MI11

Systèmes temps réel critique

Jérôme De Miras

Poste : 59 02
e-Mail : demiras@hds.utc.fr

Communications temps réel

Exigences

Exigences (1)

- Latence du protocole
  - Gigue minimale
  - Latence faible et connue
  - Livraison simultanée en multicast
- Composabilité
  - Encapsulation temporelle (pare feu temporel)
    - Pas de signaux qui traversent les CNI
    - Propriétés temporelles séparées entre CNI et hôte
  - Aider le client et le serveur
    - CS exerce un contrôle du flux des requêtes
  - Flexibilité
    - Support de différentes configurations qui peuvent changer au cours du temps
    - Message sporadiques urgent avec un délai minimal

Exigences (2)

- Détection d'erreurs
  - Détection et correction d'erreur sans gigue
  - Sinon avertissement de l'émetteur et des autres clients
  - Gérer les blackout (EMI) : détection et reprise
  - Détection des erreurs de nœuds (Membership Service)
- Accusé de réception de bout en bout
  - La validation d'une action peut apparaître sur un autre nœud
  - L'action d'un actionneur doit être vérifiée (ex : Three Mile Island Nuclear Reactor #2, 28 mars 1979)

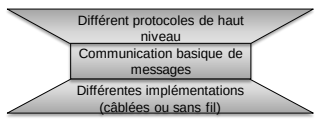
Structure physique

- Point à point
  - Onéreux
  - Trop de ports et de câbles
- Bus ou anneau :
  - dépend de la technologie de câblage
  - Bus : paire torsadée
  - Anneau : fibre optique
- Eloignement physique des SRU d'une FTU
  - Augmente le câblage
  - Renforce la sureté en cas de dommage physique

Eléments de conception

Modèle « waistline »

- Abstraction simple décrivant le service basique de transport de messages (BTMS) remplissant les exigences citées
  - Système unidirectionnel pour qu'une faute du récepteur n'impacte pas l'émetteur
  - Notion proche du service datagramme, les exigences temporelles en plus



Propriétés temporelles du BTMS

- En fonction des propriétés temporelles on distingue trois types de messages
  - Messages Event-Triggered
    - Produits sporadiquement
    - Pas de garanties temporelles entre émission et réception
    - Possibilité de dépassement de la capacité de transmission
  - Messages Rate-Constrained
    - Produits sporadiquement avec une limite de fréquence
    - Garantie de ne pas dépasser un pire cas de latence de transport
    - Gigue dépendante de la charge du réseau
  - Messages Time-Triggered
    - Acceptation mutuelle par l'émetteur et le récepteur des instants d'émission et de réception
    - Garantie des instants de réception
    - Gigue dépendante de la précision du temps global

Limitations physiques de performances

- Bande passante
- Délai de propagation
  - Temps mis par un bit pour parcourir toute la longueur du réseau (2/3 vitesse de la lumière)
  - Permet de définir la longueur du canal en bits (bl) dans le délai de propagation
- L'efficacité en donnée d'un bus est déterminée par la nécessité de laisser au moins un délai de propagation entre chaque message

$$\text{efficacité} < m/(m+bl)$$

m : taille du message en bit

Contrôle de flux

- Garder la synchronisation entre émetteurs et récepteurs
- Généralement le récepteur contrôle la vitesse maximum de transmission
- 3 types de contrôle
  - Back-pressure
  - Explicite
  - implicite

Contrôle de flux back-pressure

- Le canal est occupé et un émetteur est obligé de retarder son émission
- Ex : bus CAN
  - Aucun accès autorisé à un émetteur si une émission est déjà en cours

