexion, « non fiable ». Ceci ne signifie pas qu'il est particulièrement peu fiable, mais qu'il ne vérifie pas que les paquets sont arrivés à destination, et ne garantit pas leur arrivée dans

l'ordre. Si une application a besoin de ces garanties, elle doit les assurer elle-même, ou bien utiliser TCP. UDP est généralement utilisé par des applications de diffusion, tel que les Global Data ou les applications multimédia (audio et vidéo, etc.) pour lesquelles le temps requis par TCP pour gérer les retransmissions et l'ordonnement des paquets n'est pas disponible, ou pour des applications basées sur des mécanismes simples de question/réponse comme les requêtes SNMP, pour lesquelles le surcoût lié à l'établissement d'une connexion fiable serait disproportionné au besoin.

Aussi bien TCP qu'UDP sont utilisés par de nombreuses applications. Les applications utilisant les services TCP ou UDP se distinguent par leur numéro de port. Modbus TCP utilise les services TCP. Le coupleur Factorycast permet d'utiliser UDP.

■ La couche application

C'est dans la couche application que se situent la plupart des fonctions applications du réseau.

Elles incluent HTTP (World Wide Web), FTP (transfert de fichiers), SMTP (messagerie), SSH (connexion à distance sécurisée), DNS (recherche de correspondance entre noms et adresses IP) et beaucoup d'autres.

Les applications fonctionnent généralement au-dessus de TCP ou d'UDP, et elles sont souvent associées à un port bien connu. Exemples :

- HTTP port TCP 80 ou 8080,
- Modbus port 502,
- SMTP port 25,
- FTP port 20/21.

Ces ports ont été assignés par l'Internet Assigned Numbers Authority.

□ Le protocole HTTP (HyperText Transfer Protocol)

C'est un protocole utilisé pour transmettre des pages Web entre un serveur et un navigateur (browser). HTTP est utilisé sur le Web depuis 1990.

Les serveurs Web embarqués dans les produits d'automatisme Transparent Ready permettent un accès aisé aux produits localisés n'importe où dans le monde depuis un navigateur Internet comme Internet Explorer, Netscape Navigator ou tout autre.

□ BOOTP/DHCP

Il est utilisé pour fournir automatiquement les paramètres d'adressage IP aux produits. Ceci évite d'avoir à gérer individuellement les adresses de chaque produit en reportant cette gestion dans un serveur d'adresses IP dédié.

Le protocole DHCP (Dynamic Host Configuration Protocol) permet d'attribuer automatiquement les paramètres de configuration aux produits. DHCP est une extension de BOOTP. Le protocole BOOTP/DHCP comprend 2 composants :

- le serveur pour fournir l'adresse réseau IP,
- le client qui demande l'adresse IP.

Les produits Schneider Electric peuvent être :

- clients BOOTP/DHCP permettant de récupérer automatiquement l'adresse IP en provenance d'un serveur,
- serveurs BOOTP/DHCP permettant au produit de distribuer les adresses IP aux stations du réseau.

Ces protocoles standards BOOTP/DHCP sont utilisés pour offrir le service de remplacement de produits défectueux (FDR, Faulty Device Replacement).

□ File Transfer Protocol (FTP)

Il fournit les éléments de base de transfert de fichiers. Le protocole FTP est utilisé par de nombreux systèmes pour échanger des fichiers entre produits.

□ TFTP : Trivial File Transfer Protocol

C'est un protocole simplifié de transfert de fichier, permettant également de télécharger du code à un produit. Il peut, par exemple, être utilisé pour transférer le code de démarrage (boot code) dans une station de travail non équipée d'unité de disque ou pour se connecter et télécharger des mises à jour de firmware de produits du réseau. Les produits Transparent Ready implémentent FTP et TFTP pour transférer certaines informations entre les produits.

□ NTP (Network Time Protocol)

Ce protocole est utilisé pour synchroniser l'heure d'un produit (client ou serveur) depuis un serveur fournisseur. Selon le réseau utilisé, il fournit à partir de l'heure universelle (UTC), une précision de quelques millisecondes sur un réseau local (LAN) à plusieurs dizaines de millisecondes sur un réseau étendu (WAN).

□ SMTP (Simple Mail Transfert Protocol)

Il fournit un service de transmission d'E-mail. Il permet l'envoi d'E-mail entre un émetteur et un destinataire par l'intermédiaire d'un serveur SMTP.

□ SNMP (Simple network management protocol)

La communauté Internet a développé ce standard pour permettre la gestion des différents composants d'un réseau via un système unique. Le système de gestion du réseau peut échanger des informations avec les produits agents SNMP. Cette fonction permet au gestionnaire de visualiser l'état du réseau et des produits, de modifier leur configuration et de remonter les alarmes en cas de défaut. Les produits Transparent Ready sont compatibles SNMP et peuvent être intégrés naturellement dans un réseau administré via SNMP.

□ COM/DCOM (Distributed Component Object Model) ou OLE (Object Linking and Embedding).

Il s'agit du nom de la technologie composant objet de Windows qui permet une communication transparente entre les applications Windows. Ces technologies sont utilisées dans le logiciel serveur de données OFS (OLE for Process Control Factory Server).

9.7 Services Web et Transparent Ready

Comme nous l'avons mentionné précédemment, les services universels ne permettant pas un usage industriel. Les fabricants de constituant ont donc complété les services universels d'Internet par des fonctions spécifiques aux automatismes.

Schneider Electric a développé une offre qui permet une communication "transparente" entre tous les niveaux que nous avons présentés ci-dessus et le WEB, il le définit comme étant *l'intégration des technologies web² dans ses produits et services*. Cette offre s'appuie sur deux piliers :

- Le réseau Ethernet industriel.
- Les composants WEB.

Dans le but d'offrir des "**Services**" qui sont des fonctions permettant au client d'exécuter des tâches particulières, comme envoyer une information d'un automate à un autre ou déclencher une alarme.

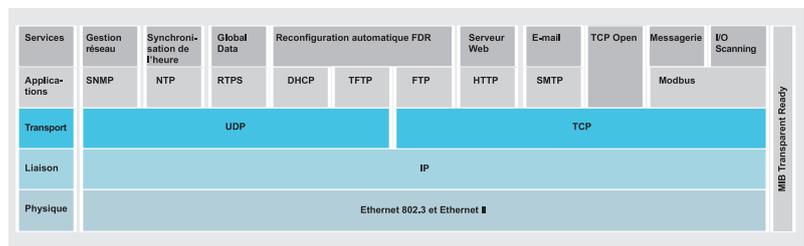
² Le terme "web technologie" est synonyme de "Internet technologie" et couvre : les protocoles internet, les langages de programmation tel que Java, html, xml, etc. ainsi que les outils qui ont révolutionné la façon de partager les informations.

■ Services Ethernet industriel

En complément des services universels Ethernet (HTTP, BOOTP/DHCP, FTP, etc.), huit types de services de communication Ethernet peuvent être fournis par les produits :

- Service de messagerie Modbus TCP.
- Service d'échange d'entrées/sorties distantes : I/O Scanning.
- Service de remplacement d'équipement défaillant : FDR (Faulty Device Replacement).
- Service d'administration de réseau : SNMP.
- Service de distribution de données Globale : Global Data.
- Service de gestion de la bande passante.
- Service de synchronisation de l'heure : NTP.
- Service de notification d'événement : SMTP (E-mail).

Le **tableau 11** positionne ces services par rapport aux différentes couches des réseaux.

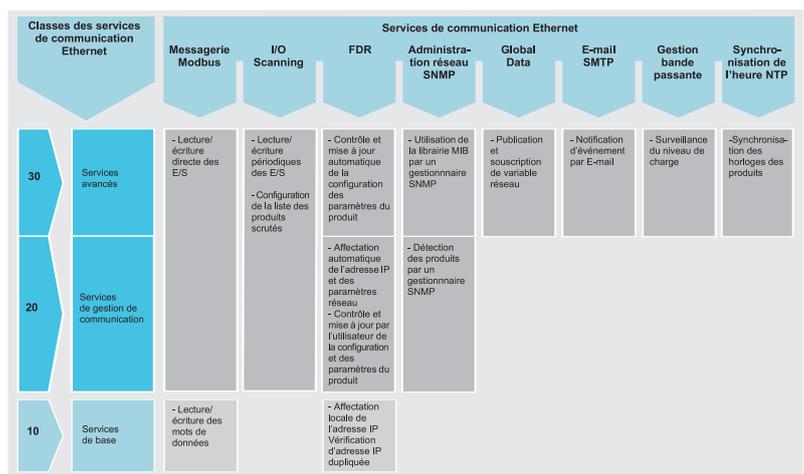


↑ Fig. 11 Services et réseaux

Ces services de communication sont regroupés en trois classes :

- Classe 10 : services de base de communication Ethernet.
- Classe 20 : services de gestion de communication Ethernet (niveau réseau et niveau produit).
- Classe 30 : services avancés de communication Ethernet.

Le **tableau 12** décrit succinctement ces services :



↑ Fig. 12 Les différents services

■ Service de messagerie : Ethernet Modbus TCP

Modbus, le standard de communication de l'industrie depuis 1979 a été porté sur Ethernet TCP/IP, pour constituer Ethernet Modbus TCP, protocole totalement ouvert sur Ethernet. Le développement d'une connexion à Ethernet Modbus TCP ne nécessite aucun composant propriétaire, ni achat de licence. Ce protocole peut être porté facilement sur n'importe quel produit supportant un stock de communication TCP/IP standard. Les spécifications peuvent être obtenues gratuitement depuis le site Web : www.modbus-ida.org.

