iutenligne

Le catalogue de ressources pédagogiques
de l'enseignement technologique universitaire.

I.U.T. de Mulhouse – G.E.I.I.

RES3 - Réseaux

CM 7 – TD6 :
Réseaux et bus de terrain

IUT Institut Universitaire de Technologie de Mulhouse

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- *CM 6 : Réseaux WLAN et sécurité*
  - *TD 5 : Réseaux Wifi et sécurité*
- **CM 7 : Réseaux et bus de terrain**
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

Jean-François ROTH
Enseignant Vacataire IUT de Mulhouse
Formateur/Consultant en réseaux et télécoms depuis 1999
Jean-Francois.ROTH@UHA.fr
JeanFrancoisROTH@MSN.com

Sommaire

- Réseaux et bus de terrain
  - Introduction
  - Normalisation
  - Classification
  - Evolution
  - Fonctionnement
  - Cas pratique : Control Area Network (CAN)
  - Cas pratique : ModBus
  - Cas pratique : Ethernet
  - Questionnement préalable

- Réseaux et bus de terrain
  - Terrain
    - Indique une couverture limitée ou délimitée géographiquement (usine, atelier, voiture...)
  - Bus
    - Au sens informatique industrielle, conducteur ou ensemble de conducteurs, communs à plusieurs circuits permettant l'échange de données entre eux
      - Liaisons communes
      - Plusieurs circuits
      - Référence à la topologie de la configuration
  - Réseau
    - Ensemble de lignes de communication qui desservent une même unité géographique
      - Peut être composé d'un seul bus
      - Caractérisé par une topologie.
      - Permet une gestion répartie : diagnostic, maintenance...
  - Un bus de terrain est un système de communication entre plusieurs ensembles communiquant
    - Capteurs, microcontrôleurs, actionneurs, mémoires...

Introduction

- Réseaux et bus de terrain
  - But initial
    - Remplacement des boucles analogiques de courant 4 - 20 mA
      - Moyen de transmission permettant de transmettre un signal analogique sur une grande distance sans perte ou modification notable de ce signal
  - Objectifs
    - Améliorer la qualité
    - Améliorer la fiabilité du système de transmission
    - Améliorer l'efficacité
      - Précision, formalisation des échanges entre équipements, …
    - Réduire les coûts d'installation et de maintenance
      - Réutilisation possible du câblage existant, moins de câblage, …
    - Permettre un contrôle décentralisé du système
      - Décentralisation du contrôle, du traitement des alarmes, diagnostics aux différents équipements de terrain
      - Intelligence déportée au niveau de ces équipements
    - Interopérabilité
      - Système ouvert

Introduction

- Réseaux et bus de terrain
  - Avantages
    - Réduction des coûts initiaux
      - Réduction massive du câblage en utilisant, en général, un seul câble pour tous les équipements
      - Possibilité de réutiliser le câblage analogique existant dans certains cas
      - Réduction du temps d'installation
      - Réduction du matériel nécessaire à l'installation
    - Réduction des coûts de maintenance
      - Complexité moindre donc moins de maintenance (fiabilité accrue)
      - Maintenance plus aisée
      - Temps de dépannage réduit, localisation des pannes possibles grâce à des diagnostics en ligne à distance
      - Outils de test dédiés (analyseur...)
      - Flexibilité pour l'extension du bus de terrain et pour les nouveaux raccordements
    - Performances globales accrues
      - Les données numériques sont transférées sans erreur de distorsion, de réflexion...
      - Les données et mesures sont généralement disponibles à tous les équipements de terrain
      - Communications possibles entre deux équipements sans passer par le système de supervision
      - Structure distribuée permettant d'avoir des algorithmes de contrôle sur chaque équipement de terrain (noeud)
      - Accès à des variables multiples pour un noeud

- Réseaux et bus de terrain
  - Avantages
    - Interopérabilité grâce à la standardisation aux niveaux matériel et logiciel (système ouvert)
      - Choix pour l'utilisateur final : prix, performances, qualité...
      - Standard profitant à l'utilisateur et non au vendeur
      - Possibilité de connexion d'équipements de différents fournisseurs respectant le même standard
      - Echange de données par des mécanismes standards (protocoles)
    - Modélisation objet des équipements et de leur fonctionnalité
      - Modèle de bloc fonctionnel aidant l'utilisateur à créer et superviser le ou les bus de terrain
  - Inconvénients
    - Connaissances supérieures nécessaires
      - Accès au bus : conflit, arbitrage, temps de latence...
      - Sécurité des informations transportées : gestion des erreurs
      - Topologie, longueur, débit
      - Supports physiques
    - Investissement en équipements et accessoires (monitoring, maintenance)
      - Coûts apparemment supérieurs
      - Choix entre solutions propriétaires et standards
    - Interrogation sur la compatibilité totale entre équipements de fournisseurs différents

- Réseaux et bus de terrain
  - Normalisation des bus de terrain
    - Un chemin long et difficile…
      - Années 1940 : Process de contrôle de capteurs de pression (USA)
      - Années 1960 : Apparition du standard boucle analogique 4-20 mA
      - Années 1970 : Boom des processeurs, contrôle centralisé
      - Années 1980 : Contrôle distribué, capteurs intelligents, réseau de terrain, début de la normalisation
      - 1994 : Fusion de WorldFIP (World Factory Information Protocol - Europe) et ISP (Interoperable System Project - USA) pour donner la Fieldbus Foundation (FF)
        - Couche physique : septembre 1992
        - Couches liaison, application,... : prévues fin 1998 mais jamais abouties ...
    - Constat
      - Plus d'une dizaine d'années de normalisation
        - Un standard de télécommunication met 3 ans pour être disponible
      - L'idée de base était d'avoir un standard avant la sortie de produits commerciaux
      - Lobbying actif de groupes d'intérêt entrainant l'échec de la normalisation niveau liaison fin 1998
      - Ralentissement de l'émergence d'un standard international de bus de terrain
      - L'absence d'un standard a entraîné l'apparition de solutions propriétaires devenues standards de fait
        - En raison d'une trop longue attente…

- Réseaux et bus de terrain
  - Distinction de deux types de bus/réseaux de terrains
    - Standards de fait
      - Interbus-S
      - ASI ou AS-i (Actuators Sensors Interface)
      - Lonworks (capteur/actionneur)
    - Standards internationaux
      - WorldFIP (France, Italie) - NFC 46-600
        - Honeywell, Cegelec, Télémécanique, EDF...
      - PROFIBUS (PROcess Field BUS, Allemagne) - DIN 19245
        - Siemens, Fisher Controls (USA)...
  - Cohabitation entre des standards de fait et des standards internationaux
    - Analogie avec Internet et les protocoles réseaux
    - Assainissement de l'offre bus de terrain
      - Uniquement les produits reconnus par tous devraient subsister
    - Homogénéisation de l'offre
      - OSI est le modèle de référence
    - Difficulté pour l'utilisateur final de s'y retrouver et de faire le bon choix
      - Questionnement sur l’assurance de pérennité assurée

Classification

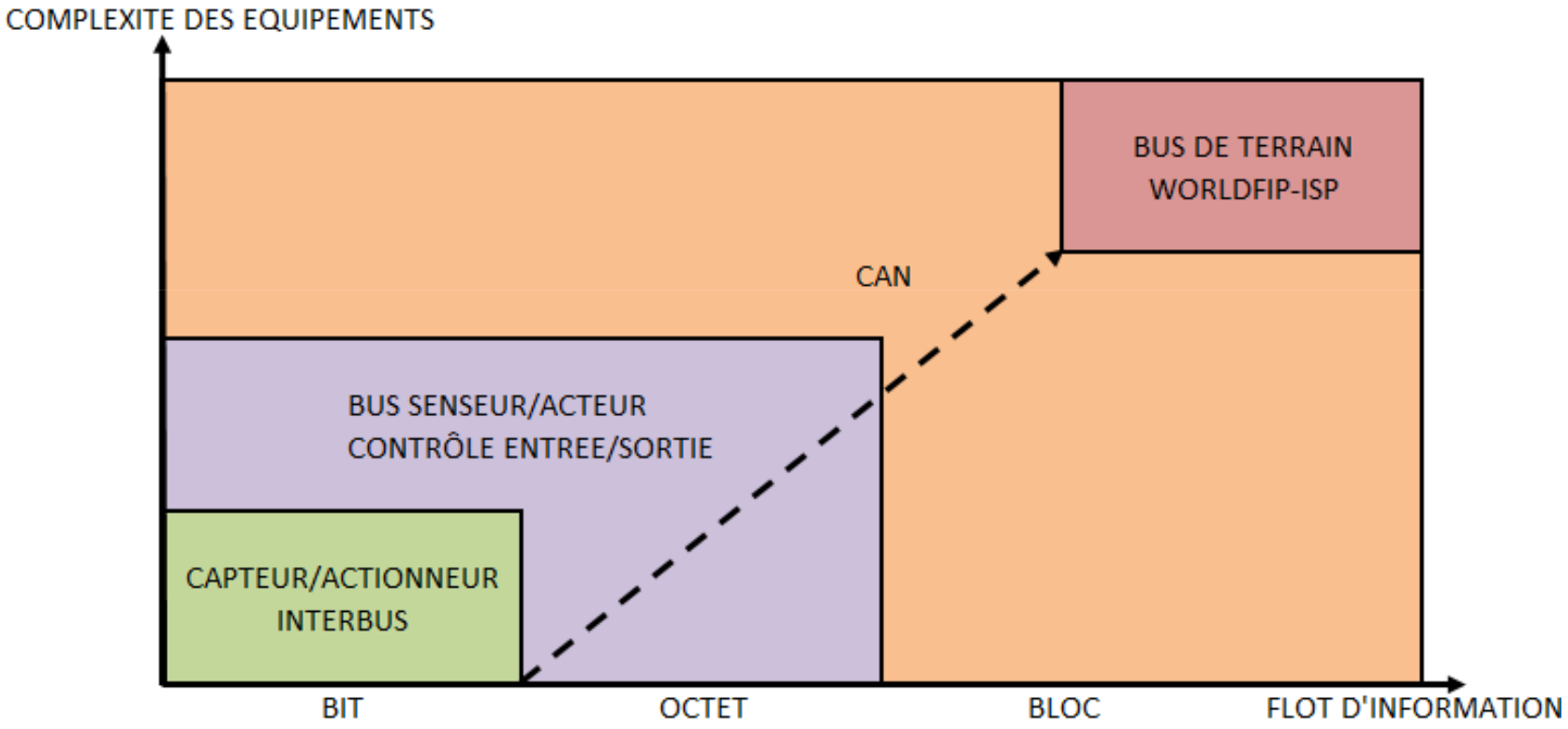
- Réseaux et bus de terrain
  - Regroupement de tous les bus de communication industriels sous le terme "bus de terrain"
    - Distinction par complexité décroissante
      - Bus d'usine : réseau local industriel basé sur EtherNet de type MAP ou TOP
        - Se rapproche du réseau local IP
        - MAP : Manufactoring Automation Protocol
        - TOP : Technical and Office Protocol
        - IP : Internet Protocol
      - Bus de terrain ("Field Bus")
      - Bus de bas niveau ("Sensor Aktor Bus") : bus capteur/actionneur
    - FieldBus
      - Bus orientés procédés continus basse vitesse
      - Bus de synchronisation entre unités de traitement, le plus souvent des automates ou des Système Numérique de Contrôle-Commande (SNCC)
      - Permet l'envoi de trames de quelques dizaines d'octets à 256 octets
      - Temps de réaction de quelques millisecondes à quelques dizaines de millisecondes
      - Relie des unités intelligentes qui coopèrent dans l'exécution de travaux (coopération de tous les noeuds)
      - Communications Maître/Esclave ou Multimaître
      - Possibilité d'accès au niveau inférieur (capteur/actionneur)
        - Exemples : Profibus FMS, Prifibus PA, FieldBus WorldFIP, Modbus +…

