



# Services pour la sûreté de fonctionnement dans les réseaux X-by-Wire

Nicolas Navet

► **To cite this version:**

Nicolas Navet. Services pour la sûreté de fonctionnement dans les réseaux X-by-Wire. Conférence Ingénierie Automobile 2003, 2003, Massy/France, 2003. <inria-00107703>

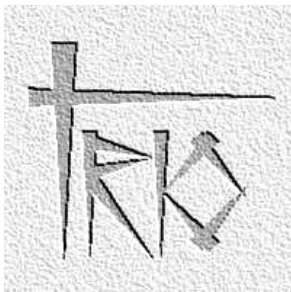
**HAL Id: inria-00107703**

**<https://hal.inria.fr/inria-00107703>**

Submitted on 19 Oct 2006

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



# Services pour la sûreté de fonctionnement dans les réseaux X-by-Wire

Nicolas NAVET

INRIA Lorraine - projet TRIO

<http://www.loria.fr/~nnavet>

Certaines images de cet exposé proviennent de :

- [1] Cours de P. Koopman (<http://www.ece.cmu.edu/~ece540/lecture/>)
- [2] Slides TTech (<http://www.tttech.com/> )
- [3] Normes TTP v0.5 et 1.0
- [4] Slides FlexRay WorkShop 2002

# Sûreté de Fonctionnement (1/2)

---

- **Définition** : « C'est l'ensemble des propriétés qui permettent aux utilisateurs d'avoir une confiance justifiée dans le service qui leur sera délivré »
- **Les attributs de SdF**:
  - ✓ **Fiabilité**
  - ✓ **Disponibilité**
  - ✓ **Sécurité**
  - ✓ **Intégrité**
  - ✓ **Maintenabilité**
  - ✓ **Confidentialité**

# Sûreté de Fonctionnement (2/2)

---

- Les entraves à la SdF:

faute  $\Rightarrow$  erreur  $\Rightarrow$  défaillance du système

- Les moyens d'obtention de la SdF voulue:

- ✓ **Prévention des fautes**

- ✓ **Tolérance aux fautes** : détection d'erreurs puis traitement des erreurs (recouvrement, confinement, redondance)