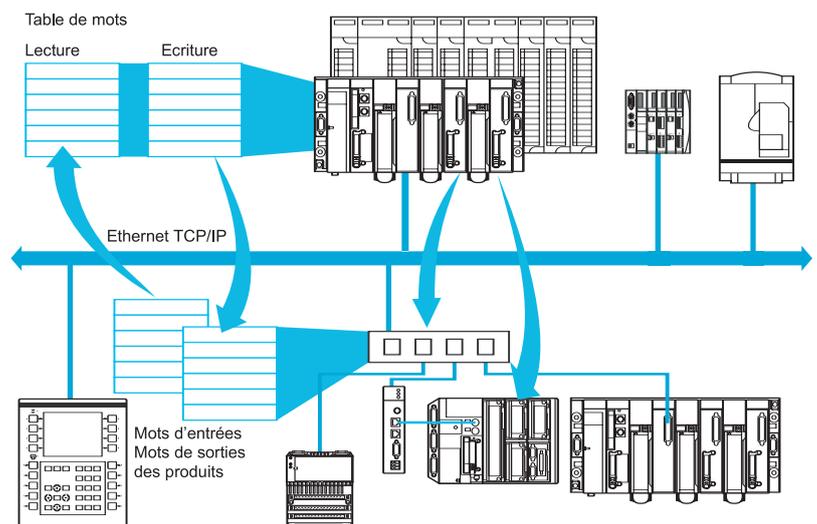
Sa simplicité permet à n'importe quel produit de terrain, tel qu'un module d'entrées/sorties, de communiquer sur Ethernet sans avoir besoin d'un puissant microprocesseur ou de beaucoup de mémoire interne. Dues à la simplicité de son protocole et au débit important d'Ethernet 100 Mbit/s, les performances de Ethernet Modbus TCP sont excellentes. Ceci permet d'utiliser ce type de réseau dans des applications temps réel, telle que la scrutation d'entrées/sorties.

Comme le protocole application est identique sur Modbus liaison série, Modbus Plus ou Ethernet Modbus TCP, il est permis de router les messages d'un réseau sur l'autre sans faire de conversion de protocole. Modbus étant implémenté au-dessus de la couche TCP/IP, les utilisateurs peuvent en plus bénéficier du routage IP permettant à des produits situés n'importe où dans le monde de communiquer sans se soucier de la distance qui les sépare.

L'organisation IANA (Internet Assigned Numbers Authority) a attribué à Ethernet Modbus TCP, le port fixe TCP 502. Ainsi Modbus devient un standard du groupement Internet. La taille maximale des données est de 125 mots ou registres en lecture et de 100 mots ou registres, en écriture.

■ Service d'échange d'entrées/sorties distantes : I/O Scanning

Ce service permet de gérer l'échange d'états entre des entrées/sorties distantes à travers le réseau Ethernet. Après une simple configuration et sans besoin de programmation spécifique, la scrutation des entrées/sorties est effectuée d'une manière transparente à l'aide de requêtes de lecture/écriture selon le protocole client/serveur Ethernet Modbus TCP. Ce principe de scrutation, via un protocole standard, permet de communiquer avec n'importe quel produit supportant un Ethernet Modbus TCP. Ce service permet de définir deux zones de mots, l'une réservée à la lecture des entrées, l'autre à l'écriture des sorties (⇒ Fig.13). Les périodes de rafraîchissement sont indépendantes du cycle automate.



↑ Fig. 13 Service d'échange d'entrées/sorties distantes

En fonctionnement, le module assure :

- La gestion des connexions TCP/IP avec chacun des produits distants.
- La scrutation des produits et la recopie des entrées/sorties dans la zone de mots configurée.
- La remontée de mots d'état permettant de contrôler le bon fonctionnement du service depuis l'application automate.
- L'application de valeurs de repli pré configurées en cas de problème de communication.

Une offre des produits matériels et logiciels permettant d'implémenter le protocole I/O Scanning sur tout type de produit connectable au réseau Ethernet Modbus TCP peut être consultée sur le site Web Modbus-IDA (www.modbus-ida.org).

■ Service de remplacement d'équipement défaillant : FDR (Faulty Device Replacement)

Le service de remplacement d'un produit défaillant utilise la technologie standard de gestion d'adresse (BOOTP, DHCP) et le service de gestion de fichiers FTP ou TFTP (Trivial File Transfer Protocol), ceci dans le but de faciliter la maintenance des équipements connectés sur Ethernet Modbus TCP.

Il permet de remplacer un produit en défaut par un produit neuf en garantissant sa détection, sa reconfiguration et son redémarrage automatique par le système. Les principales étapes pour le remplacement sont :

- Un produit utilisant le service FDR tombe en défaut.
- Un autre produit similaire est sorti du parc de maintenance, pré-configuré avec le "nom d'identification" (Device name) du produit en panne, puis réinstallé sur le réseau. Selon les produits, l'adressage peut s'effectuer à l'aide de sélecteurs rotatifs (par exemple, E/S distribuées Advantys STB, ou Advantys OTB) ou par le clavier intégré au produit (par exemple, variateurs de vitesse Altivar 71).
- Le serveur FDR détecte le nouveau produit, lui attribue une adresse IP et lui transfère les paramètres de configuration.
- Le produit substitué vérifie que tous ces paramètres sont bien compatibles avec ses propres caractéristiques et commute en mode opérationnel.

■ Service d'administration de réseau : SNMP

Le protocole SNMP (Simple Network Management Protocol) permet, depuis une station gestionnaire de réseau, de surveiller et de contrôler tous les composants de l'architecture Ethernet et ainsi d'en assurer un diagnostic rapide en cas de problème. Il permet :

- D'interroger les composants du réseau, tels que les stations informatiques, les routeurs, les commutateurs, les bridges ou les produits terminaux pour visualiser leur état.
- D'obtenir des statistiques du réseau sur lequel les produits sont connectés.

Ce logiciel de gestion de réseau respecte le modèle traditionnel client/serveur. Néanmoins, pour éviter la confusion avec les autres protocoles de communication qui utilisent cette terminologie, on parle plutôt de gestionnaire de réseau ou d'agent SNMP.

Les produits Transparent Ready peuvent être gérés par n'importe quel gestionnaire de réseau SNMP, parmi lesquels HP Openview ou IBM Netview et bien sûr l'outil de gestion de réseau Transparent Ready ConnexView. Le protocole standard SNMP (Simple Network Management Protocol) permet l'accès aux objets de configuration et de gestion qui sont contenus dans les MIB (Management Information Base) des produits. Ces MIB doivent respecter certains standards pour être accessibles par tous les outils gestionnaires du marché, mais selon la complexité des produits, les constructeurs peuvent ajouter certains objets dans la base de données MIB privée. La MIB privée Transparent Ready présente des objets de gestion spécifiques aux services de communication Transparent Ready tels que Modbus, Global data, FDR, etc. Ces objets facilitent l'installation, la mise en œuvre et la maintenance des produits.

Les produits Transparent Ready supportent 2 niveaux de gestion de réseau SNMP :

- L'interface MIB II Standard : un premier niveau de gestion de réseau est accessible via cette interface. Il permet au gestionnaire d'identifier les produits composant l'architecture et de récupérer des informations générales sur la configuration et le fonctionnement des interfaces Ethernet TCP/IP.
- L'interface MIB Transparent Ready : la gestion des produits Transparent Ready est améliorée via cette interface. Cette MIB présente un ensemble d'informations permettant au système de gestion de réseau de superviser tous les services Transparent Ready. Elle peut être téléchargée depuis le serveur FTP de tout module Ethernet Transparent Ready d'un automate programmable.

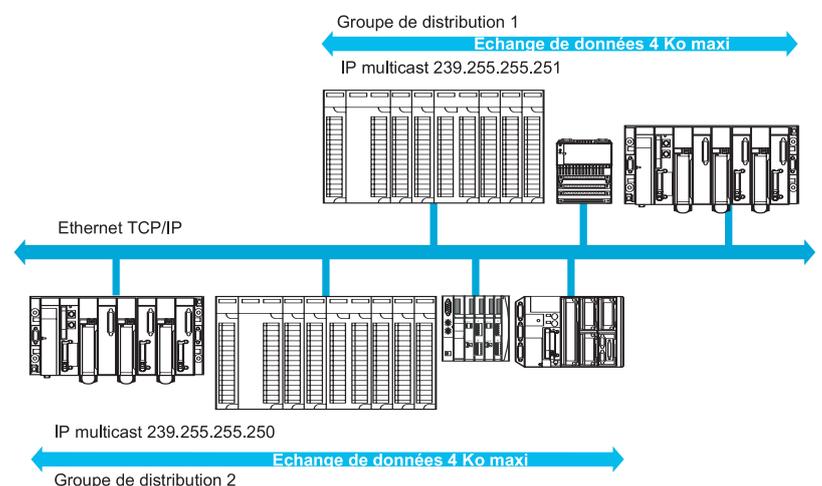
■ Service de distribution de données Globales : Global Data (⇒ Fig.14)

Le service Global Data assure la distribution en multicast de données en temps réel entre des stations appartenant à un même groupe de distribution. Il permet de synchroniser des applications distantes, ou bien de partager une base de données commune entre plusieurs applications distribuées. Les échanges sont basés sur un protocole standard de type Publication/souscription, garantissant des performances optimales avec un minimum de charge sur le réseau.

Ce protocole RTPS (Real Time Publisher Subscriber) est promu par Modbus-IDA (Interface for Distributed Automation), et est déjà un standard adopté par plusieurs constructeurs, 64 stations peuvent participer aux échanges via Global Data au sein d'un même groupe de distribution. Chaque station peut :

- publier une variable de 1024 octets. La période de publication est configurable de 1 à n périodes de la tâche maître du processeur,
- souscrire de 1 à 64 variables.