Contrôle de flux explicite

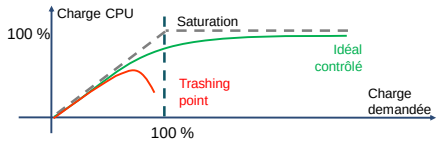
- Récepteur envoie une message explicite à l'émetteur
  - Suppose que l'émetteur est dans la sphère de contrôle du récepteur
- Ex : accusé de réception positif ou retransmission (protocole PAR)
  - Triggué par événement
    i. Le client de l'émetteur initie la communication
    ii. Le récepteur peut retarder l'émission via le canal bidirectionnel de communication
    iii. Une erreur est détectée par l'émetteur ; le récepteur ne sait pas qu'une erreur est survenue
    iv. Une redondance temporelle est utilisée pour corriger les erreurs de com.
    ↗ de la latence de com.

Contrôle de flux implicite

- Tout est défini à priori
- Les points temporels d'envoi sont connus des deux parties à l'avance
  - Le récepteur détecte une erreur si aucun message n'est là au temps convenu
- Redondance active par envoi multiple
  - Si possible sur plusieurs canaux
- Communication unidirectionnelle
  - Pas de réponse

Trashing

- Décroissance abrupte de fonctionnalité avec la charge (ex : bouchon sur la route)



- Toujours avoir un système exempt de trashing point
- Causes possibles
  - Le mécanisme de répétition dans un protocole PAR
  - Services dans l'OS
    - ↗ charge
    - ↘ ressources
- Obligation de boucler le système explicite pour diminuer la « pression » suffisamment tôt

Contrôle de flux et système TR

caractéristiques	Contrôle explicite	Contrôle implicite	Système TR dur
Signal de contrôle	Récepteur contrôle événements d'envoi de l'émetteur	Généré par le passage du temps	Récepteur possiblement hors sphère de contrôle émetteur
Détection d'erreurs	Emetteur	Récepteur	Récepteur
Sujet au trashing	Oui	Non	A éviter
Multicast	Difficile	Oui	Requis

- Ex : 8 Aout 1993
  - prototype d'avion « fly by wire » s'écrase
  - Réponse trop lente aux ordres du pilote
- L'interfaçage entre les deux types n'est pas simple
  - Ex : implicite → explicite
    - nécessité de bufférisér : quelle taille ?

OSI pour TR ?

Modèle de référence OSI

- 1 couche : 1 aspect particulier du problème de communication
- Les piles de protocole PAR sont basées sur ce principe
  - Les 2 partenaires maintiennent une connexion point à point
  - Les messages sont ET
  - Contrôle de flux explicite : retransmission en cas d'erreur
  - Latence faible et gigue réduite ne sont pas des exigences

Application
Présentation
Session
Transport
réseau
Liaison données
Physique

ATM

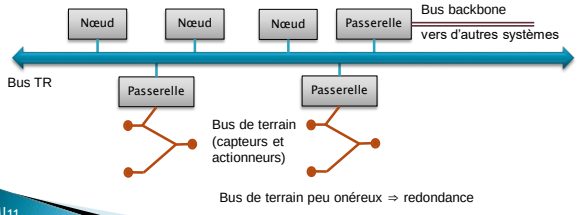
- Asynchronous Transfert Mode
- Développé pour effectuer des communications TR avec peu de gigue sur des réseaux haut débit
  - Paquet de taille fixe : 53 octets
  - Entête : 5 octets (contrôle et routage)
  - Transfert en mode Time Division Multiplexing (TDM)

Cellule (53 octets)					
Entête (5octets)					Data
Generic flow control	Channel identifier	Paylod type identifier	Cell loss priority	Header checksum	Payload
4 bits	24 bits	2 bits	2 bits	8 bits	48 octets

Architecture de communication TR

- 3 réseaux différents :
  - Bus de terrain
  - Réseau TR
  - Réseau « backbone »