- ✓ **Prévisions de fautes**

# Présentation des protocoles TTP/C et FlexRay

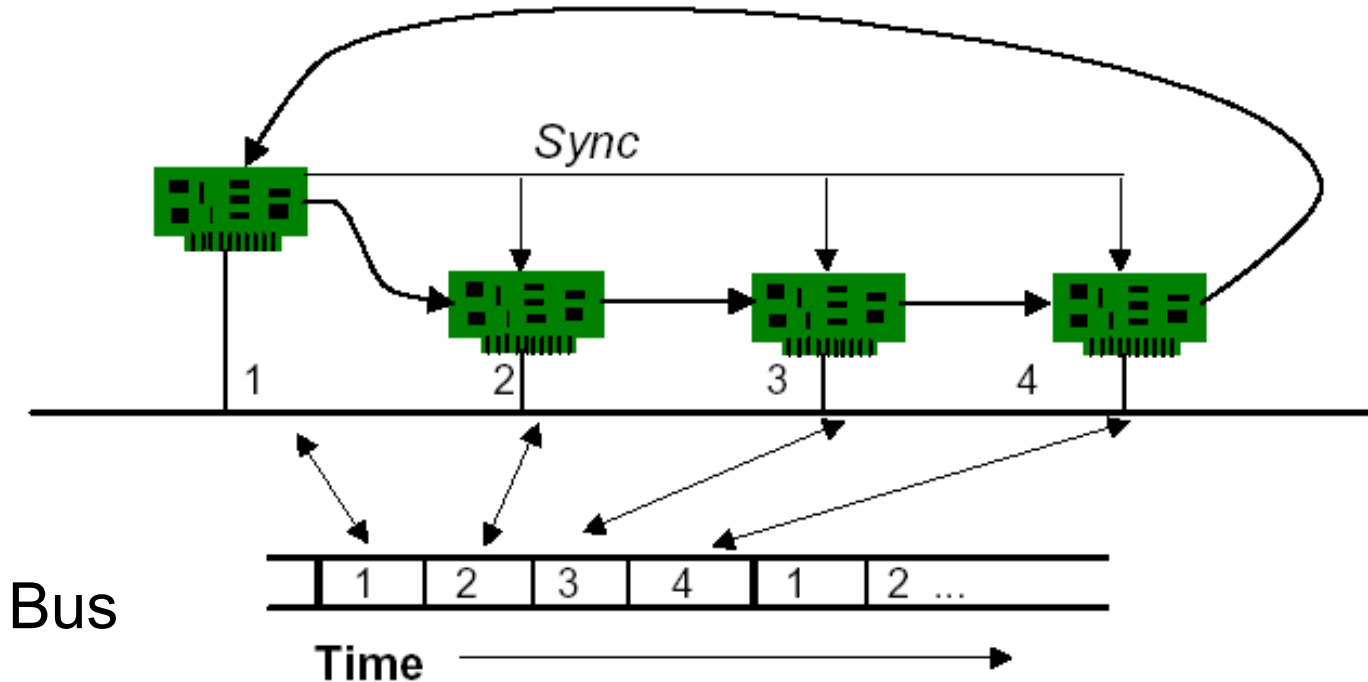
# TTP/C – Time Triggered Protocol

---

- Développé à la T.U. Vienne + TTTech
- 2 variantes : TTP/C et TTP/A
- Objectifs techniques:
  - Déterminisme
  - Tolérance aux fautes
  - Favoriser la « composabilité »
  - Support des changements de mode de marche

⇒ un bon candidat pour le X-By-Wire ..

# TPP/C – MAC de type TDMA



- Un **slot** est un intervalle de temps durant lequel une station émet un message
- Un **round TDMA** est une séquence de slots t.q. chaque station parle exactement 1 fois

# TTP/C – Implications du protocole MAC

---

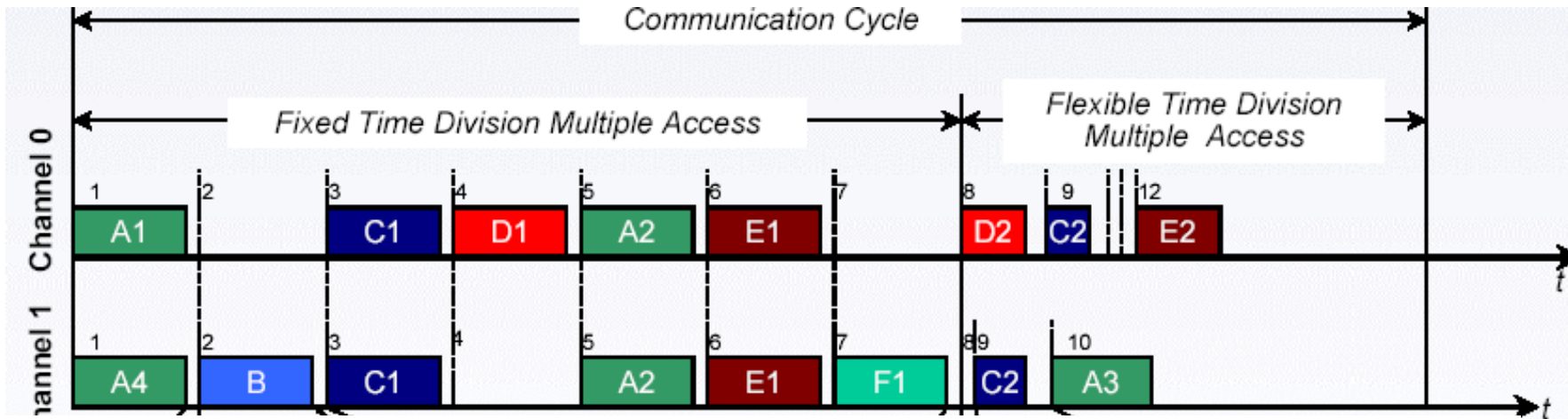
Temps de réponse borné et « heart-beat » mais:

- Perte de bande passante !
- Nécessité de micro-contrôleurs puissants
- Contrainte de temps maximum:
  - Si une station émet une seule donnée, le rafraîchissement ne peut être plus fréquent que le temps d'un round
  - Si une station émet plusieurs données, le rafraîchissement ne peut être plus fréquent que 2x le temps d'un round

**Ex:** contrainte de 5ms - réseau à 500kbit/s avec 200 bits par trames - au plus 12 trames (6 FTUs redondantes) ou 6 trames si la station émet 2 données.