Classification

- Réseaux et bus de terrain
  - Regroupement de tous les bus de communication industriels sous le terme "bus de terrain"
    - SensorBus
      - Bus de capteurs et d'actionneurs
      - Bus aux temps de réponse très courts
      - Relie entre eux des noeuds à intelligence limitée ou nulle
      - Requiert le plus souvent des actions réflexes au plus près des actionneurs
      - Nécessité d'informer dans des délais courts les niveaux supérieurs
      - Limitation du nombre de données à faire circuler sur le bus (trame unique, fixe, cyclique)
        - Exemples : AS-i, Bitbus, Seriplex…
    - DeviceBus
      - Bus de périphérie d'automatismes
      - Concept assez récent et précisant un domaine précédemment couvert par le concept de FielBus
      - Les DevicesBus sont plus orientés manufacturiers haute vitesse et déterminisme
        - Exemples : DeviceNet, DeviceWorldFIP, SDS, Interbus, Profibus DP…
    - DataBus
      - Bus informatique
      - Permet le transfert et la configuration de fichiers
      - Réseaux informatiques plutôt que réseaux d'automatismes dans la plupart des cas
        - Exemples : MMS sur Ethernet (Manufacturing Message Specification), FDDI (Fiber Distributed Interface), MAP (Manufacturing Automation Protocol), …

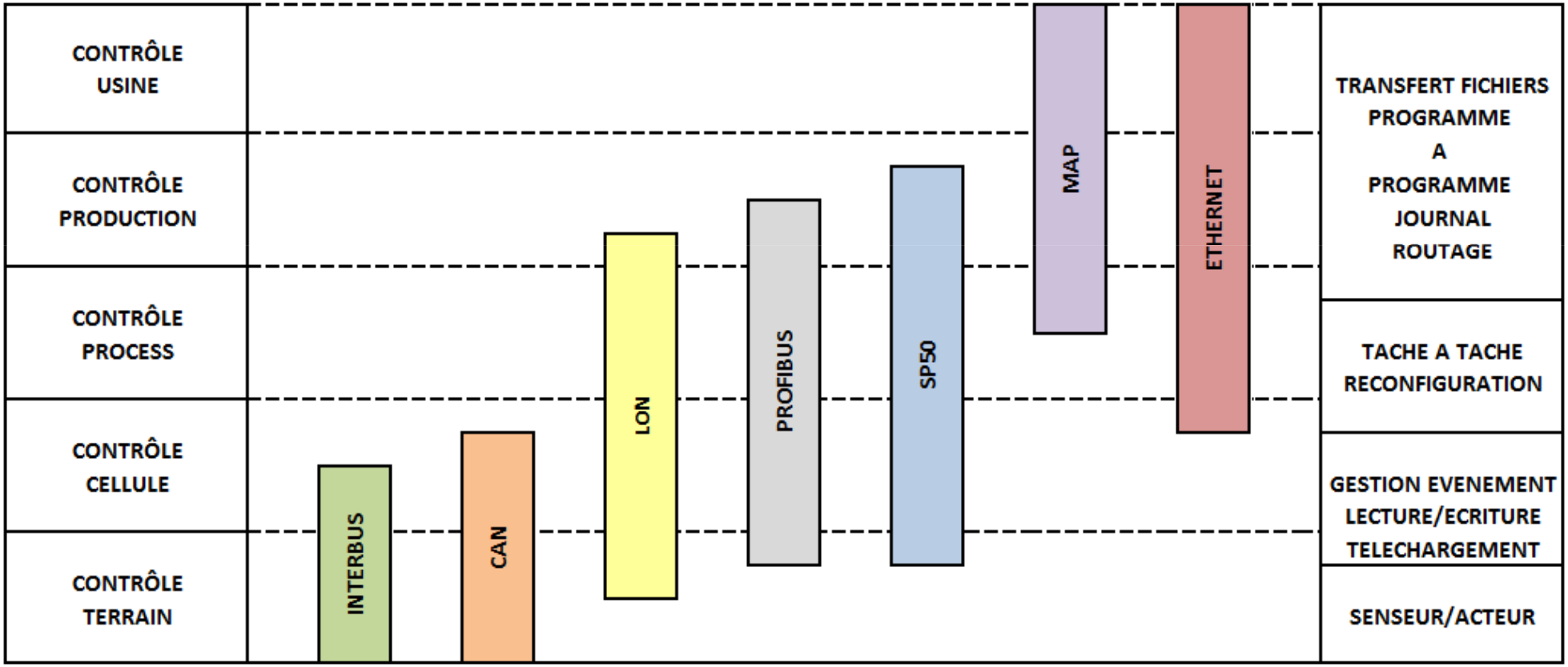
Classification

- Réseaux et bus de terrain
  - Classification des bus de terrain



Classification

- Réseaux et bus de terrain
  - Pyramide Computer Integrated Manufacturing (CIM) appliquée aux réseaux de terrain



- Réseaux et bus de terrain
  - Décollage spectaculaire du nombre de bus
    - Réseaux de terrain en France, Allemagne, Italie, GB
      - 1995 : 100000 bus / réseaux
      - 2000 : multiplié par 7 avec une augmentation de plus de 100000 par an
  - Catégories concernées
    - Consommateurs travaillant sur une installation utilisant un bus de terrain
    - Intégrateurs de systèmes utilisant un bus de terrain
    - Producteurs et fournisseurs fournissant des équipements se connectant sur un bus de terrain

- Réseaux et bus de terrain
  - Un bus de terrain est basé sur la restriction du modèle OSI à 3 couches
    - Couche physique
    - Couche liaison de données
    - Couche application
    - Modélisation respectée aussi bien par les standards de fait que les standards internationaux

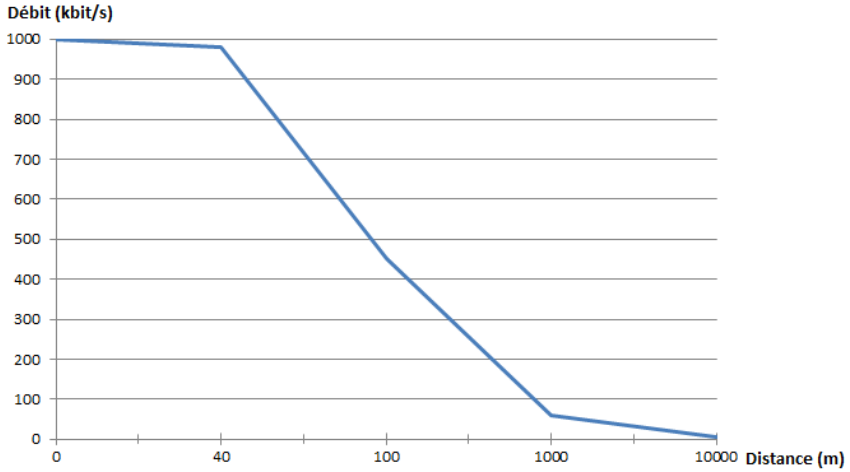
- Standard ISA/SP50
  - Standard de fait
    - Partie applicative (fonction d'automatisme réalisée par le système) normalisée
      - Utilisation des concepts de la programmation objet
    - Couches 3 à 6 vides
      - Pas de besoin d'interconnexion avec un autre réseau
      - Gain en performance
    - Implémentation d'une couche utilisateur
      - Gestion d'une stratégie de contrôle global distribué, modélisée sous forme de blocs fonctionnels ("function block")
    - Mise en place d'une base de données répartie distribuée sur le réseau pour le contrôle et l'acquisition
    - Bloc supervision ("system and network management")
      - Configuration, monitoring, contrôle des ressources du réseau