La validité de chaque variable est contrôlée par des bits d'état (Health Status bits) liés à un timeout de rafraîchissement configurable entre 50 ms et 1 s. L'accès à un élément de variable n'est pas possible. La taille totale des variables souscrites atteint 4 K octets contigus. Afin d'optimiser encore les performances du réseau Ethernet, les Global Data peuvent être configurées avec l'option "multicast filtering" qui, en relation avec les switches de la gamme ConneXium assure la diffusion des données uniquement sur les ports Ethernet où existe une station abonnée au service Global Data. Si ces "switches" ne sont pas utilisés, les Global Data sont émises en "multicast" sur tous les ports du "switch".



↑ Fig. 14 Global Data

■ Service NTP de synchronisation de l'heure

Le service de synchronisation de l'heure est basé sur le protocole NTP (Network Time Protocol). Il permet de synchroniser l'heure d'un client ou d'un serveur sur Ethernet TCP/IP depuis un serveur ou une autre source de temps de référence (radio, satellite, etc.).

Les modules de communication Ethernet Modbus TCP : -140 NOE 771 11 de la plate-forme d'automatisme Modicon Quantum Unity V2.0 (ou plus) -TSX ETY 5103 de la plate-forme d'automatisme Modicon Premium Unity V2.0 (ou plus) disposent d'un composant client NTP. Ces modules sont capables de se connecter à un serveur NTP en utilisant une requête client (unicast), afin de mettre à jour leur heure locale. Périodiquement (de 1 à 120 secondes), l'horloge du module est mise à jour avec une erreur inférieure à 10 ms pour les processeurs courants et inférieures à 5 ms pour les processeurs hautes performances. Si le serveur NTP n'est pas joignable, le module Ethernet Modbus TCP se dirige vers un serveur NTP de secours (standby).

■ Service SMTP de notification par E-mail

Ce service de notification, simple par E-mail, est programmable. Il permet à l'application automate de signaler un événement sur conditions.

L'automate crée un E-mail automatiquement et de façon dynamique, pour alerter un destinataire défini, connecté localement au réseau ou à distance. L'E-mail peut contenir des variables, des alarmes et/ou des événements. Il est à noter que ce service est disponible avec les derniers modules de communication Ethernet pour automates Modicon Premium et Modicon Quantum, ainsi que les derniers processeurs avec connexion Ethernet des mêmes automates, utilisés avec le logiciel Unity Pro. Un service plus complet et indépendant de l'application automate, est également disponible avec le module serveur Web actif FactoryCast HMI.

Un mécanisme simple et efficace est utilisé : des en-têtes de messages prédéfinies sont liées avec le corps de l'E-mail, lui-même créé dynamiquement depuis les dernières informations de l'application automate. Sur des conditions prédéterminées, l'application automate prépare le message. Par l'utilisation d'un bloc fonction, une des 3 en-têtes prédéfinies est sélectionnée, un e-mail est créé, intégrant des variables et du texte (jusqu'à 240 octets) et envoyé directement depuis l'automate. Chacune des trois en-têtes contient les éléments suivants prédéfinis :

- La liste des destinataires de l'e-mail.
- Le nom de l'émetteur et sujet.

Ces informations sont définies et mises à jour par un administrateur autorisé, utilisant les pages Web de configuration.

■ Les services Web (⇒ Fig.15)

Le niveau de service d'un serveur Web est défini par 4 classes de services identifiées par une lettre :

□ Classe A

Elle définit les équipements Transparent ready sans aucun services WEB.

□ Classe B

C'est le niveau web de base. Il fournit la possibilité de gérer des pages WEB statiques qui sont préconfigurées dans un équipement Transparent ready. Il permet d'offrir des services de diagnostic et de surveillance d'équipement à partir d'un navigateur WEB standard.

□ Classe C

C'est le niveau Web configurable. Il permet la personnalisation du site WEB d'un équipement Transparent Ready avec des pages WEB définies par l'utilisateur pour les besoins de son application. En conséquence le diagnostic et le contrôle du procédé client peut s'effectuer à partir d'un navigateur WEB standard. L'offre Factory Cast fournit ce niveau de fonctionnalité Web. Elle comprend également les outils facilitant la gestion et la modification des sites WEB embarqués.

□ Classe D

C'est le niveau Web actif. Il permet en plus de réaliser du traitement spécifique directement dans l'équipement Transparent Ready serveur WEB. Cette capacité de traitement permet de faire du pré-calcul, de la gestion d'une base de données temps réel, de la communication avec des bases de données relationnelles et des envois d'e-mail. En conséquence, la communication entre le navigateur et le serveur est réduite et optimisée. L'offre Factory Cast HMI fournit ce niveau de fonctionnalité Web. Elle comprend également les outils permettant la configuration des traitements à effectuer dans l'équipement Web serveur.

Classe serveur Web	Services Web			
	Maintenance	Contrôle	Diagnostic	Optionnel
D Serveur Web actif	- Mise à jour du site Web utilisateur	- Exécution autonome de services particuliers (par exemple, envoi E-mail, envoi de données, calculs...)	- Etats définis par l'utilisateur	- Documentation utilisateur
C Serveur Web configurable		- Editeur de variables automate - Commandes distantes - Pages Web utilisateur	- Diagnostic des services de communication - Etat des ressources internes du produit	
B Serveur Web de base	- Mise à jour à distance du logiciel du produit - Auto-tests à distance	- Description du produit	- Etat du produit	- Configuration des paramètres réseau et des services de communication Ethernet - Documentation produit
A Pas de serveur Web	- Aucun service Web			

↑ Fig. 15 Les services web

□ Les produits Transparent Ready

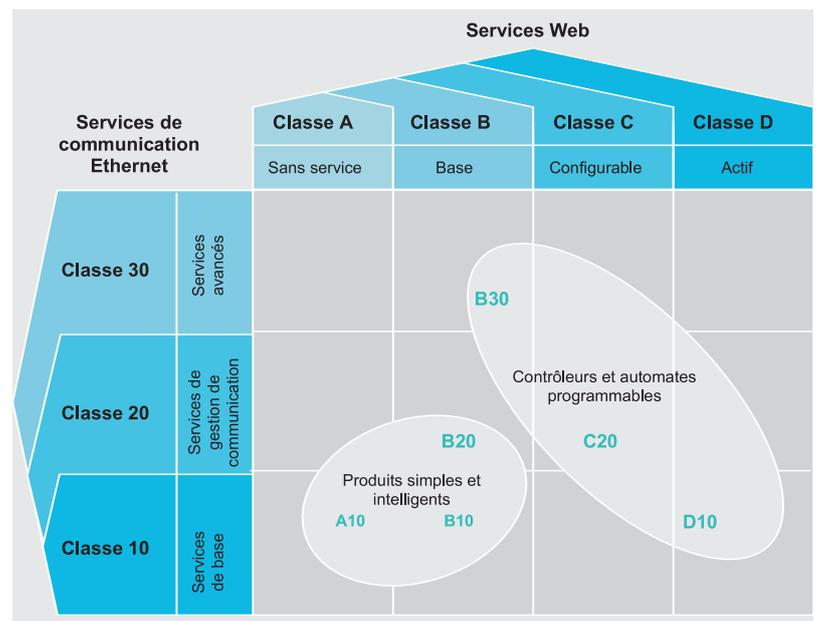
Ils s'identifient par une lettre définissant le niveau de services Web, suivie par un nombre définissant le niveau de service de communication Ethernet. Par exemple :

- Le produit de classe A10 correspond à un produit sans service Web et avec les services de base Ethernet.
- Le produit de classe C30 correspond à un produit disposant d'un serveur Web configurable et des services avancés de communication Ethernet.

Les services offerts par une classe supérieure incluent tous les services supportés par une classe inférieure. Le choix des produits Transparent Ready se fait dans 4 grandes familles :

- Produits de terrain (simples ou intelligents) du type capteurs et pré-actionneurs.
- Contrôleurs et automates programmables.
- Applications IHM (Interface Homme/Machine).
- Passerelles et serveurs dédiés.

Le tableau de sélection de la *figure 16* permet le choix des produits Transparent Ready en fonction des classes de services souhaités.



↑ Fig. 16

Le choix des produits Transparent Ready

9.8 Bus Can Open

■ Description générale

Le bus CAN (Controller Area Network) est un bus système série développé par Bosch pour l'automobile. Il fut présenté avec Intel en 1985. L'objectif était de réduire la quantité de câbles dans les véhicules (il y a jusqu'à 2 Km de câbles par voiture) en faisant communiquer les différents organes de commande sur un bus unique et non plus sur des lignes dédiées. Le but étant de réduire le poids des véhicules.

La très bonne immunité aux perturbations électromécaniques associée à la fiabilité de la transmission en temps réel a suscité l'intérêt des industriels. En 1991, naît le consortium CIA (= CAN in Automation). Son objectif est de promouvoir l'application de CAN dans l'industrie (voir le site : <http://www.can-cia.de/>).

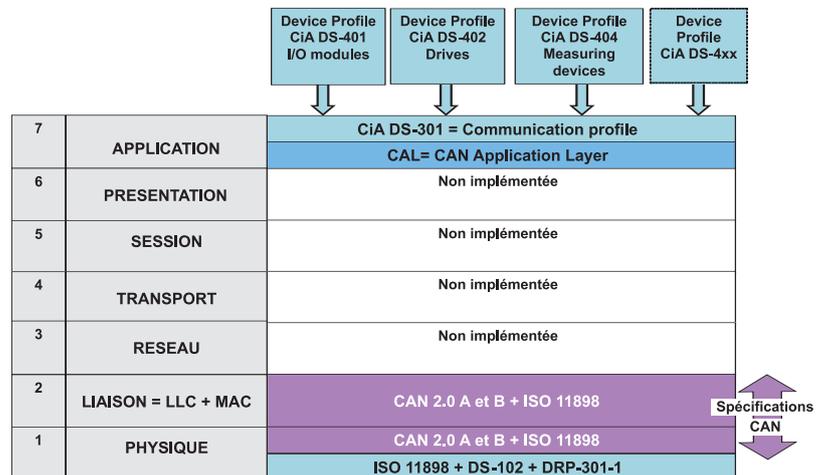
En 1993, le CIA publie les spécifications CAL = CAN Application Layer qui décrivent les mécanismes de transmission sans préciser quand et comment les utiliser. En 1995, le CIA édite le profil de communication DS-301 : CANopen.