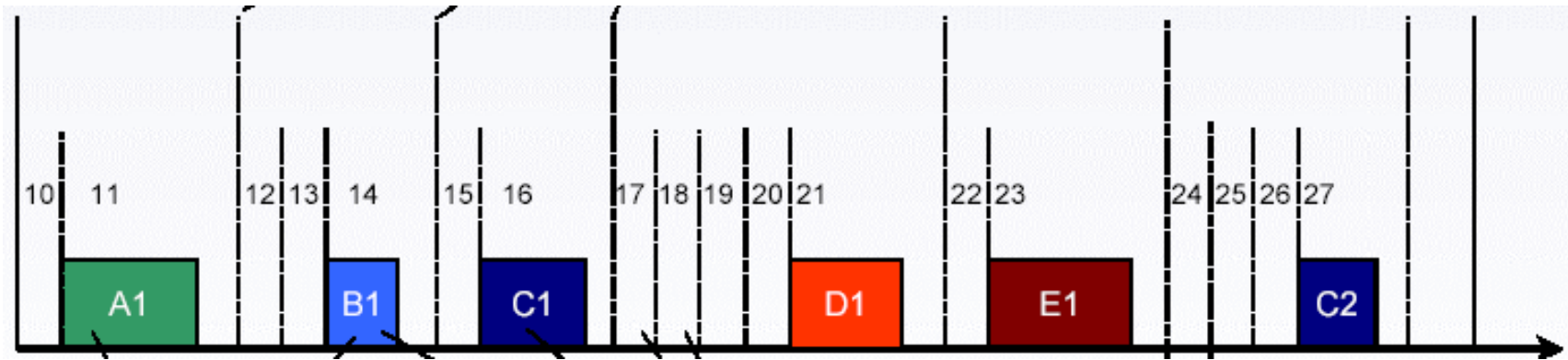


# FLEXRAY – MAC de type TDMA + FTDMA



- 3 modes de fonctionnement: statique pure, dynamique pure, mixte statique/dynamique
- Partie statique: les slots ont tous la même taille ( $\neq TTP/C$ )
- Partie statique: une même station peut obtenir plusieurs slots par cycle (jusque 16,  $\neq TTP/C$ )
- Partie statique: des slots peuvent être laissés libres pour des extensions futures ( $=TTP/C$ )

# FLEXRAY – trafic dynamique (F-TDMA)



- Chaque station possède une ou des priorités uniques sur l'ensemble du système
- Des transmissions successives de la même trame peuvent être de tailles différentes
- Pas de retransmission si erreur ( $\neq$  CAN)
- Sous certaines hypothèses sur le trafic, il est possible de calculer des pires temps de réponse (= CAN)

# **Caractéristiques / Services influant sur la Sûreté de Fonctionnement**

Analyse des protocoles selon le modèle:

- Couche physique
- Couche Liaison de Données
- Couche Application

# Niveau Couche Physique

---

- **Support de transmission** : robustesse aux EMI, résistance aux torsions ...
  - rien n'est imposé par les 2 protocoles
- **Redondance des canaux**
  - TTP/C: redondance sur tout le réseau, FlexRay : redondance partielle possible
- **Topologie** : bus, étoile ou multi-étoiles
  - grande souplesse pour les 2 protocoles
- **Technique de codage**
  - Dans TTP/C v1.0 rien n'est imposé, NRZ pour FlexRay

# Niveau Liaison de Données (1/2)

---

- **Détection d'erreurs de transmission / correction d'erreurs**
  - CRC avec distance de Hamming de 6 pour les 2 protocoles
- **Retransmission automatique en cas d'erreur de transmission**
  - non pour les 2 protocoles (!= CAN), possibilité d'utiliser la partie dynamique pour FlexRay
- **Détection d'erreurs protocolaires : erreur de communication, de synchronisation, de l'application**
  - oui pour les 2 protocoles, + efficace pour TTP/C car signalement d'erreurs par les autres stations

# Niveau Liaison de Données (2/2)

---

- Temps de réponse / giges connues
  - oui avec les 2 protocoles
- Acquittement des données
  - TTP/C oui (différé), rien de prévu pour FlexRay
- Gardien de bus: respect des caractéristiques d'émission, «babbling idiot» avoidance
  - oui pour les 2 protocoles