} Fourniture de réponses temporelles garanties



Bus de terrain peu onéreux ⇒ redondance

Comparaison réseaux

caractéristiques	Bus de terrain	Réseau TR	Réseau backbone
Sémantique message	état	état	événement
Contrôle latence/gigue	Oui	Oui	Non
Taille données typique	1-6 octets	6-12 octets	>100 octets
Synchronisation horloge	Oui	Oui	Optionnel
Tolérance aux fautes	Limitée	Oui	Limitée
Membership service	Possible	Oui	Possible
Topologie	Multicast	Multicast	Point à point
Contrôle du SC	Multi-maître	Distribué	Central ou distribué
Contrôle de flux	Implicite	Implicite	Explicite
Coût bas	Très important	Important	Peu important

Conflits de design de protocoles

Conflits

- Contrôle externe contre composabilité
  - Dans le domaine temporelle
    - Spécification temporelle complète
    - Pas de modification de propriétés individuelles après ajout de nouveaux nœuds
    - Tests individuels des nœuds
- Flexibilité contre détection d'erreurs
  - Besoin d'une connaissance à priori
- Données sporadiques contre données périodiques
  - Les objectifs de qualité ne peuvent être atteints pour les deux types simultanément
- Contrôle centralisé contre tolérances aux fautes
- Accès probabiliste contre déterminisme
  - Les arbitrages (protocole PAR) contrarie la possibilité d'obtenir un comportement prédictible

Protocoles

Event Triggered communication

- CSMA : Carrier Sense Multiple Access
  - CSMA/CD-LON : Collision Detection (Ethernet)
    - Utilisation d'un générateur de nombres aléatoires
  - CSMA/CA : Collision Avoidance
    - « bit arbitration » pour empêcher les collisions
    - Ex : CAN (Control Area Network développé par Bosch)
      - Etat dominant « 0 »
      - État récessif « 1 »

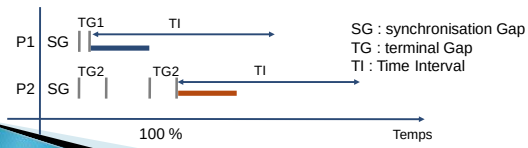
Field	Arbitration	Control	Data field	CRC	A	EOF
bits	11	6	0-64	16	2	7

Rate-Constrained communication (1)

- Token-ring (Prifibus)
  - Système avec un message spécial : le token
  - 2 paramètres
    - Token hold time
    - Token rotation time
    - Pb : perte du token
- Central master (FIP)
  - Système multi-master
  - Liste de broadcast
  - Envoi du nom d'un intervenant, réponse de l'intervenant

Rate-Constrained communication (2)

- Minislotting
  - Stratégie d'accès pilotée par le temps
  - Partition en séquences de minislots de longueur le temps de propagation dans le canal
  - Chaque nœud possède un N° unique de minislot qui doit s'écouler avec silence sur le canal avant d'avoir le droit de transmettre
  - ARINC 629
    - Principe de la salle d'attente
      - Phase 1 : admission de process
      - Phase 2 : communication



Rate-Constrained communication (3)

- Avionic Full Duplex Switched Ethernet (AFDX)
  - Bande passante allouée statiquement à chaque émetteur sur un lien virtuel
    - Lien entre un émetteur avec un nombre défini de récepteurs
  - Garanties :
    - L'ordre de délivrance est le même que l'ordre d'émission
    - Une bande passante minimum et une gigue maximum sur un lien virtuel
    - Pas de perte de donnée sur les switchs
- Bus audio vidéo
  - Synchronisation de multiple flux
  - Pire cas de délai de transport borné
  - Les ressources allouées restent valables pour la durée de la session

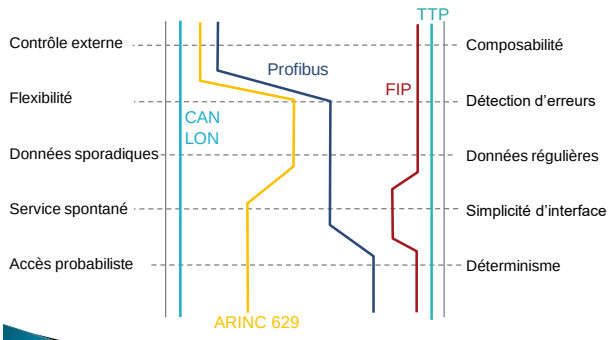
Time-Triggered communication (1)