- Control Area Network (CAN)
  - Standard de fait développé par Robert Bosh GmbH et Intel (1985) respectant les niveaux 1 et 2 du modèle OSI
    - Le niveau application a été défini par ailleurs
  - Appartient à la catégorie des bus de terrain et en est un produit reconnu
    - Norme ISO 11898 (applications haut débit)
    - Norme ISO 11519 (applications faible débit)
  - Initialement développé pour l'industrie automobile
    - Egalement utilisé de nos jours pour l'automatisme et les applications de contrôle
  - Possède des composants de différents fabricants
    - Hitachi, Motorola (68HC12), NS, NEC, Philips (87C592, 82C250), Siemens , Thomson, Toshiba
    - Utilisation de circuits bon marché
  - Essor important début des années 2000
    - 11 millions de noeuds en 1996 et 149 millions en 2001

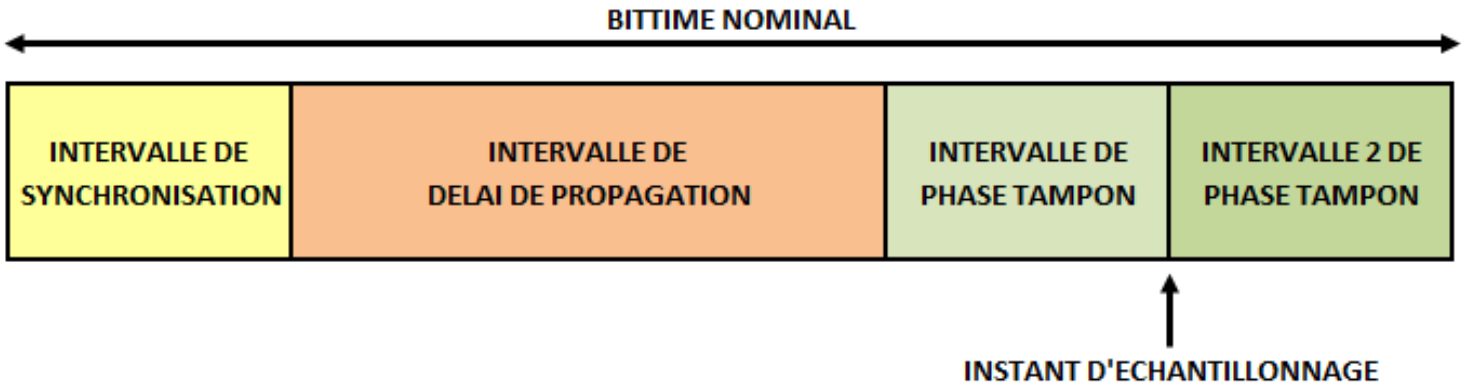
- Control Area Network (CAN)
  - Cas particulier de l'automobile
    - Depuis 2005 une voiture standard comporte une centaine de microcontrôleurs
    - Nécessité de remplacer l'équivalent de 2km de câblage (soit 100 kg de cuivre) d'une voiture
      - Intégration d'un bus série simplement grandement l'intégration des fils dans le châssis
    - En pratique, 3 bus CAN, à débits différents, cohabitent dans une voiture :
      - Un bus ultra rapide pour gérer la sécurité
        - Freinage, ABS, détection de chocs, airbags, …
      - Un bus à moyenne vitesse pour gérer le moteur
        - Commandes et capteurs
      - Un bus lent pour gérer les accessoires
        - Lampes, boutons, moteurs d'asservissements, ….

- Control Area Network (CAN)
  - Description
    - Toutes les stations (organes de commande, capteurs ou actionneurs) ont des droits identiques et sont reliés par un bus série
      - Permet l'échange de 2048 variables
      - Détection des erreurs de transmission induites par les radiations électromagnétiques
      - Permet à chaque station de communiquer sans surcharger les calculateurs des organes de commande
  - Circuits disponibles
    - Circuit "Basic CAN"
      - Lien intime entre le protocole CAN et le microcontrôleur : comportement de type UART
      - Le micro est interrompu à chaque message émis sur le bus par un autre nœud
      - Charge CPU importante
    - Circuit "Full CAN"
      - Filtrage des messages (suivant leur identificateur)
      - Permet de réduire la charge CPU et de ne pas interrompre le microcontrôleur
      - Notion de "buffering"

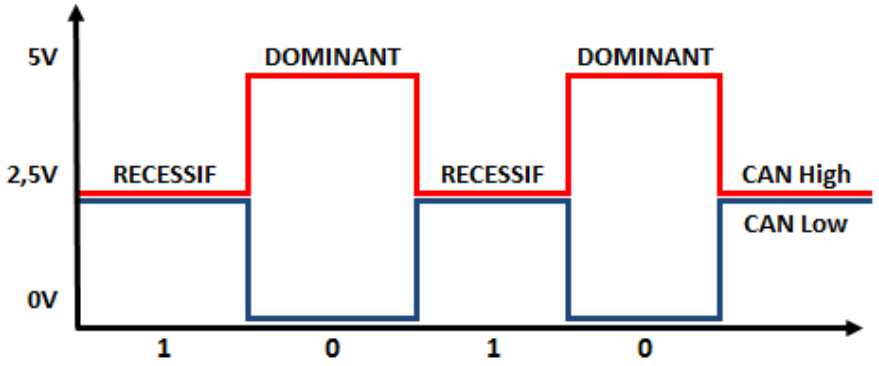
- Control Area Network (CAN)
  - Couche physique
    - Support (média) de transmission : une paire torsadée blindée ou non
    - Codage NRZ binaire avec utilisation de la technique du "bit-stuffing" (ou bit de transparence)
      - Un bit de valeur complémentaire inséré à l'émission et supprimé à réception de 5 bits consécutifs de même valeur
    - Signaux émis en différentiel sur la paire
    - Nombre max de nœuds :
      - Théoriquement lié à la taille du champ d'identification en pratique inférieur à 120 (suivant le circuit utilisé)
    - Débit brut : de 5 kb/s à 1 Mb/s suivant la longueur du réseau
    - Topologie : bus
    - Standard 11519 pour un faible débit (< 125 kbit/s)
    - Standard 11898 pour un haut débit (utilisation de connecteur SUB-D 9 points)



- Control Area Network (CAN)
  - Couche physique : synchronisation par technique du "bit-timing"
    - Méthode sophistiquée de synchronisation de bits optimisant la bande passante
    - La transmission d'un signal d'un émetteur à un récepteur avec retour à l'émetteur (un trajet aller/retour) doit être achevée en un seul bit-timing
    - Des intervalles de phase tampon sont insérés avant et après l'échantillonnage pour permettre une réception correcte

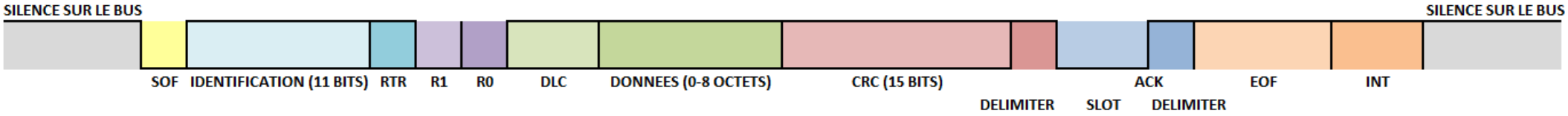


- Control Area Network (CAN)
  - Couche physique : gestion des priorités
    - Les informations échangées peuvent évoluer plus ou moins rapidement
      - Pour un moteur, l'état d'un capteur de position de pédale d'accélérateur doit être transmis plus souvent et rapidement que la température dont l'évolution est plus lente
    - Technique de transmission des bits avec mode dominant et récessif
      - Les informations sont véhiculées sur deux lignes symétriques autour d'une référence à 2.5 V
        - CAN High
        - CAN Low
      - En cas d'émission simultanée, une station en état récessif détectant un état dominant arrête d'émettre jusqu'à la libération du bus
      - Les niveaux récessifs/dominants sont lus sur CAN Low
      - Câblage suivant le principe du "ET câblé" pour l'émission :
        - Si un seul nœud transmet un bit dominant, l'état du bus est dominant
        - Si tous les nœuds transmettent un état récessif, l'état du bus est récessif