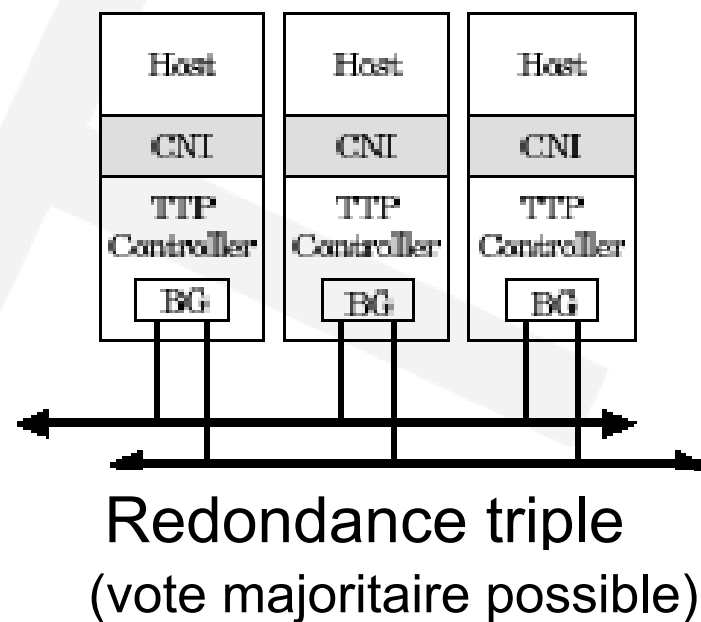
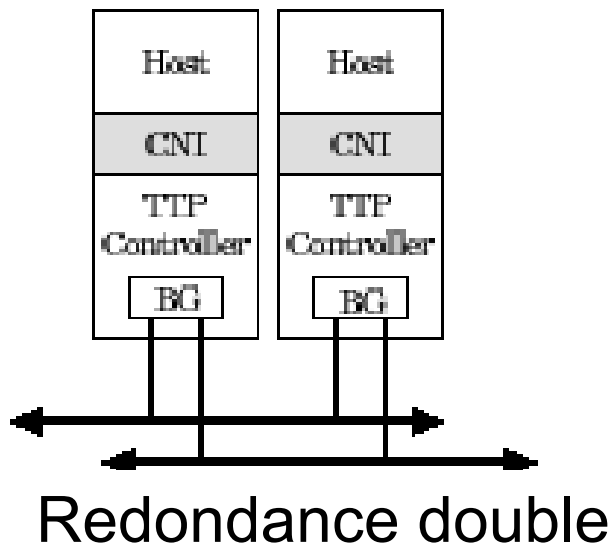
# Niveau Couche Application (1/2)

---

- Synchronisation sur une horloge globale
  - oui pour les 2 protocoles
- Support des changements de mode de marche
  - TTP/C oui, rien de prévu pour FlexRay
- Gestion des modes de veille
  - TTP/C non, FlexRay oui
- Support de la redondance calculateur
  - TTP/C oui mais ... , FlexRay non mais possible partiellement

# Support de la redondance calculateur

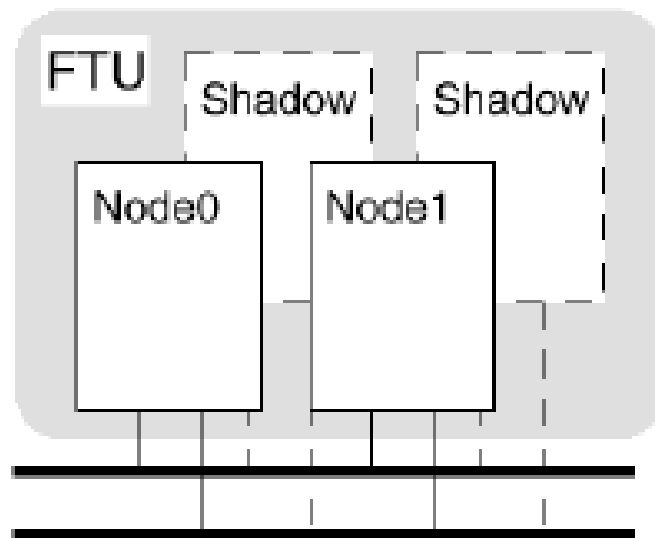
- **FTU** (Fault Tolerant Unit) = ensemble de stations qui effectuent exactement les mêmes actions