- TDMA : Time Division Multiple Acces
  - Stratégie d'accès statique distribuée
  - Nécessite un temps global
  - Le passage du temps autorise la transmission
  - La capacité d'un canal est divisé en n slots
  - 1 slot est assigné à 1 nœud
  - Le passage de tous les slots est un ***tour***
  - Tous les tours ne contiennent pas forcément les mêmes messages
  - Cycle cluster : séquence de tous les différents tours TDMA
  - Ex : TTP

Time-Triggered communication (2)

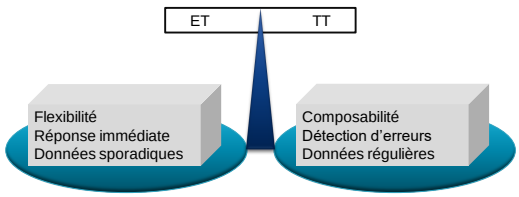
- TTP
  - CA-TCCS : Collision avoidance Time Controlled Circuit Switching
  - Synchronisation d'horloge tolérante aux fautes
  - Service d'appartenance (signalement des fautes)
- FlexRay : combinaison de deux choses
  - TT messages : TTP sans service d'appartenance
  - ET messages : ARINC 629 mini slotting sans salle d'attente

Comparaison



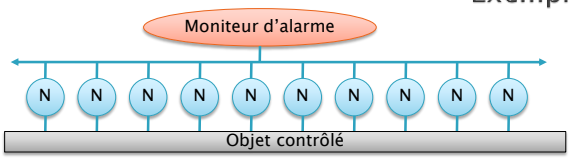
Comparaison

- Aucun protocole ne peut remplir toutes les exigences simultanément



Comparaison de performances ET/TT

Exemple



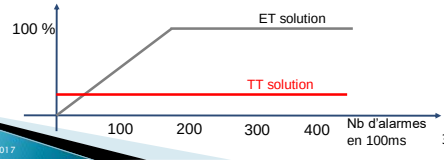
- Chaque nœud interface doit surveiller 40 alarmes binaires
- En 100 ms après l'apparition d'une alarme, l'opérateur doit être informé
- Canal de communication : 100 Kbits/seconde

Exemple : solution ET

- Utilisation du même protocole pour ET et TT (CAN par exemple)
- Implémentation ET
  - Event message → opérateur
  - Aussi vite que possible
  - Contenu : nom de l'alarme encodé sur 1 octet
  - Overhead : 44 bits + écart de 4 bits entre message → 56 bits
  - 100 Kbits : 180 messages peuvent transiter sur 100 ms
  - Pb : charge max : 400 alarmes

Exemple : solution TT

- Implémentation TT
  - 1 message périodique toutes les 100 ms pour chaque nœud
  - Données : codées sur 40 bits (5 octets)
    44 + 4 + 40 → 88 bits par message
  - 100 Kbits : 110 messages possibles et 10 utilisés (10% de la bande passante)
  - **Exigences satisfaites**



La couche physique

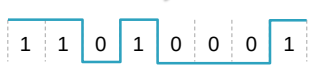
Code de transmission

- Bit pattern
- Ex : le CAN suppose que chaque « cellule bit » a le temps de se stabiliser sur le canal (arbitrage de priorité)
- Propriétés des codes de transmission
  - Synchrone : le récepteur synchronise sa logique durant la réception sur l'horloge de l'émetteur
    - Besoin de transition fréquente dans le flux de données
  - Asynchrone : synchronisation du récepteur au début du message
    - Dérive d'horloge ⇒ taille de message limitée