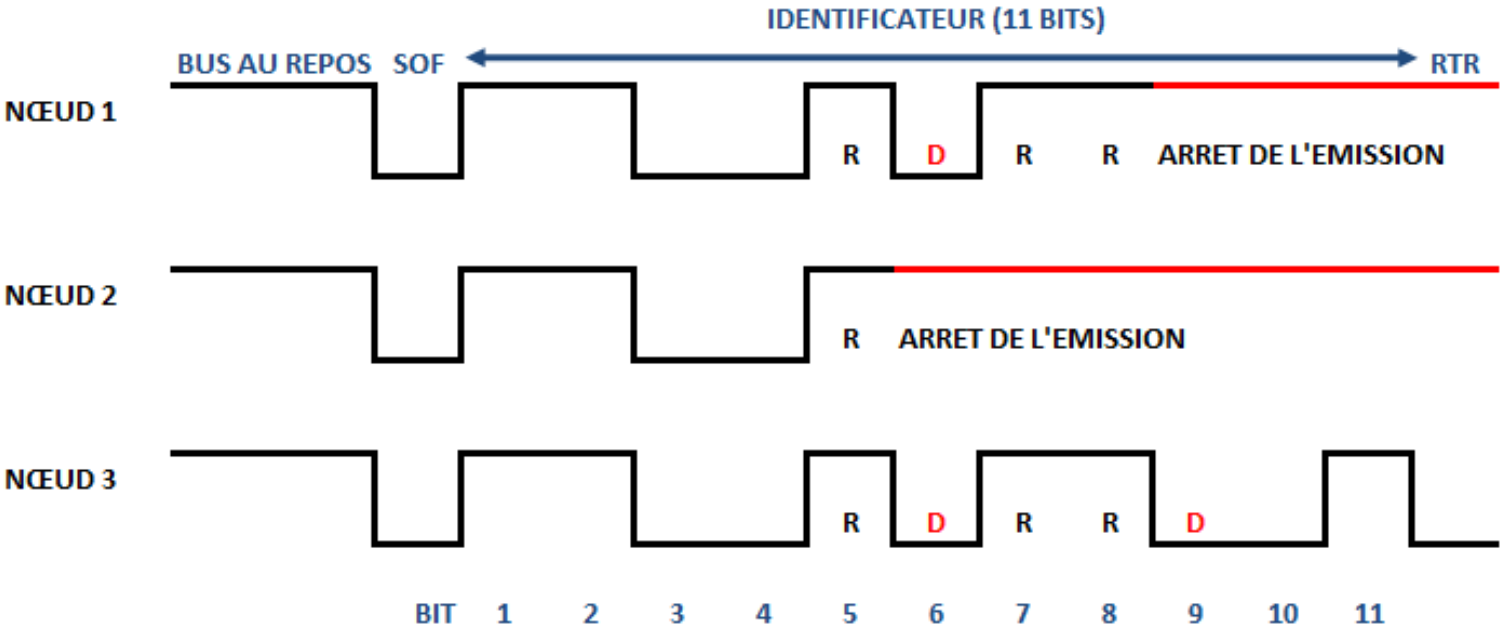


- Control Area Network (CAN)
  - Couche liaison
    - Communications multi-maîtres
      - Tout équipement connecté au bus peut en prendre le contrôle et transmettre un message dès que celui-ci est libre
    - Arbitrage de type CSMA/CA
      - Arbitrage sur le champ d'identificateur de la trame (message)
        - Bit dominant : 0
        - Bit récessif : 1
      - Les stations émettant simultanément sur le bus comparent bit à bit l'identificateur de leurs messages respectifs
        - Dès qu'une station émettrice se trouve en l'état récessif (bit à 1) et détecte une état dominant (bit à 0), elle arrête d'émettre
    - L'identificateur (en-tête) de la trame indique la priorité
      - Un identificateur faible indique une priorité forte
      - La trame de plus forte priorité est toujours transmise
      - Le temps de latence dépend de la charge du bus
        - Priorité la plus forte = 137 * bittime pour CAN 2.0A
    - Standards de trames
      - "Standard CAN" 2.0A: ID sur 11 bits (2032 nœuds en théorie)
      - "Extended CAN" 2.0B : ID sur 29 bits (536870912 nœuds en théorie)

- Control Area Network (CAN)
  - Format de la trame "Standard CAN"
    - SOF (Start Of Frame) : indique le début de la trame
    - Identification (codé sur 11 bits) : réalise l'arbitrage
    - RTR (Remote Transmit Request) : permet le distinction entre
      - Une data frame : trame de données
      - Une remote frame : traite une demande de données par un nœud
      - Une error frame : trame d'erreur
    - R0 et R1 : bit dominants réservés
    - DLC (Data Length Code) sur 4 bits : taille des données de 0 à 8 octets
    - CRC (Cyclical Redundancy Check) : Code de redondance cyclique CRC15
    - ACK (Acknowledge) sur 2 bits dont 1 récessif : acquittement de la trame
    - EOF (End Of Frame) sur 7 bits récessifs : indique la fin de la trame
    - INT : 3 bits récessifs après le champ End Of Frame



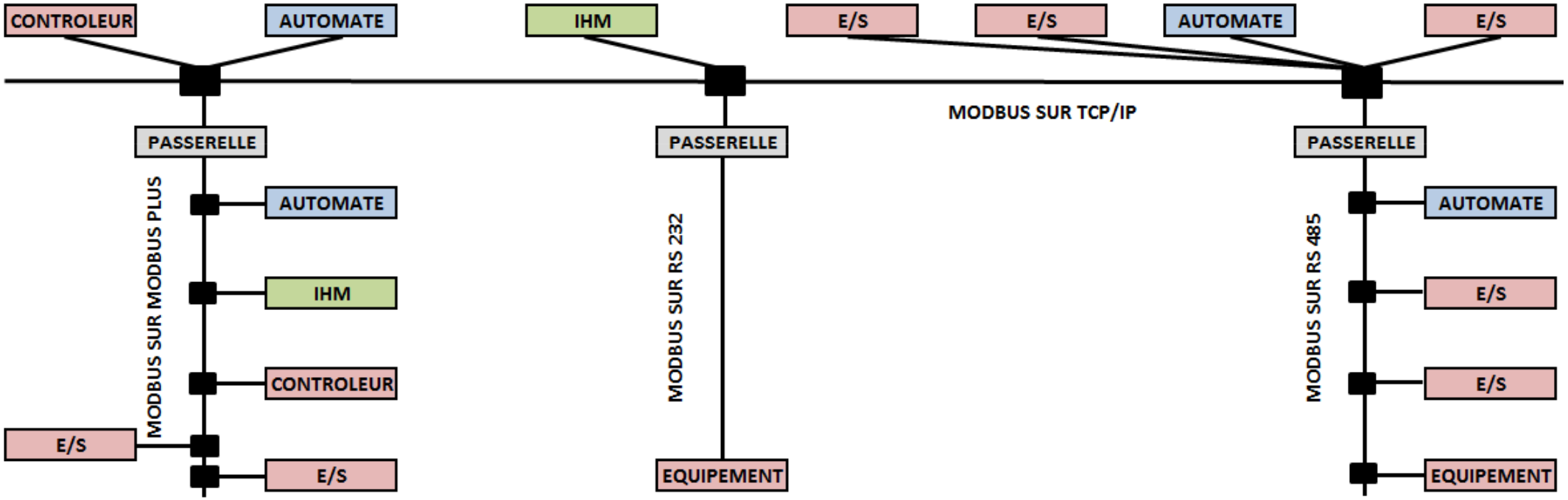
- Control Area Network (CAN)
  - Arbitrage sur le champ d'identificateur de la trame (message)
    - Les nœuds 1, 2 et 3 émettent sur le même bus
      - Au 6ème bit de l'identificateur, le nœud 2 arrête d'émettre car il a un bit récessif alors que les nœuds 1 et 3 ont un bit dominant
      - Au 9ème bit de l'identificateur, le nœud 1 arrête d'émettre car il a un bit récessif alors que le nœud 3 a un bit dominant
      - Le nœud 3 émet sur le bus



- Control Area Network (CAN)
  - Couche application
    - Pas explicitement définie dans le standard CAN
    - Différents types de couches applicatives pour CAN
      - CANopen
      - DeviceNet
      - SAE J1939
      - ISO11783 (ISOBUS)
      - NMEA2000
      - CANaerospace
      - MilCAN
      - SocketCAN
      - FlexCAN
      - CAL
      - SDS
      - CAN Kingdom

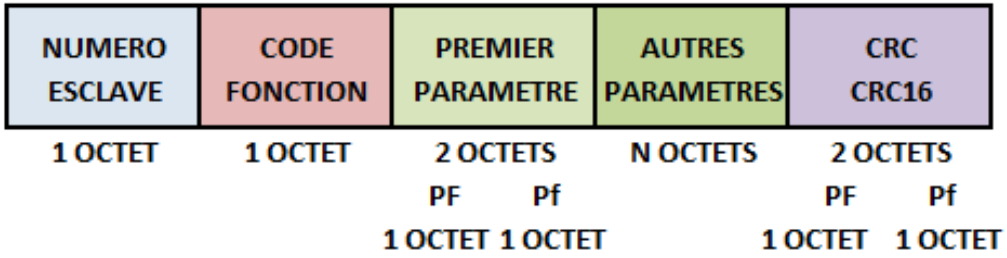
- ModBus
  - Réseau de communication série asynchrone
    - Réseau local industriel développé par la société MODICON en 1978 pour interconnecter des Automates Programmables Industriels (API)
    - Standard industriel de fait
  - Repose sur un protocole d'échange des messages au niveau de la couche 7 du modèle OSI (Application)
    - Procure un service de messagerie Client/Serveur entre divers équipements réseaux
    - Protocole de type "requête/réponse" offrant une multitude de fonctions spécifiées par des codes fonctions
  - Formes d'implémentation
    - Transmissions série asynchrone sur une large gamme de supports physiques
      - RS 232E, RS 422, RS 485, fibre optique, ondes radios, …
      - Réseau à passage de jetons à grande vitesse (ModBus plus)
      - Ethernet (ModBus TCP)

- ModBus
  - Permet de réaliser aisément des communications au sein de différents types d'architectures de réseaux
    - Exemple d'architecture



- ModBus
  - Protocole Maître/Esclave
    - Permet à un seul et unique Maître de demander des réponses à des Esclaves ou d'agir en fonction d'une requête
      - Le Maître peut s'adresser aux Esclaves individuellement ou à tous les Esclaves en même temps (broadcast)
      - Les Esclaves renvoie un message en réponse aux requêtes qui leur sont adressées individuellement
      - Une requête envoyée en broadcast n'entraîne généralement pas de réponse en retour
      - Un réseau RS485 peut contenir jusqu'à 32 nœuds
        - 1 Maître et jusqu'à 31 Esclaves
    - Modes de fonctionnement
      - Remote Terminal Unit (RTU)
      - American Standard Code for Information Interchange (ASCII)
        - Quasiment plus utilisé
    - Fonctionnement en mode Remote Terminal Unit (RTU)
      - Liaison asynchrone constituée de 8 bits (contre 7 bits en mode ASCII)
      - Début de trame détectée par un silence d'au moins 3 caractères
      - Contrôle d'intégrité de la trame réalisé par un checksum (CRC16)