Plusieurs couches applications de niveau 7 sur la *figure 17* ont été définies sur la norme CAN :

- Can Open.
- DeviceNet.
- CAL.
- SDS.
- CAN Kingdom.

Enfin en 2001, la publication par le CIA de la DS-304 permis d'intégrer des composants de sécurité de niveau 4 sur un bus Can Open standard (CANsafe).

Nous développons à la *figure 17* les caractéristiques techniques de Can Open.



↑ Fig. 17 Les couche du bus CAN

■ Les avantages de Can Open

□ Can Open utilise des trames courtes

Grâce à sa grande immunité aux perturbations électromagnétiques (EMI), Can Open, permet à la machine ou à l'installation d'effectuer un travail précis, même dans un environnement de fortes interférences. Les trames courtes Can Open et la connexion "CANground" fournissant les mêmes possibilités pour chaque équipement connecté au réseau, protègent contre les perturbations électromagnétiques (EMI).

□ Can Open permet une transmission fiable

Lorsqu'un équipement Can Open transmet ses données, le système génère et prend en compte automatiquement la priorité du message. La perte d'un télégramme à cause de problèmes de collision est impossible, et la perte de temps en attendant le prochain état inactif (idle) du réseau est évité. Can Open permet une transmission de données absolument fiable. Ceci constitue une des raisons pour lesquelles Can Open est utilisé dans les équipements médicaux nécessitant des réseaux fiables.

□ Can Open supprime les pertes de temps

Les pertes de temps sont toujours consommatrices de temps et d'argent. CANopen est conçue afin de réduire ces pertes de temps autant que possible. Avec sa distance de "Hamming" de 6, Can Open possède une très bonne détection d'erreur, et un très bon mécanisme de correction. Avec une probabilité de une erreur non détectée en 1000 ans³, Can Open est le plus fiable des réseaux pour machines et installations.

³ 1 bit d'erreur toutes les 0.7 s à 500 Kbit/s, 8 h par jour, 365 jours par an

Dans le cas où le réseau détecte une condition d'erreur, le chien de garde est la première possibilité de surveillance de l'état de l'équipement. Chaque message de diagnostic contient la source et la raison de l'erreur, ce qui permet une réaction rapide et une réduction des pertes de temps. Un diagnostic supplémentaire est développé pour améliorer le diagnostic des équipements Can Open complexes, et pour maintenir le réseau. De plus, pour aider à la détection des erreurs aléatoires, un historique des erreurs est disponible.

□ Can Open : Performance et flexibilité

La raison principale pour utiliser un réseau est sa performance et sa flexibilité à s'adapter exactement aux contraintes de l'application. Can Open fournit un dispositif unique pour l'adaptation de la transmission de données. Basé sur le modèle producteur/consommateur, Can Open permet pour la transmission de données, des communications de type diffusion générale, point à point, changement d'état et cyclique. Ce qui veut dire que les données sont transmises uniquement si nécessaire, ou suivant une base de temps spécifique. Les objets données process (PDO) peuvent être configurés individuellement. Les paramètres peuvent être changés à tout moment.

• A propos des performances

Bien que Can Open soit très flexible, la réponse du réseau est rapide. En moins de 1 ms, 256 points d'entrées/sorties numériques peuvent être traités à 1 Mbit/s⁴. Typiquement, Profibus-DP a besoin de environ 2 ms à 12Mbit/s pour le même type d'échange de données. En plus de la réponse rapide, le contrôle de priorités des messages peut être changé.

Can Open fournit les possibilités d'adapter la transmission de données aux contraintes de l'application.

⁴ Source : Grid Control

□ Can Open autorise une baisse des coûts

Can Open combine facilité d'installation avec équipements à faible coût. Can Open n'a pas besoin d'une liaison équipotentielle entre les équipements comme beaucoup de bus de terrain. Une mauvaise connexion entraîne non seulement des erreurs de communication, mais peut aussi causer des dommages sur les équipements du bus de terrain.

En outre, les composants pour Can Open sont produits en grande quantité, ce qui diminue leur prix. Schneider Electric fournit cet avantage de coût à ses clients.

Un prix de 10 à 20 % moindre par rapport à d'autres bus de terrain peut être attendu.

■ Présentation du fonctionnement de CAN

CAN est un bus série basé sur un modèle publication-souscription. Dans ce modèle, un éditeur envoie un message aux souscrivants. CAN a été développé en utilisant une architecture de type "broadcast".

L'expéditeur (éditeur) émet le message accompagné d'un identifiant. Les destinataires (souscrivants) filtrent les messages du bus suivant leurs critères d'envoi. Si ce message leur est destiné, ils vont alors le lire et le traiter. Le destinataire devient alors un expéditeur (⇒ Fig.18).

Le schéma de la figure 18 nous montre le mode "push" (envoi) du modèle publication-souscription. CAN peut aussi supporter le mode "pull" (réception) du modèle publication-souscription. Un client peut déclencher l'envoi d'un message à partir d'une demande de transmission distante. La demande de transmission distante (RTR "Remote Transmission Request") est une trame CAN qui comporte les "flags" (bits d'état) RTR. Lorsque le producteur reçoit une telle demande, il transmet la réponse associée (⇒ Fig.19).

Dans une architecture "broadcast", les différents nœuds du réseau peuvent émettre en même temps. CAN résout ce problème grâce à 2 mécanismes. Premièrement, un expéditeur surveille l'artère de communication pour vérifier si un autre nœud émet déjà. Si l'artère de communication est libre, le nœud commence à émettre. Plusieurs nœuds peuvent commencer à émettre, mais jamais en même temps. Ce problème est résolu par un schéma de priorité.



↑ Fig. 18 Le fonctionnement de CAN



↑ Fig. 19 Les modes « push » et « pull » du modèle publication-souscription

Une trame CAN (⇒ Fig.20) débute avec un bit début de trame (SOF "Start Of Frame"). Onze bits d'identification suivent, du plus significatif au moins significatif. Le bit suivant est le bit de demande d'émission à distance, qui est suivi de 5 bits de contrôle et jusqu'à 8 octets de données utiles. Les bits de contrôle sont : l'ID étendu (IDE), un bit réservé, et 3 bits codant la longueur en octet des données utiles dans la partie donnée (DLC). Une séquence de vérification de la trame (FCS "Frame Check Sequence") jusqu'à 8 octets, suit les données utiles. L'émetteur transmet un bit récessif d'acquittement (ACK), qui est remplacé par un bit dominant par les destinataires qui auront reçu la trame sans erreur.

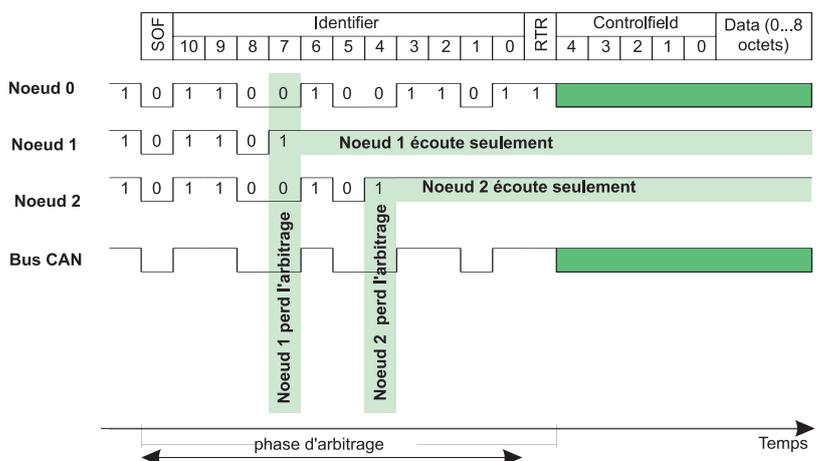


↑ Fig. 20 Trame CAN

Le bit fin de trame (EOF "End Of Frame") indique la fin de la trame. Le bit IFS ("Intermission Frame Space") du bus doit rester en position récessive avant le départ de la prochaine trame. Si aucun nœud n'est prêt à émettre, le bus restera en l'état. Le codage des bits possède 2 valeurs, dominante et récessive. Si 2 nœuds émettent en même temps, le récepteur ne verra que la valeur dominante. En codage binaire, la valeur '0' est dominante et la valeur '1' est récessive. Lorsqu'un nœud émet, il est toujours entendu sur le bus. S'il émet une valeur récessive, et qu'il reçoit un bit dominant, il s'arrête d'émettre et continue de recevoir le bit dominant. Ce mécanisme simple évite les collisions sur le bus CAN. Le message possédant l'identifiant le plus petit est prioritaire sur le bus.

CAN est un bus système à accès multiple, avec écoute de porteuse, détection de collision et arbitrage des priorités des messages (CSMA/CD+AMP). Les collisions ne se produisant jamais, le bus CAN est souvent décrit comme un CSMA/CA (accès multiple avec écoute de porteuse et évitement de collision).

La trame du message décrite sur la figure 21 est une trame de base.



↑ Fig. 21 Trame de base de message sous CAN

Pour des applications qui nécessitent un plus grand nombre d'identifiants, la trame CAN étendue de message a été définie.