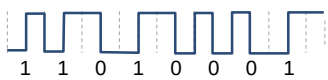
Exemples de codes de transmission

- Code NR2 (non return to zéro)
  - « 0 » bit niveau bas
  - « 1 » bit niveau haut

} Code non synchronisant

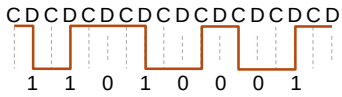


- Code Manchester
  - Code resynchronisant
  - Le plus petit élément correspond à une demi cellule bit



Exemples de codes de transmission (2)

- Modulation de fréquence modifiée (MFM)
  - Taille d'un élément : 1 cellule bit
  - Resynchronisant
  - « 0 » est encodé par aucun changement sur un point donnée
  - « 1 » : changement de niveau en un point donnée

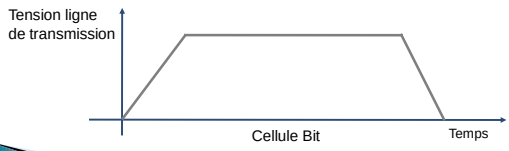


Forme du signal

- La forme des éléments détermine les émissions électromagnétiques générées
  - Interférences (EMI)

- Montée
- Maintien
- descente

} Eviter les variations brusques
⇒ antagonisme avec l'augmentation de la vitesse de transmission



RTNET

Ethernet temps réel

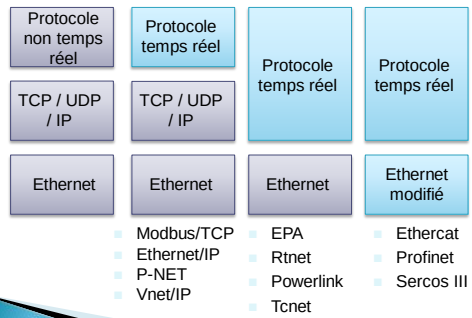
Communications temps réel

Caractéristiques :
- Latence
- Gigue
- Bande passante

Déterminisme de la communication :
Capacité à assurer un délai maximum de transmission

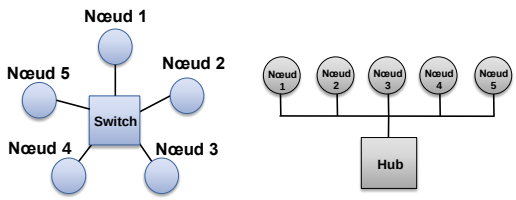
Ethernet temps réel

- Plusieurs possibilités en fonction des besoins



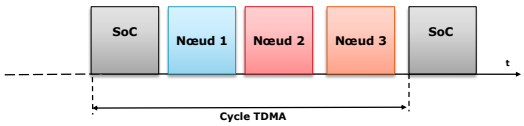
Rtnet

- Matériel standard
- TDMA
- Horloge distribuée
- Topologie étoile ou bus

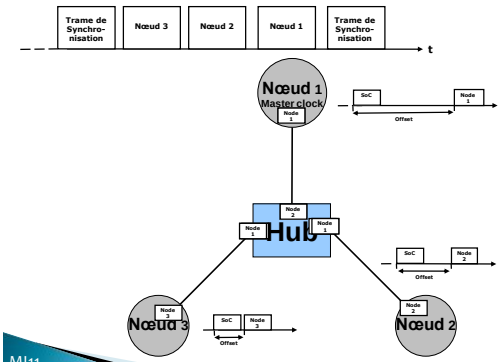


TDMA (1/2)

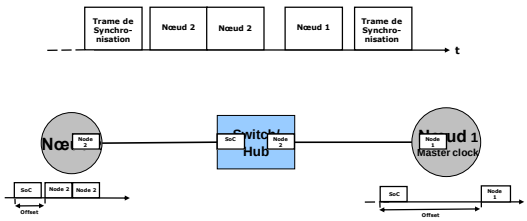
- Cycle et slots sont définis par l'utilisateur
- Trame de synchronisation à chaque début de cycle
- Slots définissant les temps d'émission pour chaque nœud