- ModBus
  - Requête en mode Remote Terminal Unit (RTU)
    - Numéro d'Esclave
      - Identifie l'Esclave concerné par la trame
        - Variable de 1 à 247
    - Code fonction
      - Identifie le rôle et la finalité de la trame
        - Variable de 01 à 19
    - Premier paramètre
      - Adresse du bit ou mot adressé
        - Composé de son octet de poids fort (PF) et son octet de poids faible (Pf)
    - Autres paramètres (ou données)
      - Informations additionnelles liées au code fonction
        - Quantité de mots adressés, valeur du bit ou du mot, …
        - Ecrites dans plusieurs mots consécutifs
    - Contrôle de Redondance Cyclique
      - Détection des erreurs de transmission avec un CRC16
        - Composé de son octet de poids fort (PF) et son octet de poids faible (Pf)



- ModBus
  - Codes fonction
    - La requête doit comporter tous les paramètres nécessaires à l'Esclave destinataire pour réaliser l'action spécifiée par le code transmis
      - Adresse du bit, adresse du mot adressé, …

CODE	FONCTION ASSOCIEE
01 (01 HEX)	LECTURE DE N BITS DE SORTIE CONSECUTIFS
02 (02 HEX)	LECTURE DE N BITS D'ENTREE CONSECUTIFS
03 (03 HEX)	LECTURE DE N MOTS DE SORTIE CONSECUTIFS
04 (04 HEX)	LECTURE DE N MOTS D'ENTREE CONSECUTIFS
05 (05 HEX)	ECRITURE DE 1 BIT DE SORTIE
06 (06 HEX)	ECRITURE DE 1 MOT DE SORTIE
07 (07 HEX)	LECTURE DU STATUT D'EXCEPTION
08 (08 HEX)	ACCES AUX COMPTEURS DE DIAGNOSTIC
09 (09 HEX)	TELECHARGEMENT, TELEDECHARGEMENT ET MODE DE MARCHE
10 (0A HEX)	DEMANDE DE COMPTE RENDU DE FONCTIONNEMENT
11 (0B HEX)	LECTURE DU COMPTEUR D'EVENEMENTS
12 (0C HEX)	LECTURE DES EVENEMENTS DE CONNEXION
13 (0D HEX)	TELECHARGEMENT, TELEDECHARGEMENT ET MODE DE MARCHE
14 (0E HEX)	DEMANDE DE COMPTE RENDU DE FONCTIONNEMENT
15 (0F HEX)	ECRITURE DE N BITS DE SORTIE
16 (10 HEX)	ECRITURE DE N MOTS DE SORTIE
17 (11 HEX)	LECTURE D'IDENTIFICATION
18 (12 HEX)	TELECHARGEMENT, TELEDECHARGEMENT ET MODE DE MARCHE
19 (13 HEX)	RESET DE L'ESCLAVE APRES ERREUR NON RECOUVERTE

- ModBus
  - Réponses en mode Remote Terminal Unit (RTU)
    - Réponse associée aux fonctions 01, 02, 03 et 04

NUMERO ESCLAVE	CODE FONCTION	NOMBRE DE CARACTERES	DONNEES RECUES	CRC CRC16
1 OCTET	1 OCTET	1 OCTET	N OCTETS	2 OCTETS
		PF		PF Pf
				1 OCTET 1 OCTET

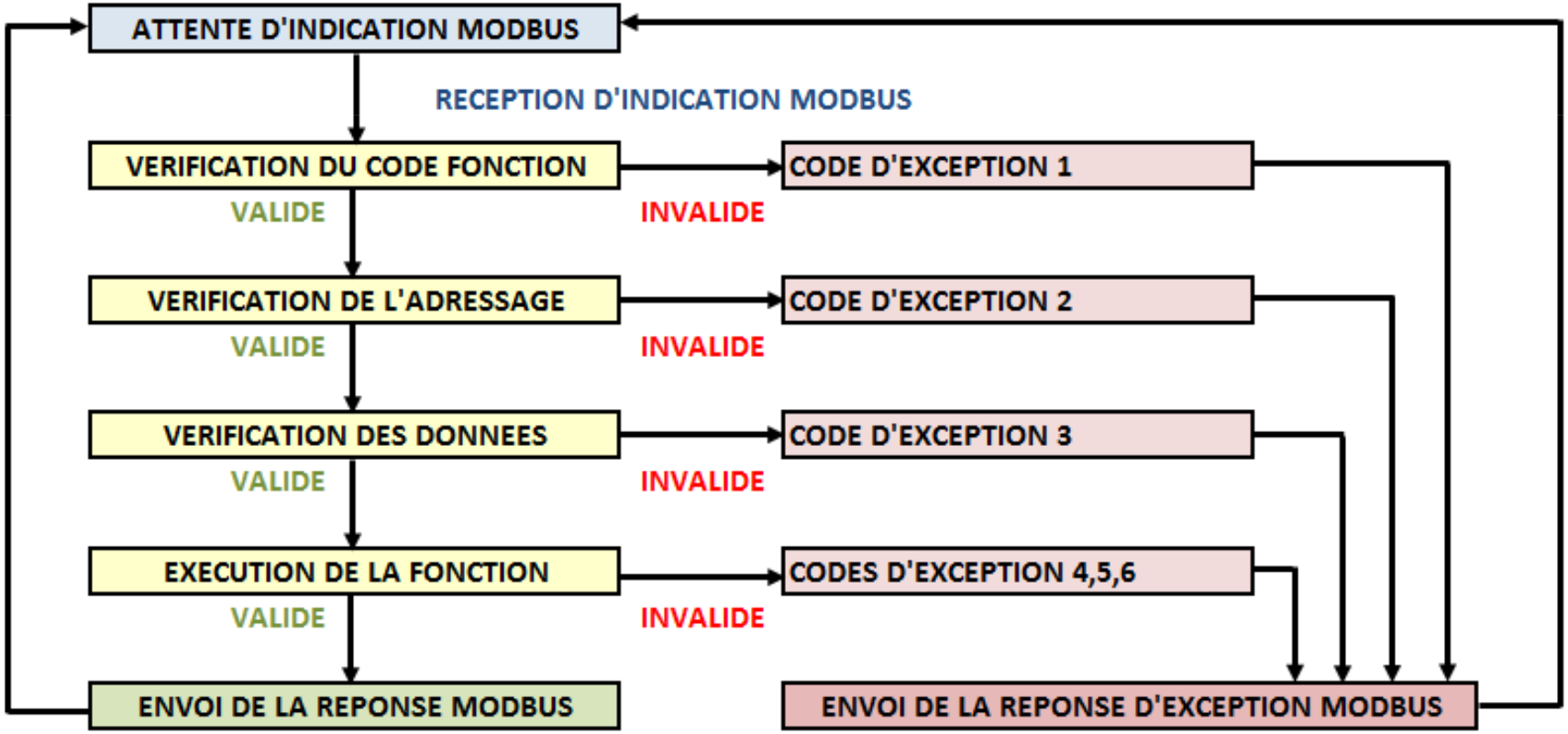
    - Réponse associée aux fonctions 05 et 06

NUMERO ESCLAVE	CODE FONCTION	ADRESSE AFFECTEE	DONNEE ECRITE	CRC CRC16
1 OCTET	1 OCTET	2 OCTETS	2 OCTETS	2 OCTETS
		PF Pf	PF Pf	PF Pf
		1+1 OCTET	1+1 OCTET	1+1 OCTET

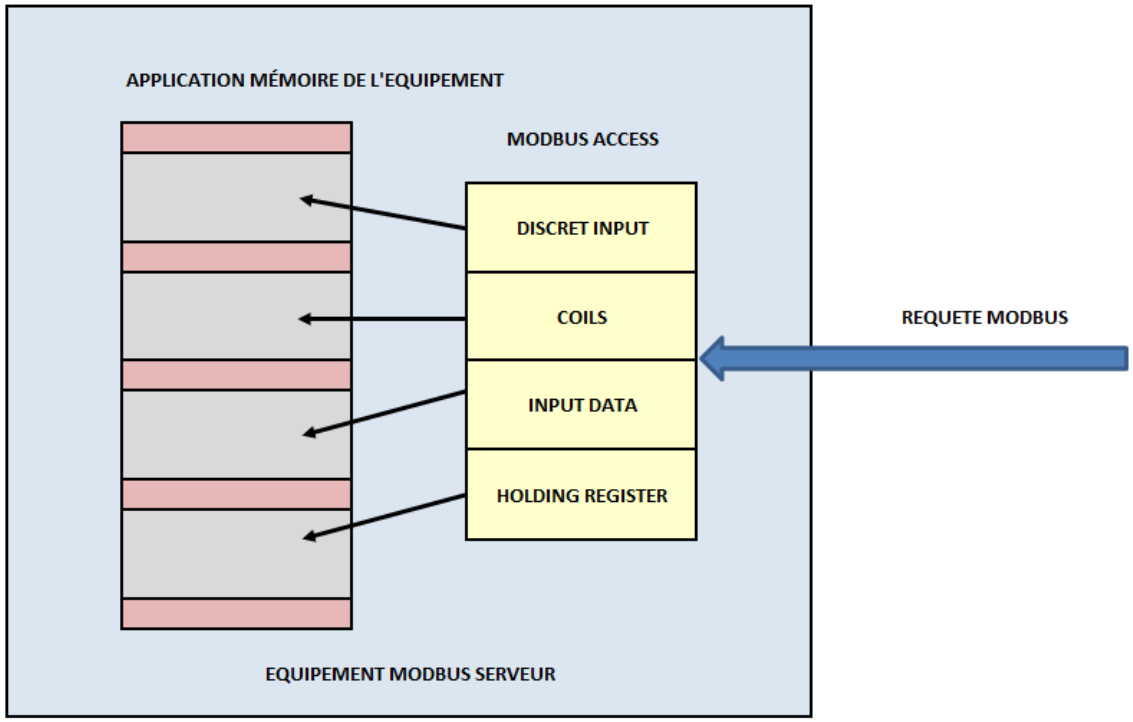
    - Réponse associée aux fonctions 05 et 06