# FTU: 2 types de redondance

- Node « fantôme » (shadow SRU) : émet dans les slots d'une station active lorsque celle-ci devient défectueuse - ne possède pas de slots propres



- Node « réplique »: possède un slot propre

# FTU: qu'en attendre ?

---

- Protection contre:
  - disparition d'une station (crash, déconnexion..)
  - des transmissions corrompues par des EMI
  - des erreurs de mesure (capteurs) ou de calcul
  - ...
- Sous l'hypothèse d'une défaillance unique (hypothèse de conception de TTP/C) :
  - une redondance double assure protection dans « le domaine temporel »
  - redondance triple assure en plus une protection dans « le domaine des valeurs »
- **Problème TTP/C** : « history-state » lors de la réintégration (pas de trafic dynamique)
- **Problème FlexRay**: rien de prévu pour stations fantômes

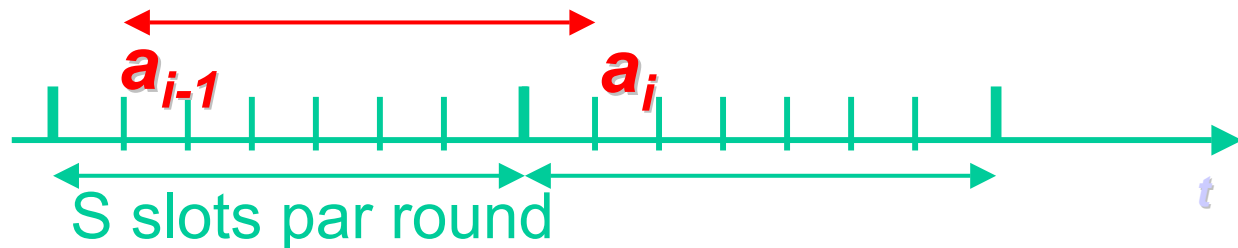
# Niveau Couche Application (2/2)

---

- **Connaissance de la vivacité des stations / évitement de cliques** (= ensembles de stations ayant une vision  $\neq$  des stations qui fonctionnent correctement)
  - **TTP/C oui**
    - Vivacité des stations: vecteur de Membership
    - Algorithme d'évitement de cliques  
mais règle de la majorité
  - **FlexRay non ..** mais implémentation éventuellement possible au niveau applicatif

# TTP/C : la règle de la majorité

- **Principe:** pour éviter la formation de cliques, **déconnexion des stations « minoritaires »**
- **Mécanisme:** avant d'émettre, une station vérifie que dans le dernier round ( $S$  slots), le nombre de messages correctement émis est supérieur au nbre de messages incorrects, sinon déconnexion (« freeze »)



- En cas d'erreurs de transmission multiples: si une station « freeze » alors les stations s'arrêtent une à une ..

# Conclusions – TTP/C vs FlexRay

---

## ■ TTP/C :

- + **Nombreux services pour la SdF** (mode de marche, redondance, membership, clique avoidance,...)
- + Visiblement conçu pour la certification
- Comportement en dehors des hypothèses de fautes !? Ces hypothèses sont-elles les bonnes pour l'automobile ??
- Flexibilité / incrémentalité faible

## ■ FlexRay :

- + Conçu spécifiquement pour l'automobile (réutilisation soft. développé pour CAN, mode veille,...)
- + Flexibilité (trafic dynamique, redondance non-obligatoire, ...)
- **Peu de fonctionnalités liées à la SdF** (redondance, membership)
- Validation du protocole !

# Références

---

- B. Gaujal, N. Navet, *Maximizing the Robustness of TDMA Networks with applications to TTP/C*, INRIA RR-4614, 2002. Disponible à l'adresse <http://www.loria.fr/~nnavet>
- TTA Group, *TTP/C specification v1.0*, Juillet 2002.
- Présentations effectuées lors du FlexRay Workshop 2002. Disponible sur le site <http://www.flexray.com>
- J.-C. Laprie, *Guide de la sûreté de fonctionnement*, Cépadués Editions, 1995.