TDMA (2/2)

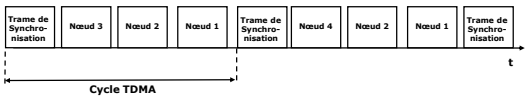


Configuration

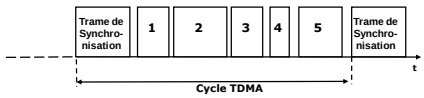


Configuration

- Slots alternés



- Taille des slots

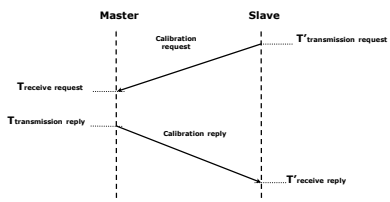


Horloge distribuée

- Précision Time Protocol (IEEE 1588)
- Chaque nœud doit se synchroniser par rapport à une horloge de référence
- Chaque nœud doit également mesurer le temps de trajet d'un paquet
- Le maître émet à chaque début de cycle une trame de synchronisation

Synchronisation

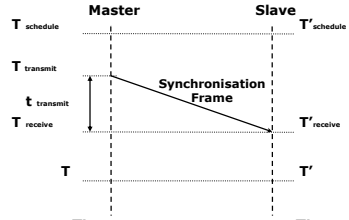
- **Chaque noeud effectue lors de son arrivée une estimation de la latence**



$T_{transmit} = ½ * (T'_{receive\ reply} - T'_{transmission\ request}) - (T_{transmission\ reply} - T_{receive\ request})$

Synchronisation

- A chaque début de cycle, les nœuds synchronisent leurs horloges

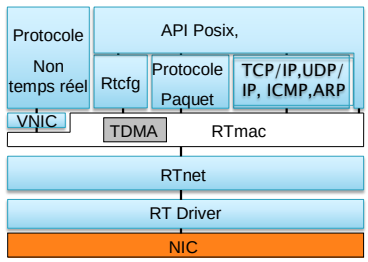


$t_{offset} = T_{receive} - T'_{receive} = T_{transmit} + t_{transmit} - T'_{receive}$

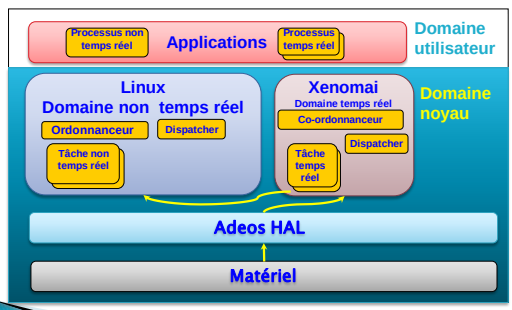
$T = T' + t_{offset}$

Protocole de communication

- Ensemble de modules noyau :



Noyau temps réel



Tâches critiques

- Modification du driver associé au contrôleur Ethernet
  - Buffer, allocation/libération mémoire
  - Attente active (spinlock)
  - Gestion des interruptions
  - Enregistrement de la valeur de l'horloge temps réel au moment de l'émission et de la réception

Configuration

- Tout doit être configuré à l'avance :
  - Il faut prendre en compte tous les scénarios de communication et notamment le cas « au pire »
  - Un module permet de configurer tous les nœuds depuis un serveur
- Configuration des slots :
  - Durée maximale
  - Offset
  - Slot normal, alterné, accolé
  - Les slots peuvent être associés à une application par un mécanisme d'identifiant et de priorité

Communication

- Utilisation de socket :
  - Linux pour du trafic non temps réel
  - Rtdm pour du trafic temps réel
- Des priorités peuvent être définies pour des données utilisant le même slot