NUMERO ESCLAVE	CODE FONCTION	ADRESSE AFFECTEE	NB DONNEES ECRITES	CRC CRC16
1 OCTET	1 OCTET	2 OCTETS	2 OCTETS	2 OCTETS
		PF Pf	PF Pf	PF Pf
		1+1 OCTET	1+1 OCTET	1+1 OCTET

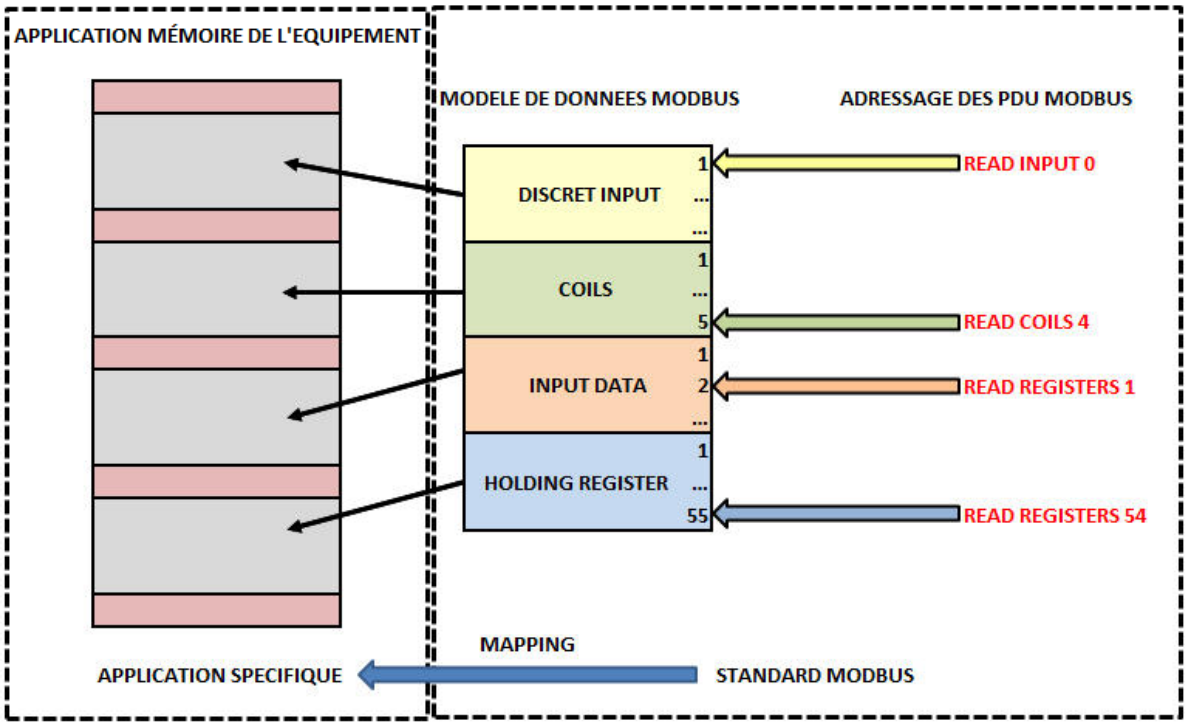
- ModBus
  - Définition d'une transaction ModBus
    - Chaque paramètre d'une requête est analysé à sa réception
      - Si le résultat est valide, la réponse envoyée est le code de la fonction requise
        - Principe d'acquittement
      - Si le résultat n'est pas valide, l'émetteur reçoit en réponse un code indiquant la nature de l'erreur



- ModBus
  - Modèle de données
    - Structure ne reconnaissant que quatre types de données de base :
      - Les entrée logiques (Discret Input) : 1 bit
      - Les sorties logiques (Coils) : 1 bit
      - Les registres d'entrée (Input Data) : mot de 16 bits
      - Les registres internes (Holding Register) : mot de 16 bits
    - Chaque équipement organise ses données en blocs (blocks) de la manière convenant le mieux à ses applications



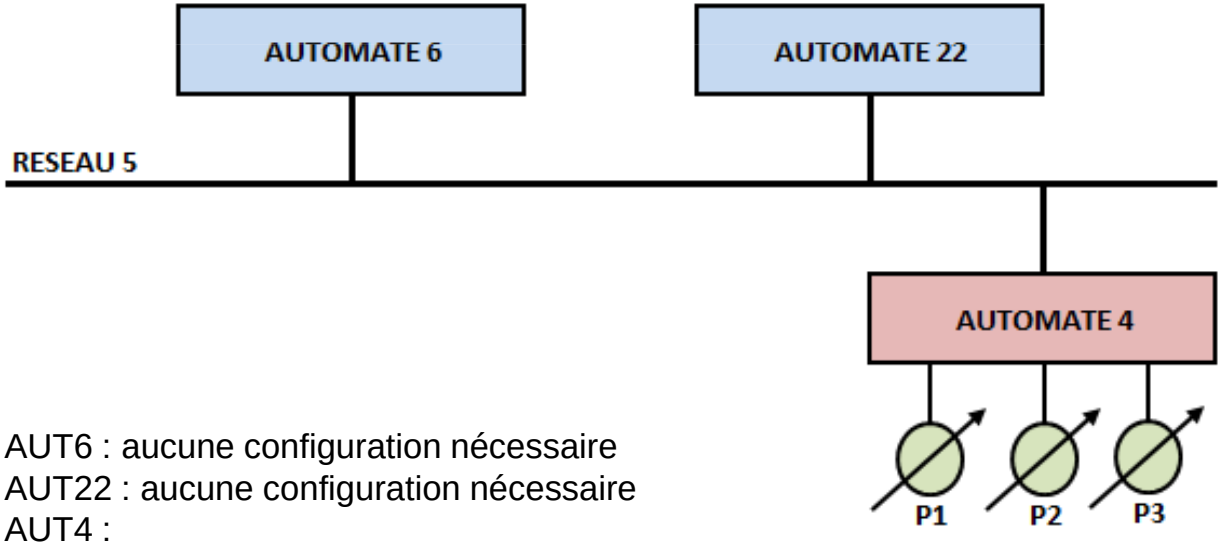
- ModBus
  - Modèle d'adressage
    - Définition de règles précises d'adressage
      - Dans un Packet Data Unit (PDU) ModBus chaque donnée est adressée de 0 à 65535
        - Un Packet Data Unit correspond au code fonction plus les données
      - Dans un modèle de données Modbus chaque donnée d'un bloc est numérotée de 0 à n
      - Une donnée Modbus "D" est adressée dans le Packet Data Unit D-1



- ModBus
  - Fonction de communication ModBus maître
    - Fonction READ_VAR
      - Permettant de lire des données consécutives d'un système distant via un réseau ModBus reliant des automates de la gamme TSX
    - Synthaxe
      - READ_VAR (adresse destinataire, type d'objet, numéro du premier objet à lire, nombre d'objets, valeur, paramètres de gestion de la fonction)
        - Type d'objet : tous les bits ou mots, internes ou systèmes, y compris les paramètres de blocs fonctions (%M, %S, %MW, %TM, %MN, %R, %C, %DR)
        - Numéro du premier objet : double mot indiquant l'indice du premier objet à lire
        - Nombre d'objets : mot spécifiant le nombre d'objets à lire
        - Valeur : tableau de mots où sont rangés les objets lus
        - Paramètre de gestion de la fonction : table de 4 mots avec H00 lecture correcte, H01 erreur d'opération, H02 réponse incorrecte, H03 taille de la réponse incohérente
    - Exemple
      - OPERATE READ_VAR (ADR# {1.2}SYS,'%MW',80,3,%MW10:3,%MW200:4)
        - Lecture des mots internes %MW80, %MW81 et %MW82 de l'automate 2 du réseau 1
        - Les valeurs des 3 mots lus sont rangés respectivement dans les mots %MW10, %MW11 et %MW12
        - Les paramètres de gestion de la fonction sont implantés à partir du mot %MW200

- ModBus
  - Fonction de communication ModBus maître
    - Fonction WRITE_VAR
      - Permettant d'écrire des données consécutives sur système distant via un réseau ModBus reliant des automates de la gamme TSX
    - Synthaxe
      - WRITE_VAR (adresse destinataire, type d'objet, numéro du premier objet à lire, nombre d'objets, valeur, paramètres de gestion de la fonction)
        - Type d'objet : tous les bits ou mots, internes ou systèmes, y compris les paramètres de blocs fonctions (%M, %S, %MW, %SW, %KW, %MD, %KD)
        - Numéro du premier objet : double mot indiquant l'indice du premier objet à écrire
        - Nombre d'objets : mot spécifiant le nombre d'objets à écrire
        - Valeur : tableau de mots où sont rangés les objets écrits
        - Paramètre de gestion de la fonction : table de 4 mots avec H00 écriture correcte, H01 erreur d'opération, H02 réponse incorrecte, H03 taille de la réponse incohérente
    - Exemple
      - OPERATE WRITE_VAR(ADR# {2.3}SYS,'%MW',50,5,%MW20:5,%MW100:4)
        - Ecriture des mots internes %MW50, %MW51, %MW52, %MW53 et %MW54 de l'automate 3 du réseau 2
        - Les valeurs des 5 mots écrits sont rangés respectivement dans les mots %MW20, %MW21, %MW22, %MW23 et %MW24
        - Les paramètres de gestion de la fonction sont implantés à partir du mot %MW100

- ModBus
  - Application pratique
    - Trois automates TSX (AUT4, AUT6 et AUT22) sont reliés par un réseau ModBus
    - Trois potentiomètres de consignes sont reliés à l'automate AUT4
    - Le but est de diffuser les informations de consignes de l'automate AUT4 aux 2 autres automates
      - Programmation de chacun des 3 automates pour la partie communication à l'aide des fonctions de communication READ/WRITE