La trame étendue possède 18 bits identifiants supplémentaires situés dans l'en-tête, après les bits de contrôle. Ce qui étend la gamme de 211 à 229 identifiants différents. Les deux types de trames peuvent coexister dans un seul bus.

CAN possède plusieurs mécanismes différents pour détecter des messages incorrects :

- La séquence de vérification de la trame (FCS) contient le contrôle par redondance cyclique (CRC) de la trame. Le récepteur vérifie le CRC de la trame et compare le résultat à la FCS. S'ils ne sont pas égaux, cela signifie que la trame comporte une erreur CRC.
- Le récepteur détecte les erreurs dans la structure de la trame. Si la trame a une structure défectueuse, la trame comporte une erreur de format.
- Le récepteur d'une trame publie un bit d'acquittement (ACK) dominant si il a reçu une trame sans erreur. Si l'émetteur ne reçoit pas ce bit d'acquittement dominant, il émet une erreur d'acquittement.
- CAN utilise le codage non retour à zéro (NRZ) avec bourrage de bits. Si l'émetteur doit transmettre 5 bits égaux dans une ligne, il introduit un bit inversé additionnel. Ce bourrage de bit permet au récepteur de se synchroniser sur le train de bits. Les récepteurs suppriment les bits de bourrages de la trame transmise. Si plus de 5 bits ont la même valeur, le récepteur détecte une erreur de bourrage de bits.

Il existe plusieurs niveaux d'application des protocoles possible sur CAN, comme DeviceNet et Can Open, étant donné que CAN ne définit pas un niveau d'application de protocole par lui-même.

■ Présentation de Can Open

Can Open définit une couche d'application et un profil de communication basé sur CAN.

□ Can Open définit les objets de communication (messages) suivants

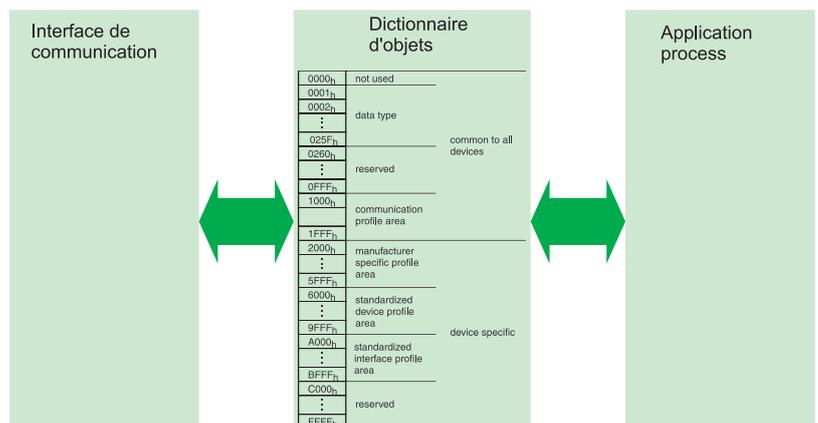
- Objet données processus (PDO).
- Objet données service (S00).
- Objet gestion réseau (NMT).
- Objet fonction spéciale (SYNC, EMCY, TIME).

□ Propriétés

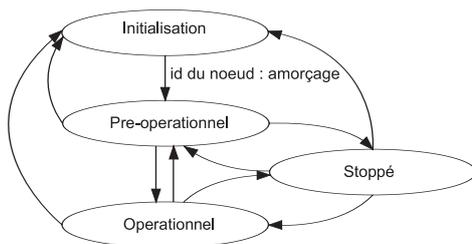
- Transmission des données séries, basée sur le CAN.
- Jusqu'à 1 Mbit/s.
- Efficacité d'environ 57 %.
- Jusqu'à 127 nœuds (équipements).
- Possibilité de plusieurs maîtres.
- Interopérabilités de différents équipements provenant de différents fabricants.

□ Dictionnaire d'objet

Le dictionnaire d'objet (⇒ Fig.22) est une interface entre le programme d'application et l'interface de communication.



↑ Fig. 22 Le dictionnaire d'objet Can Open



↑ Fig. 23 Les objets gestion réseau (NMT) sous Can Open

- **Objets données process (PDO)**

Les objets données process (PDO) sont utilisés pour leur rapidité de transmission des données process. Un PDO peut transporter des données utiles jusqu'à 8 octets, ce qui est le maximum pour une trame CAN. La transmission d'un PDO utilise le modèle producteur consommateur de CAN étendu par transferts synchronisés. Le transfert synchronisé des PDOs s'appuie sur le transfert des messages SYNC sur le bus CAN. Un PDO est envoyé en mode cyclique après un nombre configurable (de 1 à 240) de messages SYNC reçus. Il est aussi possible d'attendre la disponibilité des variables du processus d'application et d'envoyer un PDO après la prochaine réception d'un message SYNC. Ceci est appelé le **transfert synchronisé acyclique**.

- **Objets données service (SDO)**

Les objets données services (SDO) sont prévus pour la transmission des paramètres. Les SDOs fournissent un accès au dictionnaire d'objet des équipements distants. Un SDO n'a pas de restriction de longueur. Si les données utiles ne s'adaptent pas à la trame CAN, elles seront divisées en plusieurs trames CAN. Chaque SDO est acquitté.

La communication SDO utilise la communication point à point, avec un point agissant en tant que serveur et les autres en tant que clients.

- **Objets gestion réseau (NMT)**

Les objets gestion réseau (NMT) changent les états, ou contrôlent les états d'un équipement Can Open (⇒ Fig. 23). Un message NMT est un message avec l'identifiant CAN 0. Ce qui fournit aux messages NMT le plus haut niveau de priorité. Le message NMT consiste toujours en 2 octets de données utiles dans la trame CAN. Le premier octet contient la commande NMT encodée. Le second octet contient l'ID du nœud adressé.

Un équipement CANopen démarre dans l'état « initialisation » une fois le bouton de mise en service appuyé. L'équipement effectue ensuite son initialisation. Lorsque l'équipement a terminé son initialisation, il fournit un objet NMP de démarrage afin de prévenir le maître.

Le protocole de détection de collision pour la surveillance de l'état de l'équipement est implémenté avec les objets NMT.

- **Objets fonctions spéciales (SYNC, EMCY, TIME)**

Can Open doit avoir un producteur SYNC pour synchroniser les actions des nœuds Can Open. Un producteur SYNC émet (périodiquement) l'objet SYNC. L'objet SYNC possède l'identifiant 128. Ceci peut entraîner l'apparition d'un retard ("Pte") due à la priorité de ce message.

L'erreur interne d'un équipement peut déclencher un objet urgence (EMCY). La réaction des clients EMCY dépend des applications. Le standard Can Open définit plusieurs codes d'urgence. L'objet urgence est transmis dans une trame CAN unique de 8 octets.

Une trame CAN avec l'ID CAN 256 et 6 octets de données utiles peut être utilisée pour transmettre l'heure du jour à plusieurs nœuds Can Open.

Cet objet temps (TIME) contient la valeur de la date et de l'heure dans l'objet de type Time-Of-Day.

- **Mécanismes de surveillance (Watchdog)**

Can Open possède 2 méthodes de surveillance de l'état des équipements. Un gestionnaire réseau peut scruter régulièrement chaque équipement à des intervalles de temps configurables. Cette méthode est appelée "Node guarding". Cette technique est cependant consommatrice de bande passante.

Un autre mécanisme est l'envoi régulier d'un message de la part de chaque équipement. Cette méthode permet d'économiser la bande passante par rapport à la méthode dite "Node guarding".

• Longueur du réseau et débit

La longueur est restreinte par le débit dû au procédé de priorité par bit (⇒ Fig.24).

Débit (Kbit/s)	1000	800	500	250	125	50	20	10
Longueur maxi (m)	20	25	100	250	500	1000	2500	5000

↑ Fig. 24 Le procédé de priorité par bit

Dans les documents concernant Can Open, la longueur maximale la plus souvent rencontrée pour un débit de 1 Mbit/s est de 40 m. Cette longueur est calculée sans isolation électrique comme utilisée dans les équipements Can Open de Schneider Electric. En tenant compte de l'isolation électrique, la longueur minimum calculée du bus est de 4 m à 1 Mbit/s. Cependant, l'expérience a montré qu'en pratique, la longueur maximum est de 20m.

Débit (kbps)	1000	800	500	250	125	50	20	10
L max. (m) (1)	0,3	3	5	5	5	60	150	300
Σ L max. (m) étoile locale(2)	0,6	6	10	10	10	120	300	600
Interval min(m) 0,6 x Σ L local (3)		3,6	6	6	6	72	180	360
Σ L max. (m) de tous les bus (4)	1,5	15	30	60	120	300	750	1500

↑ Fig. 25 Tableau des limites de longueur concernant les dérivations

Limitation de longueur concernant les dérivations.

Les limitations concernant les dérivations doivent être prises en compte et sont fixées par les paramètres donnés en figure 25.

- (1) L maxi : longueur maximum d'une dérivation.
- (2) EL maxi étoile locale : valeur maximale de la longueur cumulée des dérivations à un même point lorsqu'un boîtier de dérivation multipoint est utilisé pour créer une topologie étoile locale.
- (3) Intervalle mini : Distance minimum entre 2 boîtiers de dérivation. Longueur maximum des dérivations en un même point. Cette valeur peut être calculée cas par cas pour chaque dérivation : l'intervalle minimum entre deux dérivations est égale à 60% de la longueur cumulée des dérivations au même point.
- (4) EL maxi (m) de tous les bus : valeur maximale de la longueur cumulée de l'ensemble des intervalles et des dérivations sur le bus.

■ Association selon les classes de conformité

Schneider Electric a défini les classes de conformités pour les équipements maîtres et esclaves Can Open de manière similaire à la classification pour Ethernet Modbus TCP et les services Web. Les classes de conformités définissent quel dispositif un équipement peut supporter et assure une compatibilité ascendante des fonctionnalités de chaque classe (⇒ Fig.26).

Caractéristiques				
Classes de conformité		M10	M20	M30
Paramètres des couches	ID de l'esclave	1-16	1-63	1-127
	Débit binaire	Kbit/s 125, 250, 500	M10 + 50, 1000	M20 + 10, 20, 800
	LSS	-		Maître
Equipements supportés		16	63	126
NMT (Objet gestion réseau)	Maître NMT	Maître NMT, conforme à DS301		
	Manager CANopen	-		
	Procédure d'amorçage	Conforme à DSP302		
	Horloge	-		Producteur
SDO (Objet données service)	Auto configuration	-		Supportée
	Client SDO	1	1	2
	Serveur SDO		1	1
	Manager SDO	-		1
PDO (Objet données processus)	Transfert de données SDO	Expédié, transfert de segment		
	COB-ID	Lecture seule	Lecture/écriture	Lecture/écriture
	PDO TT	254, 255	M10 + 0, 1-240	
	PDO Inhibit Time	-	TPDO's (lecture/écriture)	RPDO's & TPDO's (lecture/écriture)
SYNC	PDO Event Timer	-	TPDO's (lecture/écriture)	RPDO's & TPDO's (lecture/écriture)
	SYNC	-	Producteur	Producteur/consommateur
HEALTH	TRIGGER	-		Producteur
	EMCY		Consommateur	Consommateur/producteur
Paramètres	HEALTH	Bits de vie (Heartbeat)	16 consommateurs 1 producteur	63 consommateurs 1 producteur
	Surveillance des noeuds du bus (Node guarding)	Non	Oui	Oui
Paramètres	Enregistrement des paramètres	Non	Oui	Oui
	Classes de conformité			
		S10	S20	S30
Paramètres des couches	ID de l'esclave	1-63	1-127	1-127
	Débit	Kbit/s 125, 250, 500	S10 + 50, 1000	S20 + 10, 20, 800
	LSS	-		Esclave
Equipements de diagnostic			DEL ou écran	
NMT (Objet gestion réseau)	Diagnostic local	-		
	Esclave NMT	<ul style="list-style-type: none"> - Démarrage de noeud distant - Arrêt de noeud distant - Entrée pré opérationnelle - Reset de noeud - Reset de communication 		
SDO (Objet données service)	Horloge	-		Consommateur
	SDO Client	-		1
	SDO Serveur	1		2
	SDO Transfert de données	Expédié, transfert de segment		
PDO (Objet données processus)	COB-ID	Lecture seule	Lecture/écriture	Lecture/écriture
	PDO TT	254, 255	S10 + 0, 1-240	
	PDO paramètres de mappage	FIX (lecture)		-
	Paramètres de connexion	Prédéfinis	Libre	
	PDO Inhibit Time	-	TPDO's (lecture/écriture)	RPDO's & TPDO's (lecture/écriture)
	PDO Event Timer	-	TPDO's (lecture/écriture)	RPDO's & TPDO's (lecture/écriture)
SYNC	SYNC	-	Consommateur	Producteur/consommateur
	TRIGGER	-		Consommateur
HEALTH	EMCY		Producteur	Consommateur/producteur
	HEALTH	Bits de vie (Heartbeat)	1 consommateur 1 producteur	
Paramètres	Surveillance des noeuds du bus (Node guarding)	Non	Oui	oOui
	Enregistrement des paramètres	Non	Non	Nui

Nota : S00 et M00 sont utilisés pour les produits qui ne sont pas 100% conformes à la classe de conformité.

↑ Fig. 26 Tableau de choix des classes de conformité

9. Réseaux industriels

- 9.8 Bus Can Open
- 9.9 Synergie Ethernet et Can Open
- 9.10 Bus AS-Interface (AS-I)

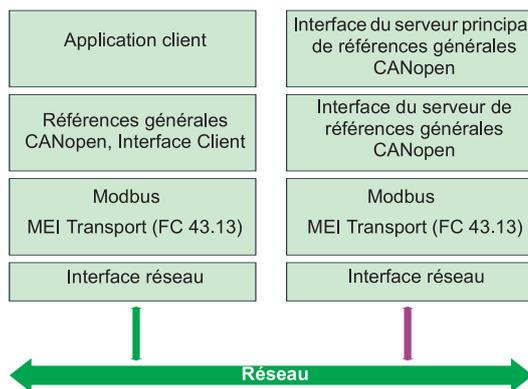
Le *tableau 27* montre les meilleures associations de produits possibles selon les classes de conformité.

Classe de conformité	S10	S20	S30
M10	Association possible	Restriction d'utilisation	
M20			
M30			

↑ *Fig. 27* Classe de conformité et des meilleures associations de produit

Il est cependant possible d'utiliser un équipement esclave avec un maître de classe de conformité inférieure (ex. S20 avec M10), ou un équipement maître avec un esclave de classe de conformité supérieure (ex. M10 avec S20), en utilisant uniquement les équipements supportés par la classe de conformité de niveau inférieur.

9.9 Synergie Ethernet et Can Open



↑ *Fig. 28* Communication de Can Open dans un réseau Ethernet Modbus TCP

Un profil commun de communication (DS-301) définit entre autre l'allocation des identifiants COB-ID pour chaque type de message.

Des profils propres à chaque famille de produits, tels que les E/S tout ou rien (DS-401), E/S analogique, variateurs de vitesse (DS 402), encodeurs, décrivent les différents objets associés.

CAN in Automation et Modbus-IDA ont travaillé ensemble pour créer une norme qui permette une transparence totale entre Can Open et Ethernet Modbus TCP. Cette collaboration a donné comme résultat la spécification CiA DSP309-2, définissant les standards des communications entre un réseau Ethernet Modbus TCP et un bus Can Open. La spécification définit les services de "mapping" permettant à des équipements Can Open de communiquer dans un réseau Ethernet Modbus TCP à travers une passerelle (⇒ *Fig. 28*).

L'accès aux informations d'un équipement Can Open est possible en lecture et en écriture par un grand nombre de fonctions de contrôle d'équipement.

9.10 Bus AS-Interface (AS-I)

■ Description générale

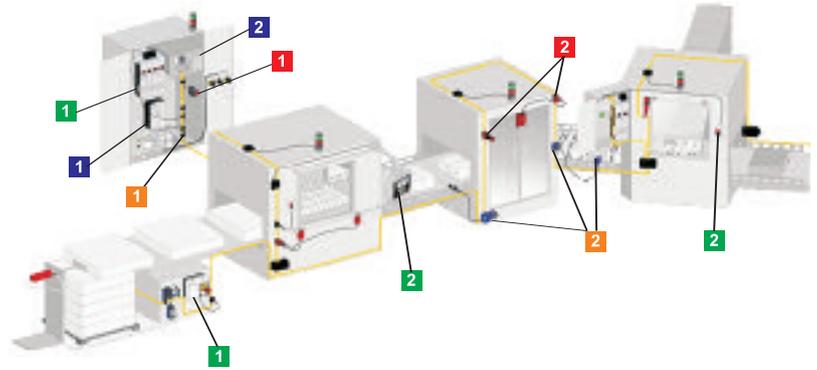
De nos jours les machines disposent de nombreux capteurs et actionneurs avec très souvent la nécessité d'extension et d'intégration de la sécurité. AS-Interface est le réseau niveau capteurs / actionneurs qui correspond aux besoins des systèmes d'automatismes industriels.

Le réseau AS-Interface véhicule la puissance et les données nécessaires sur un seul câble composé de deux fils. Les constituants utilisés sur AS-Interface peuvent être facilement remplacés à l'identique lors de la maintenance, le nouvel esclave reçoit automatiquement l'adresse du produit remplacé.

AS-Interface est une alternative économique au câblage parallèle entre les automates et les capteurs / actionneurs.

L'ensemble de l'offre Schneider Electric est conforme au standard défini par l'organisme AS-international association. AS-Interface est un système ouvert qui garantit l'interchangeabilité et l'interopérabilité entre les différents produits du marché.

AS-Interface est un protocole mature qui a prouvé depuis plus de 10 ans sa facilité d'usage et sa fiabilité dans différents domaines tel que le convoyage, la manutention, l'assemblage, illustrés sur la *figure 29*.



↑ Fig. 29 AS-Interface

- | | |
|---------------------------|--------------------------|
| 1 Interface IP20 | 1 Moniteur de sécurité |
| 2 Interface IP67 | 2 Interface de sécurité |
| 1 Constituant de contrôle | 1 Alimentation puissance |
| 2 Constituant de dialogue | 2 Maître AS-I |

AS-Interface est caractérisé par un câble jaune (⇒ Fig.30) et une forme particulière, qui permet d'éviter les inversions entre les deux fils. Ce câble auto-cicatrisant utilise une prise vampire qui autorise le raccordement et le déplacement d'un capteur/actionneur sans l'aide d'outil.

AS-Interface est exclusivement un bus de terrain de type maître/esclave qui comprend un "maître" (PC, API, Contrôleur ...) chargé d'assurer la gestion des états des capteurs/actionneurs et de les transmettre à l'automatisme. D'autres atouts sont à mettre à l'actif d'AS-Interface comme une topologie libre, que ce soit en étoile ou en ligne le réseau fonctionne.



↑ Fig. 30 Constituants de l'AS-Interface

Pendant dix ans, AS-Interface ne sut gérer que des capteurs/actionneurs tout ou rien. Certains fournisseurs proposaient des versions analogiques lentes comme la mesure de température ou de niveau, mais à chaque fois les produits étaient propriétaires, et le nombre d'adresses limité à 31 rendait l'utilisation de l'analogique marginale.