AUT6 : aucune configuration nécessaire
AUT22 : aucune configuration nécessaire
AUT4 :
%MW0 = %IW0.0
%MW1 = %IW0.1
%MW2 = %IW0.2
WRITE_VAR (ADR# {5,6}SYS, '%MW',10,3, %MW0:3, %MW50:4)
WRITE_VAR (ADR# {5,22}SYS, '%MW',10,3, %MW0:3, %MW50:4)

- Ethernet
  - Technologie de plus en plus utilisée comme solution de communication dans l'industrie
    - Utilisation inéluctable dans les ateliers : technologie banalisée, performante, fiable, peu onéreuse
    - Son point faible : son indéterminisme dû à la méthode d'accès CSMA/CD
    - Reste incontournable pour mettre en oeuvre des programmes d 'automatisation répartis d'autant plus que les flux de données ne cessent de croître
  - Avantages
    - Interface bon marché
    - Compatibilité avec les solutions informatiques de gestion
    - Protocoles banalisés ouverts et utilisables immédiatement
    - Augmentation constante des débits : 10, 100, 1000 Mbit/s
    - Contraintes déterministes atteintes grâce à l'utilisation conjointe de switches avec des débits élevés
  - Inconvénients
    - Câblage complexe et onéreux (hub, switch...).
    - Connectique non adaptée au milieu industriel (RJ45 vs M12)
    - Sécurité du réseau non assuré
    - Protocoles classiques non adaptés aux contraintes industrielles
    - Contraintes temporelles non garanties

- Ethernet
  - Alternatives Ethernet industrielles
    - Ethernet/Industrial Protocol (Ethernet/IP) de Rockwell
      - Encapsulation de messages deviceNet ou ControlNet dans un paquet TCP ou UDP
    - ProfiNet de Siemens
    - High Speed Ethernet (HSE) de Fieldbus Foundation (FF)
      - Fédération des bus de terrain supportant le mode de transmission H1
      - Présente toutes les caractéristiques de H1 (modèle producteur/consommateur, approche objet...)
      - Basé sur l'encapsulation du protocole H1 dans une trame Ethernet à 100 Mb/s
    - IDA soutenue par Schneider Electric
    - Catégories de solutions techniques :
      - Solutions qui encapsulent les données dans une trame EtherNet ou paquet TCP/UDP
      - Solutions qui utilisent des passerelles ou des serveurs "proxy"
  - Solution Ethernet avec TCP/IP ou UDP/IP envisageable dans les cas suivants
    - Utilisation d'Ethernet à 100 Mbit/s ou 1000Mbit/s
    - Utilisation d'Ethernet commuté
    - Utilisation du protocole de transport UDP ou TCP en fonction du besoin

Questionnement préalable

- Réseaux et bus de terrain
  - Nécessité de se poser des questions avant de faire un choix engageant une entreprise
    - Questionnement général
      - Utilisation d'un standard de fait ou un standard international
      - Utilisation d'un système ouvert ou une solution propriétaire
      - Spécifications techniques publiées par un organisme indépendant ou non
      - Nécessité ou non de payer des royalties ou des licences
      - Existence ou non d'un "user group"
      - Interopérabilité totale de la solution
    - Questionnement sur le matériel
      - Immunité au bruit
      - Durcissement aux rayonnements
      - Circuits disponibles auprès de différents fabricants
      - Mémoire embarquée sur le circuit
      - Fonctionnalités diverses disponibles comme sur un microcontrôleur
      - Existence ou non de modules du commerce prêts à l'emploi
      - Téléalimentation ou non

Questionnement préalable

- Réseaux et bus de terrain
  - Nécessité de se poser des questions avant de faire un choix engageant une entreprise
    - Questionnement sur le bus de terrain
      - Identification de la topologie du réseau
      - Identification du type de support
      - Longueur maximale du support physique
      - Nombre maximum de noeuds
      - Technique d'adressage
      - Protocoles mis en oeuvre
      - Temps de réponse maximum
      - Débit en bits/s ou messages/s suivant la configuration
      - Possibilité d'émission de messages
      - Possibilité de multimaître
      - Possibilité de diffusion en "broadcasting"
      - Possibilité de réessai sur erreur
      - Possibilité de redondance du support de transmission
      - Possibilité d'utiliser des répéteurs
      - Estimation de la charge de travail pour configurer le réseau
      - Estimation de la charge de travail ajouter/enlever un noeud
      - Influence induite par l'ajout ou le retrait d'un noeud

Questionnement préalable

- Réseaux et bus de terrain
  - Nécessité de se poser des questions avant de faire un choix engageant une entreprise
    - Questionnement sur l'environnement de développement
      - Bus d'interface disponible (VME, PC...)
      - Logiciels disponibles pour PC (Windows XP, 7, 8, 2010, 2013, …)
      - Logiciels disponibles pour VME (VxWorks, OS9, LynxOS)
      - Outils de supervision disponibles (configuration, diagnostics...)
      - Interface de programmation disponible (API)
      - Existence des testeurs ou analyseurs de protocole pour PC ou autre
    - Questionnement sur les coûts
      - Coûts des circuits d'interface ou microcontrôleur
      - Coûts des modules du commerce
      - Coûts des kits de développement et des licences
  - Questionnement impératif dans de nombreux domaines liés aux réseaux et à l'informatique
    - Non spécifique au réseaux et bus de terrain et applicable dans tous les cas

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- *CM 6 : Réseaux WLAN et sécurité*
  - *TD 5 : Réseaux Wifi et sécurité*
- *CM 7 : Réseaux et bus de terrain*
  - **TD 6 : Réseaux et bus de terrain**
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

- Exercice 1 (25 minutes)
  - Ecrivez le programme dans l'automate identifié par l'adresse 0.1.1 (réseau, automate, carte) donnant les résultats suivant lors du démarrage d'un moteur
    - Lecture des registres
      - Démarrage de la lecture sur un front montant du démarreur M0
      - Lecture des registres 452, 455, 461 et 466
      - Le contenu de ces registres sont écrit respectivement dans les mots MW10, MW20, MW30 et MW40
      - Le compte rendu de lectures sont écrit respectivement dans les mots MW150, MW160, MW170 et MW180
      - Le bit d'activité MW150:X0 passe à 1 lors de l'exécution de la fonction et revient à 0 à la fin de l'exécution
      - Le bit d'activité MW160:X0 passe à 1 lors de l'exécution de la fonction et revient à 0 à la fin de l'exécution
      - Le bit d'activité MW170:X0 passe à 1 lors de l'exécution de la fonction et revient à 0 à la fin de l'exécution
      - Le bit d'activité MW180:X0 passe à 1 lors de l'exécution de la fonction et revient à 0 à la fin de l'exécution
    - Ecriture des registres
      - Ecriture dans le démarreur sur le front montant de M0
      - Les informations stockées dans le mot MW100 seront écrites dans le registre 704 une fois transmises
      - Les informations stockées dans le mot MW110 seront écrites dans le registre 705 une fois transmises
      - Les mots MW200 et MW210 sont des comptes rendus de lecture
      - Le bit d'activité MW200:X0 passe à 1 pendant l'exécution de la fonction et revient ensuite à 0
      - Le bit d'activité MW210:X0 passe à 1 pendant l'exécution de la fonction et revient ensuite à 0

- Exercice 1 (25 minutes)
  - Ecrivez le programme dans l'automate identifié par l'adresse 0.1.1 (réseau, automate, carte) donnant les résultats suivant lors du démarrage d'un moteur
    - Lecture des registres
      - If %M0 then
        %MW150:X0 := 1;
        READ_VAR (ADR 0.1.1,'%MW',452,1,%MW10:1,%MW150:4)
        %MW160:X0 := 1;
        READ_VAR (ADR 0.1.1,'%MW',455,1,%MW20:1,%MW160:4)
        %MW170:X0 := 1;
        READ_VAR (ADR 0.1.1,'%MW',461,1,%MW30:1,%MW170:4)
        %MW180:X0 := 1;
        READ_VAR (ADR 0.1.1,'%MW',466,1,%MW40:1,%MW180:4)
        End_if;
    - Ecriture des registres
      - If %M0 then
        %MW200:X0 := 1;
        WRITE_VAR (ADR 0.1.1,'%MW',704,1,%MW100:1,%MW200:4)
        %MW210:X0 := 1;
        WRITE_VAR (ADR 0.1.1,'%MW',705,1,%MW110:1,%MW210:4)
        End_if;