Le consortium a lancé une nouvelle version, la V2. Avec elle, le nombre d'adresses double avec un total de 62 esclaves tout ou rien possibles par maître. Mais la grande évolution est sa capacité à recevoir des capteurs/actionneurs de type analogique. Un panachage est possible entre les capteurs analogiques et ToR. Dans ce dernier cas le nombre d'esclaves connectables va diminuer, mais il restera dans le domaine du possible. Avec ce profil analogique, il est possible de relier n'importe quel capteur/actionneur analogique sur n'importe quel maître AS-Interface.

Cette nouvelle version amène aussi des changements au niveau du diagnostic du réseau. Dans la version première, seuls les défauts du réseau étaient détectés. La V2 prend en compte, tous les défauts internes des modules.

Bien entendu, la comptabilité -sur un même réseau- de la V2 et la V1 est assurée.

■ Les avantages d'AS-Interface (⇒ Fig.31)

La simplicité	La simplicité du système de câblage est due à : <ul style="list-style-type: none"> • L'usage d'un câble unique pour raccorder tous les actionneurs et capteurs dans un système d'automatisme. • La gestion des communications intégrée aux produits.
La réduction des coûts	Les coûts peuvent être réduits jusqu'à 40 % par : <ul style="list-style-type: none"> • Réduction des temps de conception, installation, mise en service et évolutions. • Espace gagné dans les enveloppes, grâce à des produits plus compacts et à l'élimination des enveloppes intermédiaires depuis que la majorité des fonctions peuvent être délocalisées sur la machine. • Elimination des canalisations des câbles de contrôle.
La sécurité	AS-Interface permet d'améliorer la fiabilité, la disponibilité opérationnelle et la sécurité : <ul style="list-style-type: none"> • Les erreurs de câblage ne sont plus possibles. • Pas de risque de mauvaise connexion. • Haute immunité aux interférences électromagnétiques (EMC). • Les fonctions de sécurité de la machine peuvent être totalement intégrées dans AS-Interface.

↑ Fig. 31

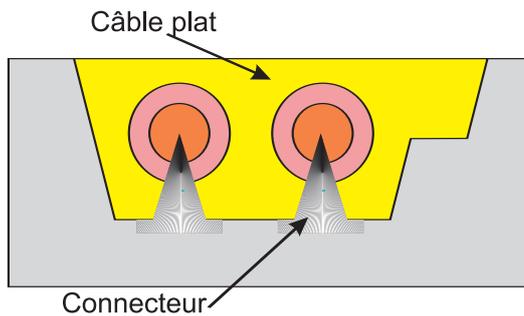
Les avantages de l'AS-Interface

■ Les composants d'AS-Interface

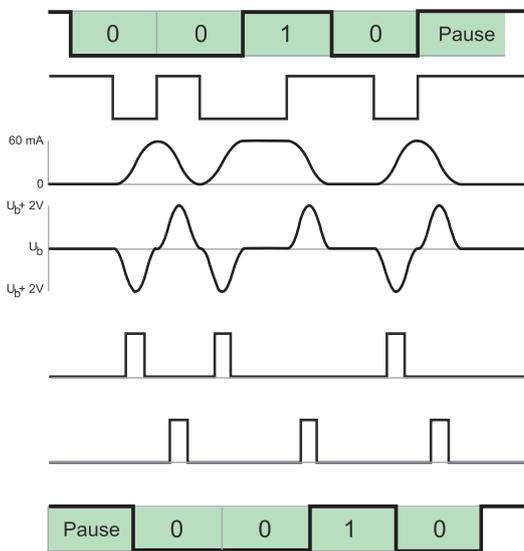
Ils sont regroupés en familles (⇒ Fig.32), nous invitons le lecteur à se reporter aux catalogues de produits de Schneider Electric pour plus d'informations.

Les interfaces pour produits génériques	Ils permettent à n'importe quel produit standard (capteur, actionneur, démarreur, etc.) d'être connecté sur un réseau AS-Interface. Ils permettent une grande liberté dans le choix et sont particulièrement adaptés aux modifications et améliorations des machines qui étaient précédemment réalisées en câblage conventionnel. Ces interfaces sont disponibles pour montage en en enveloppes (IP20) ou en montage direct sur la machine (IP67).
Les interfaces dédiés et composants Le maître	Les interfaces dédiés (modules de communication...) permettent la communication avec le câble AS-Interface. Les composants dédiés intègrent une interface et peuvent donc être connectés directement sur le câble AS-Interface. Ils autorisent un câblage très rapide, mais offre un choix moins large que les composants génériques. C'est le composant central du système, sa fonction est de gérer les échanges de données avec les interfaces et composants (appelés aussi esclaves) répartis dans l'installation. Il peut recevoir : 31 interfaces ou composants en version V1 (temps cycle 5ms) 62 interfaces ou composants en version V2 (temps de cycle 10ms) Le maître est : Soit intégré dans un contrôleur programmable, sous la forme d'une extension par exemple, Soit connecté au bus de terrain, il s'agit alors d'une passerelle.
L'alimentation AS-Interface	C'est une source très basse tension de 29.5 à 31.6V pour les interfaces, et composants alimentés à travers le câble AS-Interface. elle est protégée contre les surtensions et les court-circuits. Seul ce type d'alimentation peut être utilisé sur une ligne AS-Interface. Comme le câble AS-Interface est limité en courant, il est parfois nécessaire d'adjoindre une source supplémentaire pour certains circuits, en particulier pour les actionneurs.
Le câble plat	Le câble jaune, connecté à l'alimentation de puissance, assure les deux fonctions suivantes : - Transmettre les données entre le maître et les esclaves. - Alimenter les capteurs et actionneurs. Le câble noir, connecté à la source auxiliaire 24V fourni la puissance aux actionneurs mais aussi aux capteurs qui possèdent des entrées isolées. Le profile mécanique de ces câbles rend impossible tout inversion de polarité, le matériau utilisé permet une connexion rapide et fiable des différents composants. La déconnexion d'un produit, pour modification de l'équipement par exemple, le câble retrouve sa forme d'origine par auto-cicatrisation Ces câbles supportent 8A maximum et sont disponibles en deux versions : - En caoutchouc pour les applications standards. - En TPE pour les applications ou le câble est soumis aux projections d'huile.
Solutions de sécurité sur AS-Interface (Voir le chapitre 6 dédié à la sécurité)	Les informations standard du processus peuvent être transmises en même temps et sur le même média que les informations relatives à la sécurité jusqu'au niveau 4 du standard EN 60954-1. L'intégration dans AS-Interface se fait par l'adjonction d'un moniteur et de composants de sécurité connectés sur le câble jaune AS-Interface. Les informations de sécurité sont échangées seulement entre le moniteur de sécurité et ses composants, ceci est transparent pour les autres fonctions standards. De ce fait, un système de sécurité peu être ajouté sur une installation AS-i existante.
Le terminal d'adressage	Puisque les composants sont connectés en parallèle sur le bus AS-Interface, il est nécessaire d'assigner une adresse différente à chacun. Cette fonction est assurée par un terminal qui se raccorde individuellement aux différents composants

↑ Fig. 32 Les composants d'Asi-Interface



↑ Fig. 33 Principe du raccordement As-i



↑ Fig. 34 Forme des signaux courant et tension

■ Principe de fonctionnement du réseau AS-i

□ Connectique

Le système de raccordement utilisé est appelé communément « prise vampire ». Le connecteur comporte deux aiguilles qui effectuent la liaison électrique par percement de l'isolant du câble. Les deux parties du connecteur sont ensuite visées l'une sur l'autre pour assurer la qualité de la connexion. Ce système de connecteur (⇒ principe figure 33) est normalisé et permet de réaliser facilement tout type d'équipement jusqu'à des niveaux de protection IP67.

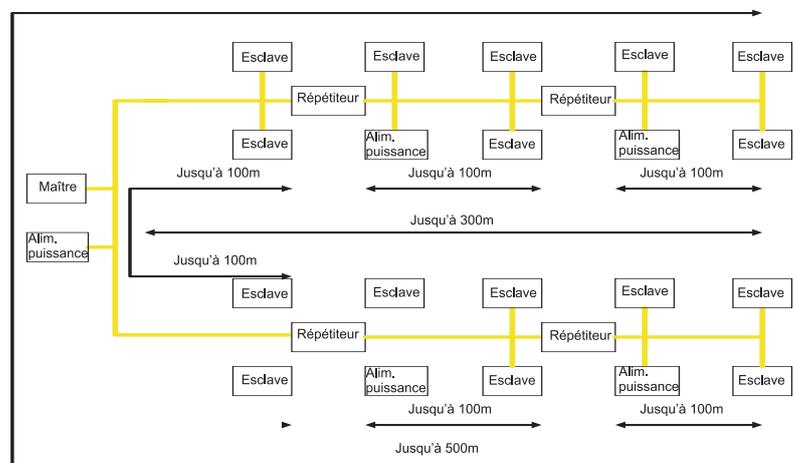
□ Modulation des signaux

De part sa conception le réseau As-i fonctionne sans adjonction de bouchon de terminaison et ce quelque soit la topologie utilisée. Le principe utilise la modulation du courant basée sur un encodage Manchester, deux inductances situées dans l'alimentation convertissent ce signal en tension sinusoïdale. La forme du signal généré évite de blinder le câble (⇒ Fig.34).

□ Longueur du réseau

La longueur du réseau est conditionnée par la déformation du signal et par la chute de tension en ligne. La distance maximale entre deux esclaves ne doit pas dépasser 100m (⇒ Fig.35). Cette distance peut être augmentée par l'adjonction de répéteurs avec les limites suivantes :

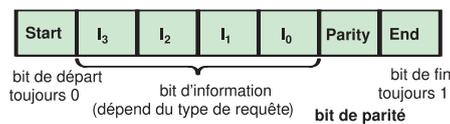
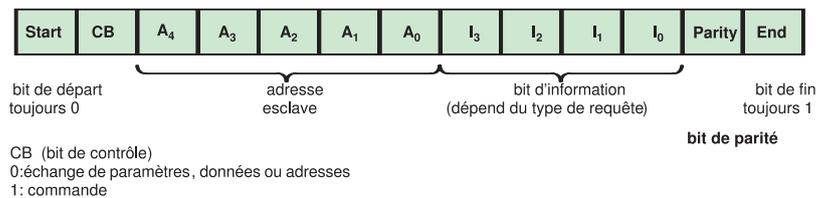
- deux répéteurs au maximum par ligne,
- la distance maximale avec le maître ne doit pas dépasser 300m,
- l'utilisation d'une terminaison passive permet d'étendre la distance de 100m à 200m,
- une terminaison active permet d'atteindre 300m.



↑ Fig. 35 Longueurs limites du réseau As-i

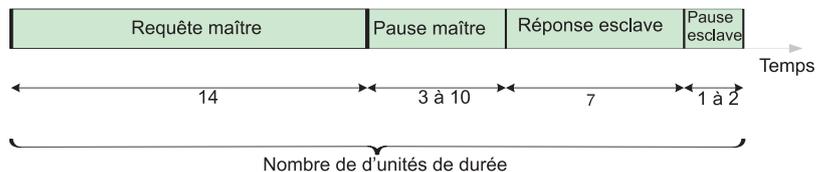
□ Principe du protocole

Le principe de communication est basé sur un protocole à un seul maître. Le maître système interroge les esclaves à tour de rôle, ceux-ci répondent en envoyant les données requises (⇒ Fig.36). Quand tous les esclaves ont été interrogés, le cycle se répète et continue indéfiniment. Le temps de cycle dépend du nombre d'esclaves du système et se détermine facilement.



↑ Fig. 36 Trames maître et esclave

AS-I utilise plusieurs méthodes pour garantir la sûreté du transfert de données. Le signal est vérifié par le récepteur, s'il n'a pas la forme requise il n'est pas pris en compte. L'utilisation d'un bit de parité associé à un message court (7 et 14 bits) assure l'intégrité logique de l'information. Le temps mort du maître provoque l'acquiescement (⇒ fig.37).



↑ Fig. 37 Constitution du temps de réponse

La durée d'un bit est de 6 µs. A la vitesse de 166.67 Kbits/s -en ajoutant l'ensemble des bits de pause- le temps de cycle maximum ne dépassera pas 5082 µs.

- Chaque cycle se décompose en trois parties
 - échange de données,
 - gestion du système,
 - mise à jour/insertion d'un esclave.

Le profil AS-Interface du maître détermine ses capacités exactes. En général, il possède les fonctions suivantes :

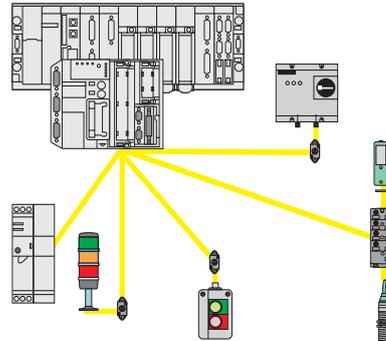
- initialiser le système,
- identifier les esclaves connectés,
- transmettre les paramètres esclaves aux esclaves,
- assurer l'intégrité des échanges de données cycliques avec les esclaves,
- gérer les diagnostics du système (état de fonctionnement des esclaves, contrôle du bloc d'alimentation, etc.),
- communiquer toutes les erreurs détectées au contrôleur du système (automate, etc.),
- reconfigurer les adresses des esclaves si le système subit une quelconque modification.

Les esclaves décodent les demandes provenant du maître et leur répondent immédiatement. Toutefois, un esclave ne répondra pas à des commandes erronées ou inappropriées venant du maître. Les capacités fonctionnelles d'un esclave sont définies par son profil AS-Interface.

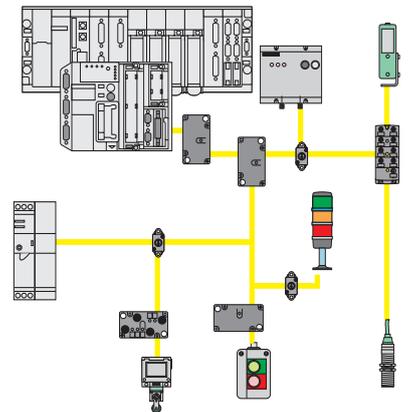
■ Topologie et câblage d'AS-Interface

L'absence de restrictions permet toute sorte de configurations du système et de liaisons entre les capteurs et actionneurs, en voici quelques illustrations (⇒ fig.38).

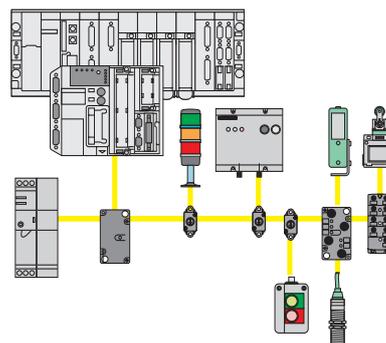
Point à point



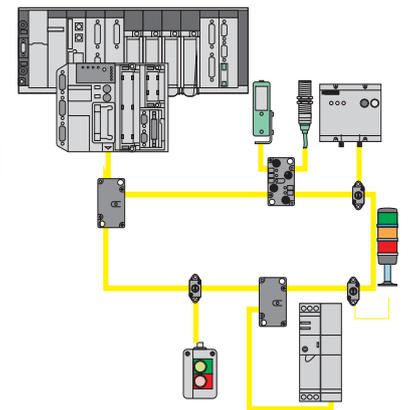
En arbre



En ligne



En anneau



↑ Fig. 38 Types de réseaux possibles

■ Les versions d'AS-Interface

La première version (V1) a été suivie d'une nouvelle évolution V2.1 qui intègre les améliorations suivantes :

- possibilité de connecter un maximum de 62 esclaves, la V1 n'en acceptant que 31,
- possibilité de transmettre un message "défaut périphérique" au maître sans inhiber l'esclave qui conserve sa possibilité de fonctionner lorsque la continuité de service est critique,
- prise en compte des esclaves analogiques.

■ Profil

Le profil d'un équipement AS-Interface détermine ses capacités. Deux produits AS-Interface ayant les mêmes fonctions et le même profil fonctionnent exactement de la même manière, quels que soient les fabricants. Ils sont interchangeables à l'intérieur d'un même système. Le profil est fixé en usine au moyen de deux ou trois caractères figés dans l'électronique interne de l'équipement. Il ne peut pas être modifié. Jusqu'à présent, plus de 20 profils ont été définis par l'association AS-i. Ils sont décrits dans la suite de ce sous-chapitre.

Le tableau 39 donne les compatibilités entre les différentes versions

	Esclave V1	Esclave V2.1 avec adressage standard	Esclave V2.1 avec adressage étendu	Esclave analogique
Maitre V1	Compatible	Compatible mais les défauts de périphérique ne sont pas signalés	Non compatible	Non compatible
Maitre V2	Compatible	Compatible	Compatible	Compatible

↑ Fig. 39 Les versions d'As-Interface : les compatibilités

□ Profils du maître

Les profils du maître définissent les capacités individuelles de chaque type de maître AS-Interface. Il existe quatre types de profils du maître : M1, M2, M3, M4, cette dernière est compatible avec les versions précédentes.

□ Profils d'esclave

Tous les esclaves disposent d'un profil, ce qui signifie qu'ils sont considérés comme des périphériques "asifiés" comportant un circuit ASIC. Font partie de cette catégorie les composants dédiés (tels que les actionneurs intelligents) et les interfaces (qui connectent des composants traditionnels au système AS-Interface). Les profils, semblables à des cartes d'identité, ont été définis afin de distinguer les actionneurs et les capteurs en les répartissant dans de grandes familles. Le système des profils est particulièrement utile lorsqu'il s'agit de remplacer un esclave. Par exemple, deux actionneurs fabriqués par différents constructeurs mais ayant le même profil sont fonctionnellement interchangeables sans programmation ni adressage.

9.11 Conclusion

L'emploi de réseaux de communication dans les architectures d'automatisme industriel permet d'augmenter leur flexibilité et donc de répondre aux besoins d'adaptation des machines et des installations. Se faisant, ils obligent à des choix qui nécessitent des connaissances particulières afin d'effectuer les bonnes sélections parmi la multitude de réseaux de communication existants. Des critères simples sont applicables : ouverture, standardisation et adéquation :

- Choisir un réseau ouvert, par opposition à un réseau propriétaire, permet de rester libre du choix de ses fournisseurs de produits d'automatisme.
- Choisir un réseau standardisé au niveau international permet de garantir sa pérennité et son évolution.
- Choisir la bonne adéquation entre le besoin de la machine ou de l'installation et les performances du réseau permet d'optimiser son investissement.

Ce dernier point est celui qui, vraisemblablement, nécessite une connaissance précise de l'offre des réseaux de communication qui longtemps ont été perçus comme complexe, tant pour les sélectionner, que pour les mettre en œuvre ou les maintenir. Les fournisseurs ont tous travaillé à pallier cette difficulté. Schneider Electric a pour sa part décidé de ne proposer que des réseaux de communication réellement ouverts, basés sur des standards internationaux et adaptés aux besoins des différents niveaux d'une architecture d'automatisme en définissant des classes d'implémentation qui permettent un choix simple et optimal.