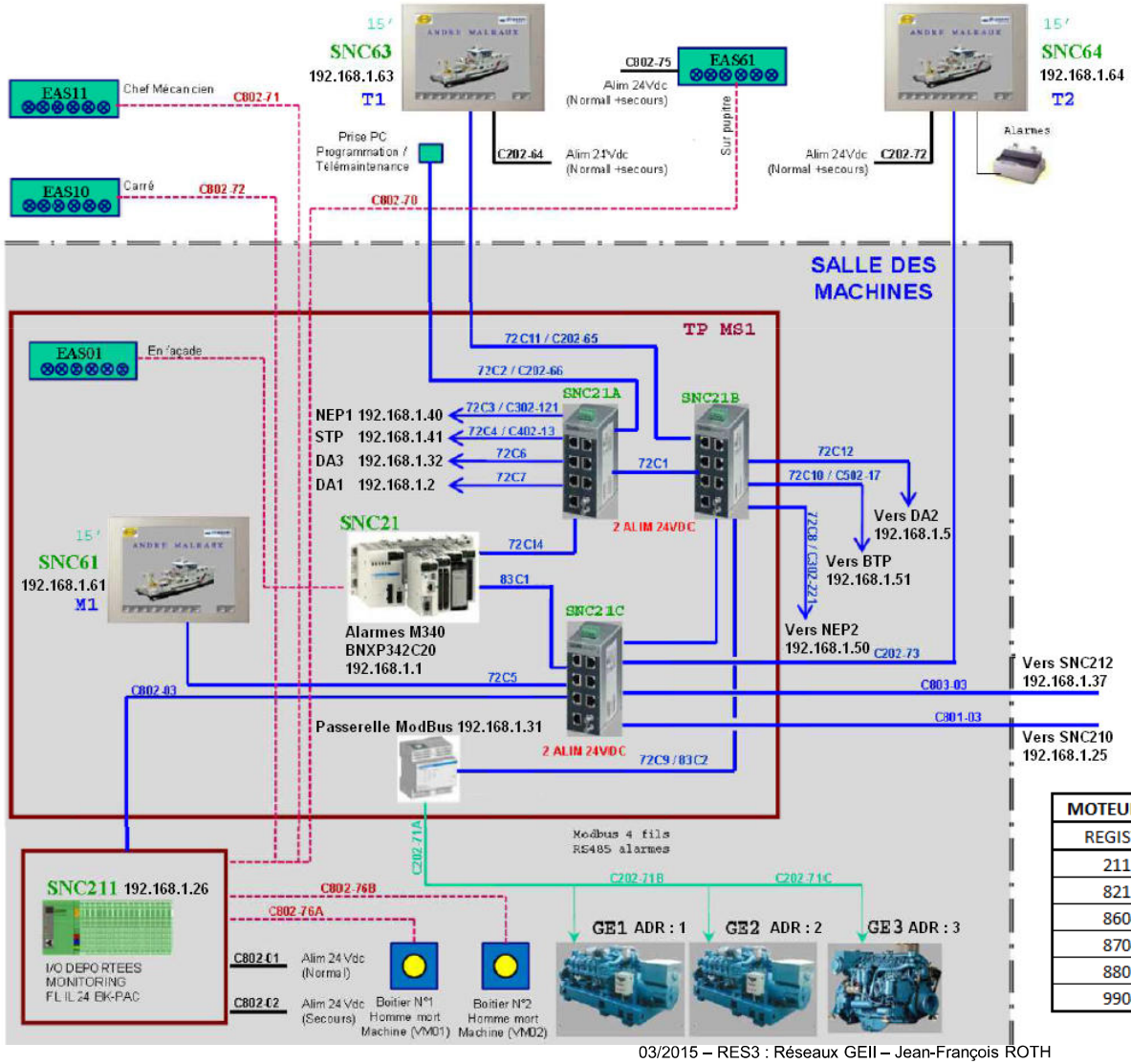
- Exercice 2 (15 minutes)
  - Décrivez les opérations réalisées par le programme suivant écrit dans l'automate du banc de levage
    - READ_VAR (ADR#{2.25}SYS,'%MW',450,20,%MW8600:20,%MW8445:4)
      - L'adresse de l'automate du banc de levage est 25 et celui-ci se trouve dans le réseau 2
      - Lecture de 20 mots à partir du registre 450
      - Les valeurs des 20 mots lus sont rangés respectivement dans les mots allant de %MW8600 à %MW8619
      - Les paramètres de gestion de la fonction sont implantés à partir du mot %MW8445
  - Décrivez les opérations réalisées par le programme suivant écrit dans l'automate de la porte de garage
    - READ_VAR (ADR#{2.128}0.0.1,'%MW',0,20,%MW8675:20,%MW8475:4)
      - L'adresse de l'automate gérant, entre autres, la porte de garage est 128 et celui-ci se trouve dans le réseau 2
      - L'adresse de la porte automatique de garage est 0.0.1
      - Lecture de 20 mots à partir du registre 0
      - Les valeurs des 20 mots lus sont rangés respectivement dans les mots allant de %MW8675 à %MW8694
      - Les paramètres de gestion de la fonction sont implantés à partir du mot %MW8475

- Exercice 3 (55 minutes)
  - En considérant la trame Ethernet suivante, obtenue par l'analyseur de protocoles WireShark, ainsi que le schéma réseau et le tableau lié aux registres ModBus (page 47)
    - Remarque : la trame est donnée sans préambule, ni SFD, ni CRC

0000	00 80 f4 03 4f 89 74 2f 68 40 07 35 08 00 45 00
0010	00 34 4c 04 40 00 80 06 e3 86 c0 a8 01 40 c0 a8
0020	01 1f c5 b9 01 f6 24 ee 56 15 a9 8c d2 60 50 18
0030	00 fc fc 44 00 00 00 00 00 00 00 06 01 03 21 9c
0040	00 01

1. Quelle est l'adresse physique de l'appareil ayant initié l'échange ?
2. Quelle est l'adresse réseau et le nom de l'appareil ayant initié l'échange ?
3. Quel est le port à partir duquel le message a été envoyé ?
4. Quelle est l'adresse physique de l'appareil a qui est destiné le message ?
5. Quelle est l'adresse réseau et le nom de l'appareil a qui est destiné le message ?
6. Quel est le port sur lequel le message a été envoyé ?
7. Sachant qu'un entête ModbusTCP débute par 2 octets d'identifiant de la transaction (généralement 2 fois la valeur 0) puis 2 octets de version du protocole (2 fois la valeur 0) puis 2 octets indiquant la longueur du message (en octets) précède le message, quel est le message ModBus véhiculé ?
8. Que concluez-vous au niveau réseau du contenu de cette trame Ethernet ?

- Exercice 3 (55 minutes)
  - Schéma réseau et contenu des registres



MOTEUR GE1	MOTEUR GE2	MOTEUR GE3	CONTENU DES REGISTRES
REGISTRE	REGISTRE	REGISTRE	INDICATION FOURNIE
2111	2112	2113	NIVEAU D'HUILE EN L
8211	8212	8213	TEMPERATURE EN °C
8604	8605	8606	VITESSE DE ROTATION EN TR/MIN
8704	8705	8706	PUISSANCE EFFECTIVE EN kW
8801	8802	8803	CONSOMMATION HORAIRE DE CARBURANT EN L
9904	9905	9906	ETAT DU MOTEUR MARCHE/ARRET

- Exercice 3 (55 minutes)
  - En considérant la trame Ethernet suivante, obtenue par l'analyseur de protocoles WireShark, ainsi que le schéma réseau et le tableau lié aux registres ModBus (page 47)
    - Remarque : la trame est donnée sans préambule, ni SFD, ni CRC

0000	00 80 f4 03 4f 89 74 2f 68 40 07 35 08 00 45 00
0010	00 34 4c 04 40 00 80 06 e3 86 c0 a8 01 40 c0 a8
0020	01 1f c5 b9 01 f6 24 ee 56 15 a9 8c d2 60 50 18
0030	00 fc fc 44 00 00 00 00 00 00 00 06 01 03 21 9c
0040	00 01

1. Adresse Ethernet source : 74:2F:68:40:07:35
2. Adresse IP source : c0 a8 01 40 soit 192.168.1.64, il s'agit de SNC64 (équipement de supervision)
3. Port TCP source : c5 b9 soit 50617
4. Adresse Ethernet destination : 00:80:F4:03:4F:89
5. Adresse IP destination : c0 a8 01 1f soit 192.168.1.31, il s'agit de la passerelle ModBus TCP
6. Port TCP destination : 01 f6 soit 502 (port standard modbus TCP)
7. Message ModBus : 00 00 00 00 00 06 01 03 21 9c 00 01
   - 00 00 00 00 : Identifiant de la transaction (2 octets) et version du protocole (2 octets)
   - 06 : longueur du message, soit 6 octets
   - 01 : Groupe moteur GE1
   - 03 : Indique une lecture de N mots de sortie en ModBus (Page 30 du CM7)
   - 21 9c : soit le registre 8604 (2 octets) car les 2 octets suivants 00 01 indiquent qu'il n'y a qu'un seul mot à lire
   - Le message correspond donc à une demande de la vitesse du rotation du groupe moteur GE1
8. En réseau, Modbus est un protocole applicatif véhiculé par Ethernet (physique), IP (réseau) et TCP (transport) et est encapsulé dans le champ données de la trame Ethernet

- Exercice 4 (20 minutes)
  - Présentation des Travaux Pratiques RES3
    - TP1 (4h) : Technologie ADSL
      - Mise en évidence de l'impact de la distance sur les technologies ADSL, ADSL 2+ et ReADSL 2
      - Mise en évidence de l'impact des calibres des câbles sur les technologies ADSL, ADSL 2+ et ReADSL 2
    - TP2 (4h) : Analyse de trames et Encapsulation Ethernet
      - Analyse et décodage d'un trame Ethernet à l'oscilloscope
      - Analyse des trames Ethernet générées par la commande PING pour étudier les protocoles ARP/ICMP
      - Analyse des trames Ethernet générées par la commande TFTP pour étudier les protocoles IP/UDP
    - TP3 (4h) : Configuration d'un réseau IP / Routage IP / Wifi
      - Configuration de la fonction DHCP statique et dynamique d'un routeur
      - Configuration et sécurisation d'un réseau WLAN
      - Configuration de la table de routage
    - TP4 (4h) : Réseaux et bus de terrain
      - Analyse du protocole ModBus/TCP sur automate programmable industriel
      - Configuration de la connexion vers Entrées/Sorties déportées ou commande moteur ou axe robotisé
        - Ce TP pourrait être réalisé en 3h en fonction du nombre de groupes de Travaux Pratiques
    - TP5 (2h) : TP Test
      - Partie théorique : questions sur les différents TP réalisés
      - Partie pratique : analyse d'une trame TCP/IP

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- *CM 6 : Réseaux WLAN et sécurité*
  - *TD 5 : Réseaux Wifi et sécurité*
- *CM 7 : Réseaux et bus de terrain*
  - *TD 6 : Réseaux et bus de terrain*
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances