Exposé FIMA

22 janvier 2009

Réseaux de communication et sûreté de fonctionnement enjeux, problématiques, approches

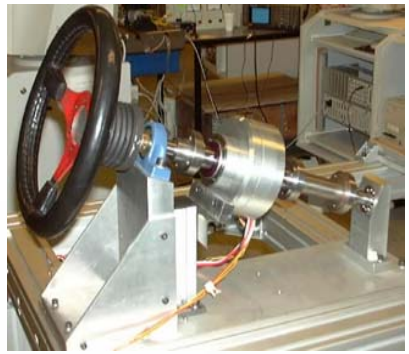
Jean-Marc THIRIET, UJF (Grenoble Universités)
GIPSA-Lab (UMR 5216)

Plan

1. Enjeux & problématique
2. Réseaux
3. Réseaux et sûreté de fonctionnement
4. Réseaux et systèmes
5. SdF de NCS

1. Enjeux

Niveau de sûreté (FMDS/RAMS) d'un système à base de réseaux, réseaux filaires



X by wire, steering by wire

- Fonction direction (steering by wire)
  - Probabilité que le véhicule ne tourne pas lorsque c'est demandé
  - Probabilité qu'il tourne de manière intempestive
- Evaluation difficile
  - Réseau plus complexe qu'un ensemble de liaisons point à point
  - Réseau plus complexe qu'un système à retard
  - Interaction Réseau-systèmes

Problématique : Sdf de systèmes à base de réseaux, communications sans fil

1er véhicule piloté

X by wire, brake by wire

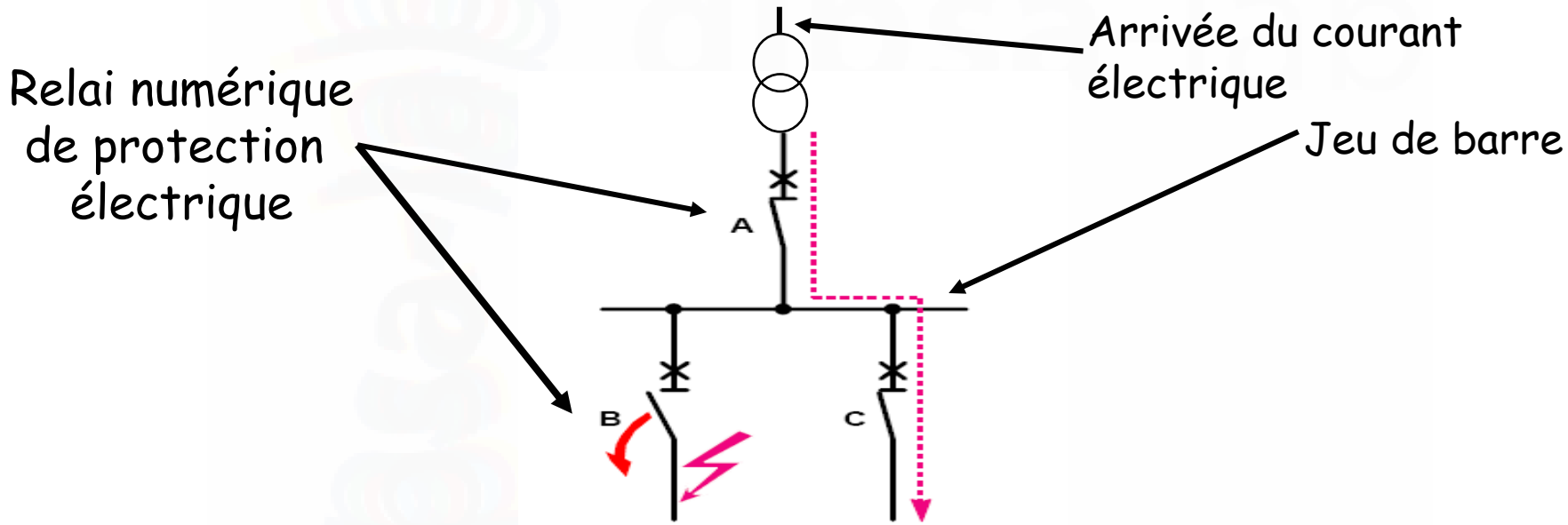
2ème véhicule suiveur

Conduite automatisée (train virtuel)

- **Fonction freinage**
  - **Premier véhicule**
    - Probabilité que le véhicule ne freine pas lorsque c'est demandé,
    - Probabilité qu'il freine de manière intempestive
  - **Second véhicule**
    - Probabilité qu'il reçoive l'information de freinage du premier véhicule si tout est correct pour le premier véhicule
    - ...

Système critique

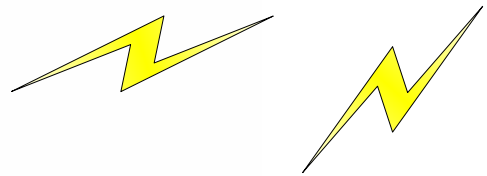
Sélectivité logique, installation de puissance électrique

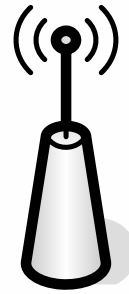


Perturbation en B, envoi d'une info en A pour éviter que A ne s'ouvre

Système embarqué (réseau filaire embarqué + réseau sans fil distant) à dynamique forte

- Drone-hélicoptère
- Définition de la mission
  - Dynamique faible (déplacement en « ligne droite »)
  - Dynamique forte (ex : slaloms entre des arbres)
  - Environnement de communication perturbé (perturbations e.m., arbres)

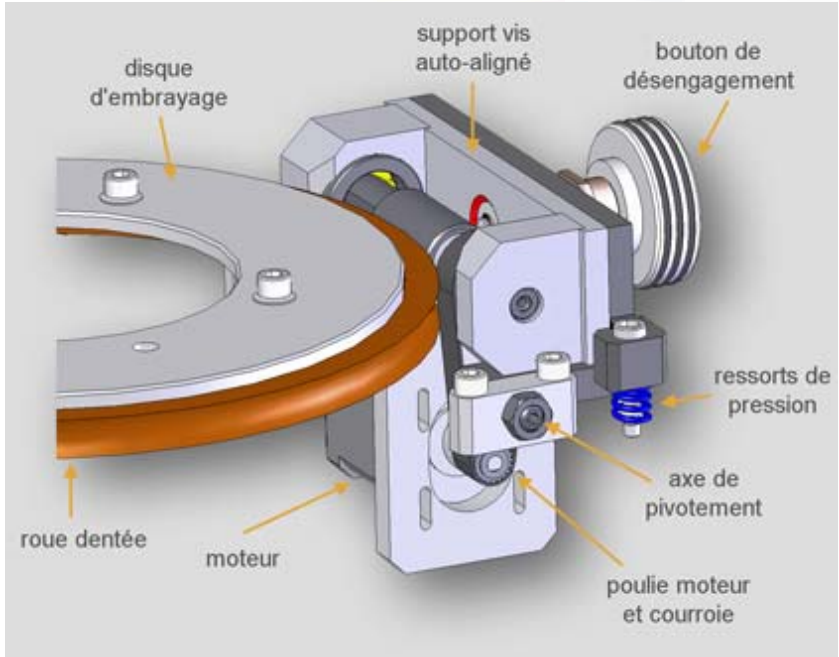




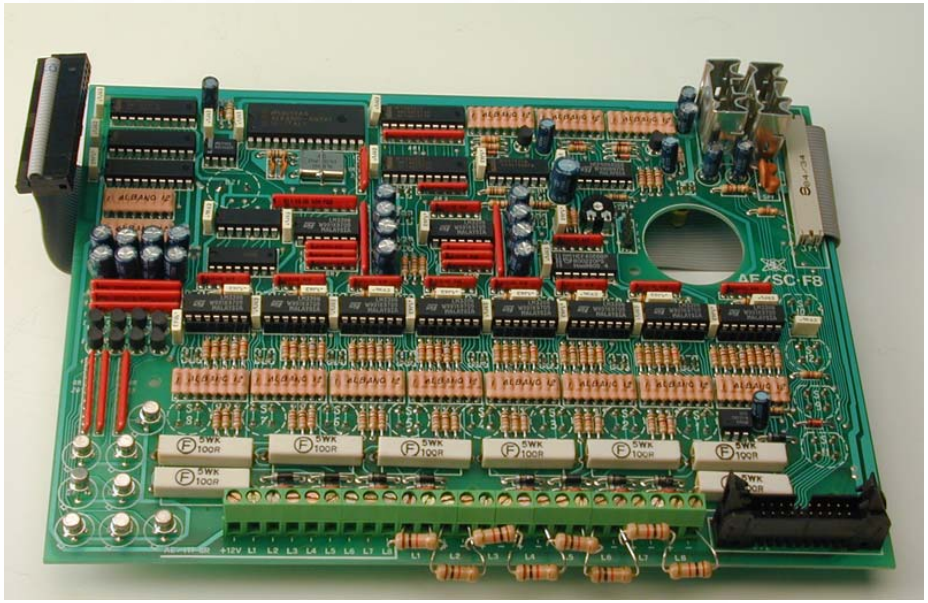
Problématique

Sûreté de fonctionnement

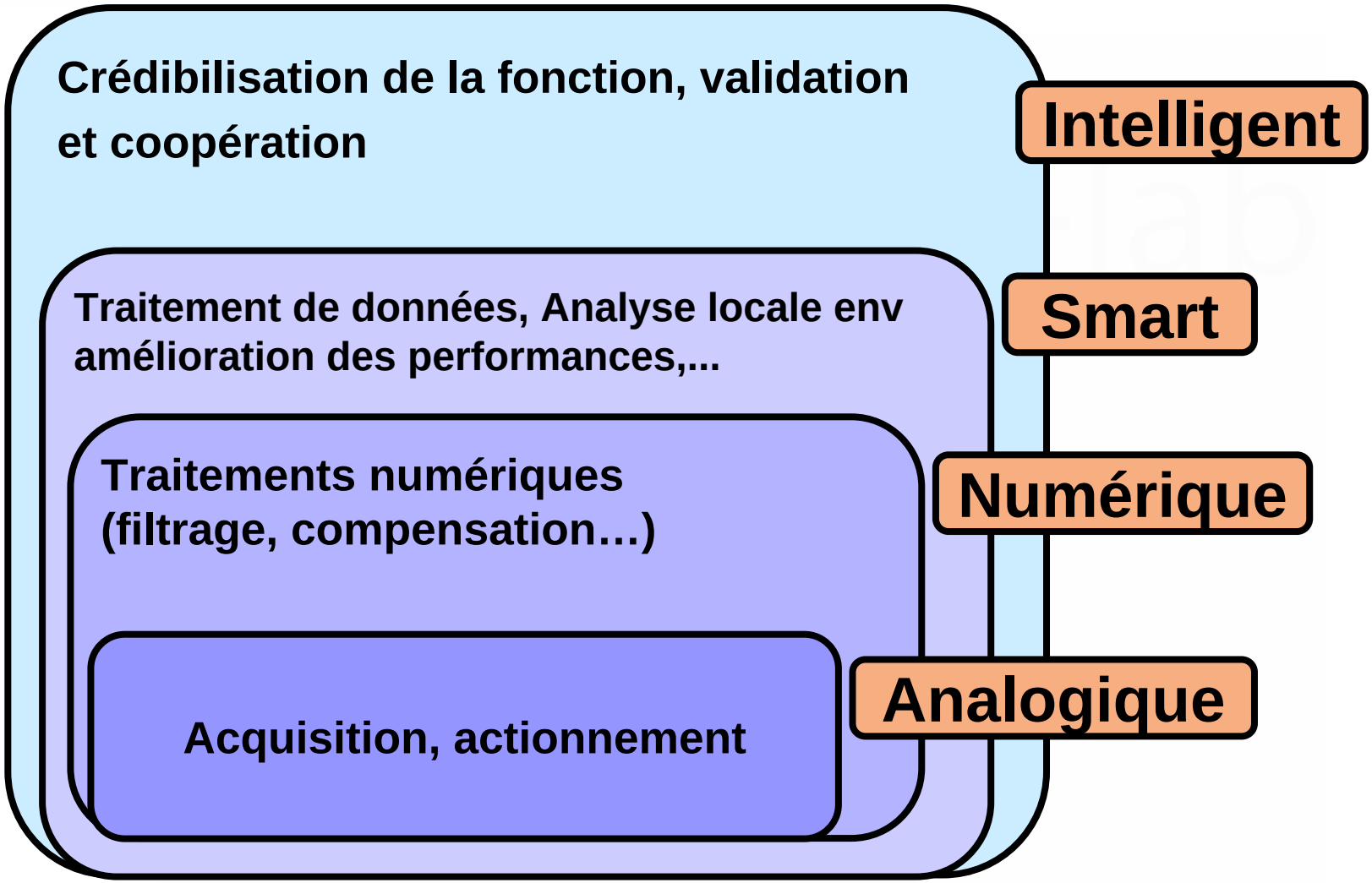
- Systèmes mécaniques



- Systèmes électroniques

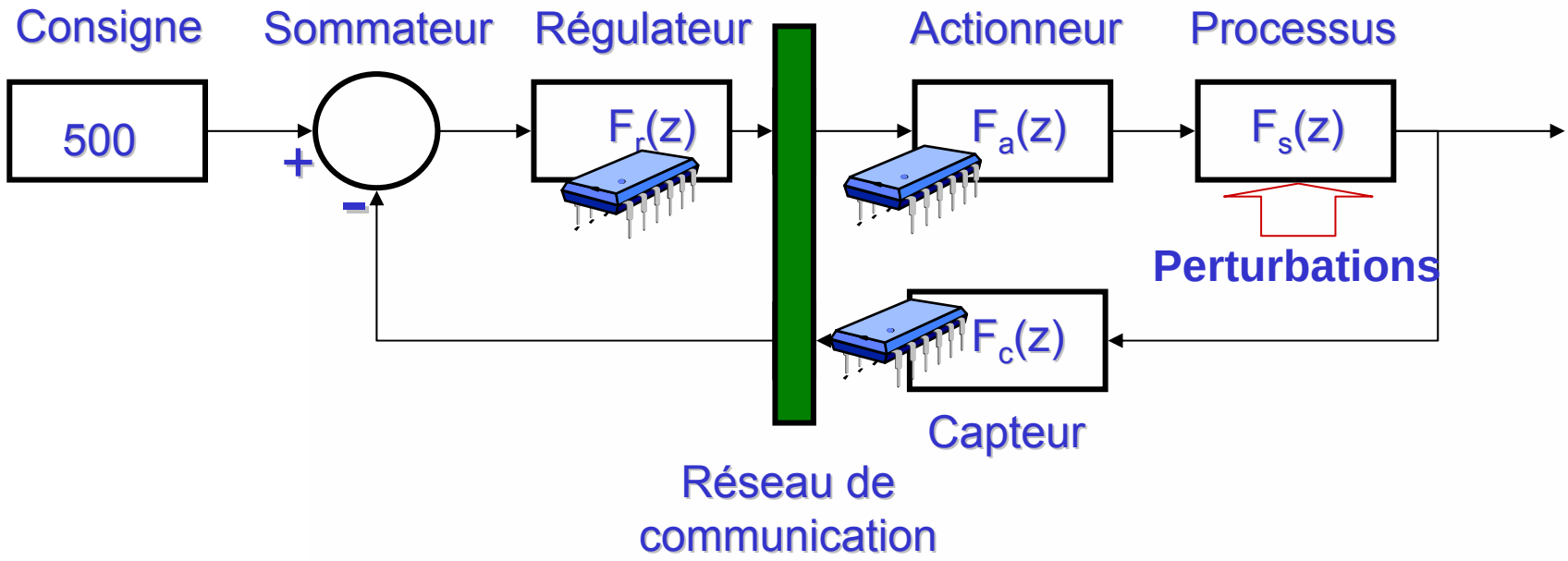


Concept d'instruments intelligents



- Intelligence vs. Complexité => conséquences sur la SdF

Système commandé en réseau
Système NCS (Networked Control System)



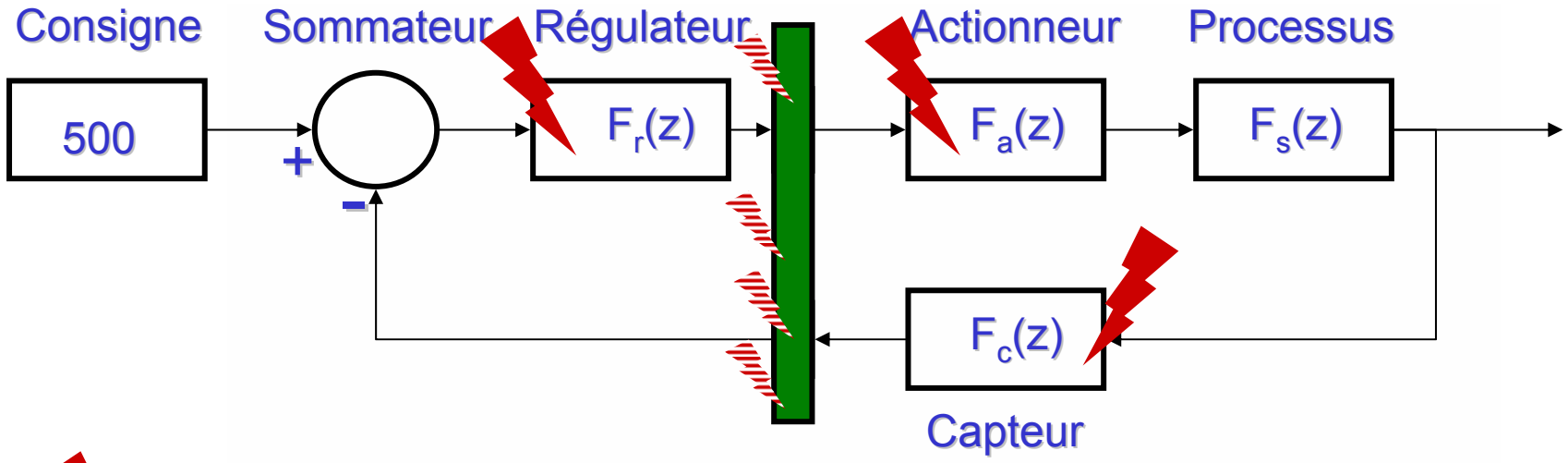
1. Composants continus/échantillonnés
2. Composant à événements discrets
3. Influence du réseau
   1. retard de transmission
   2. gigue
   3. perte d'information

→ Système hybride

→ Système à retard

Analyse par simulation

Intégration des défaillances



Modes de défaillance

- continus/échantillonnés
- à événements discrets

Echelles de temps

-Vitesse (taux de modulation, débit) du réseau

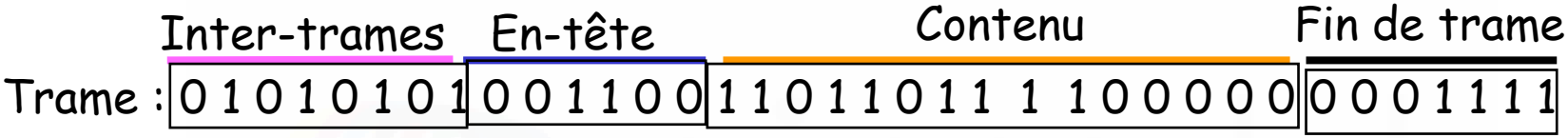
-Constante de temps du système

-Temps entre défaillances

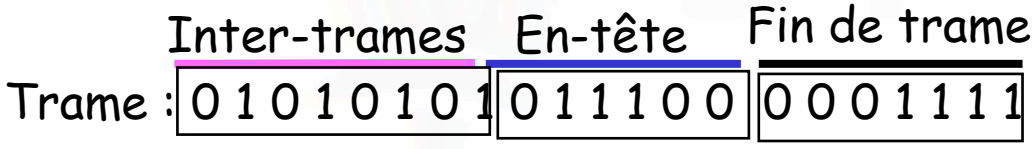
2. Le réseau filaire et non filaire…

Trames, topologie

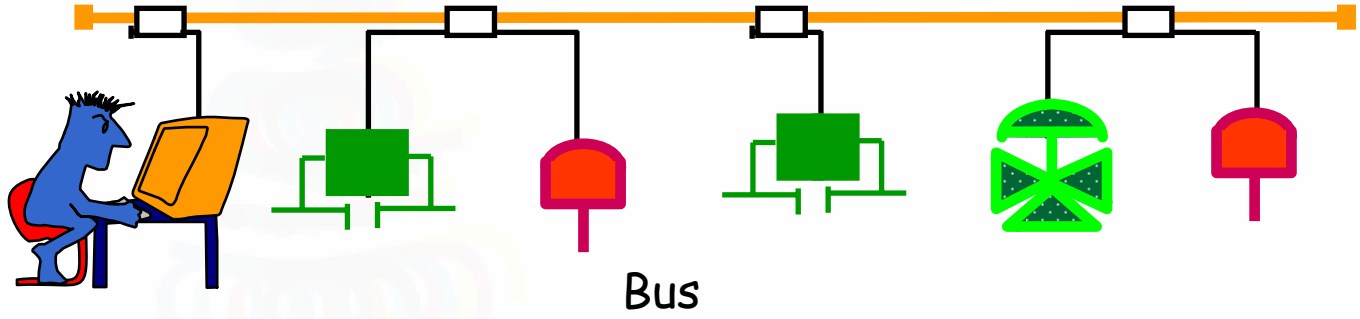
-Trames de données



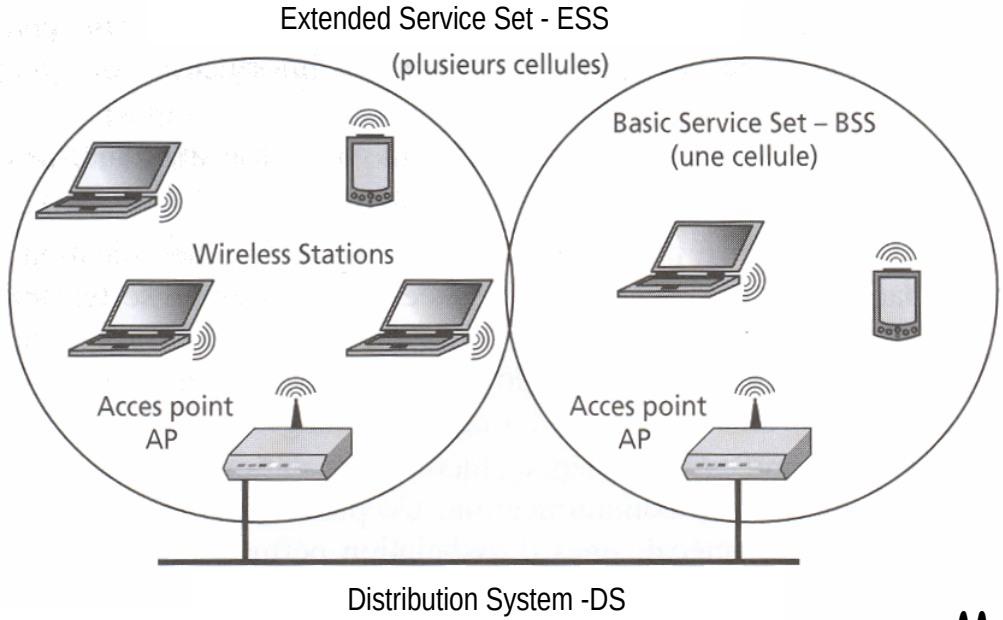
-Trames de service/contrôle (demande envoi, accusé de réception, routage…)

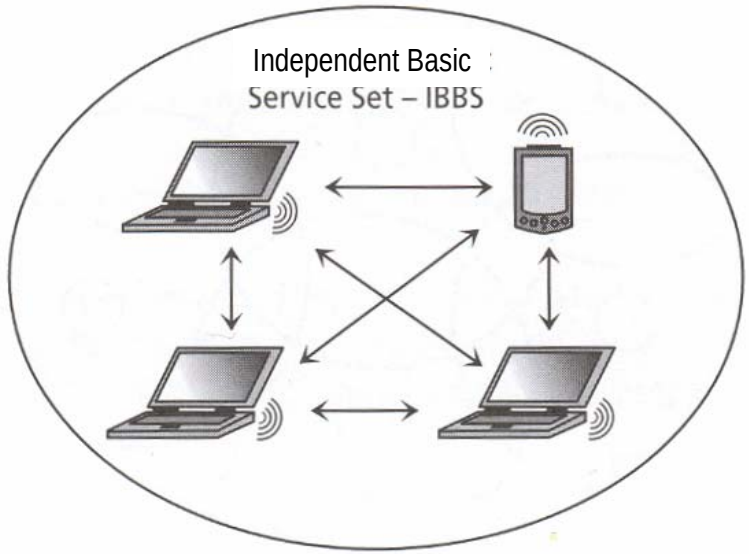


TOPOLOGIE



Topologies de réseaux sans fil





Mode infrastructure

-Plusieurs cellules

-Les AP (point d'accès) sont reliés via un réseau câblé (DS, Distribution System)

Architecture dynamique : A chaque instant, des machines peuvent entrer ou sortir du réseau

Mode ad hoc

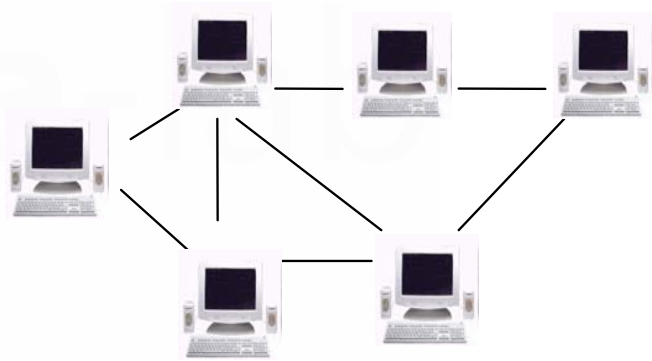
-Stations communiquant entre elles sans passer par un point d'accès

-Réalisation rapide de communications entre deux stations sans fil

-Pour pouvoir fonctionner sur un réseau étendu, ce mode doit être associé à un protocole de routage

Modes d'accès : accès aléatoire

- CSMA/CD (Carrier Sense Multiple Access /Collision Detection)
  - Carrier Sense : écoute de la porteuse
  - Multiple Access : plusieurs machines peuvent émettre simultanément (Accéder librement au bus, dès que le médium est libre sans autorisation préalable)
    => risque de collision

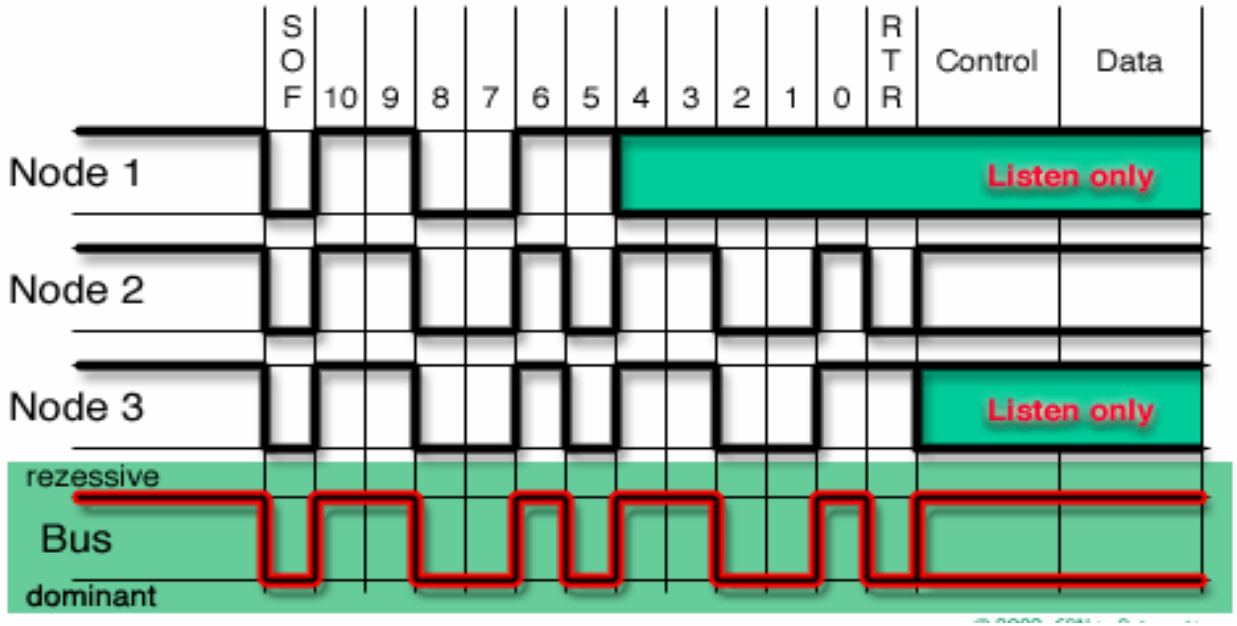


  - en cas de collision :
    1. émission d'une séquence de brouillage
    2. après un délai : nouvelle tentative
    3. abandon après trop d'échecs
  - Collision Detection : Détection des erreurs de collision et traitement (protocole probabiliste, pas de priorité)
    - Ex sur Ethernet, chaque machine émet quand elle veut

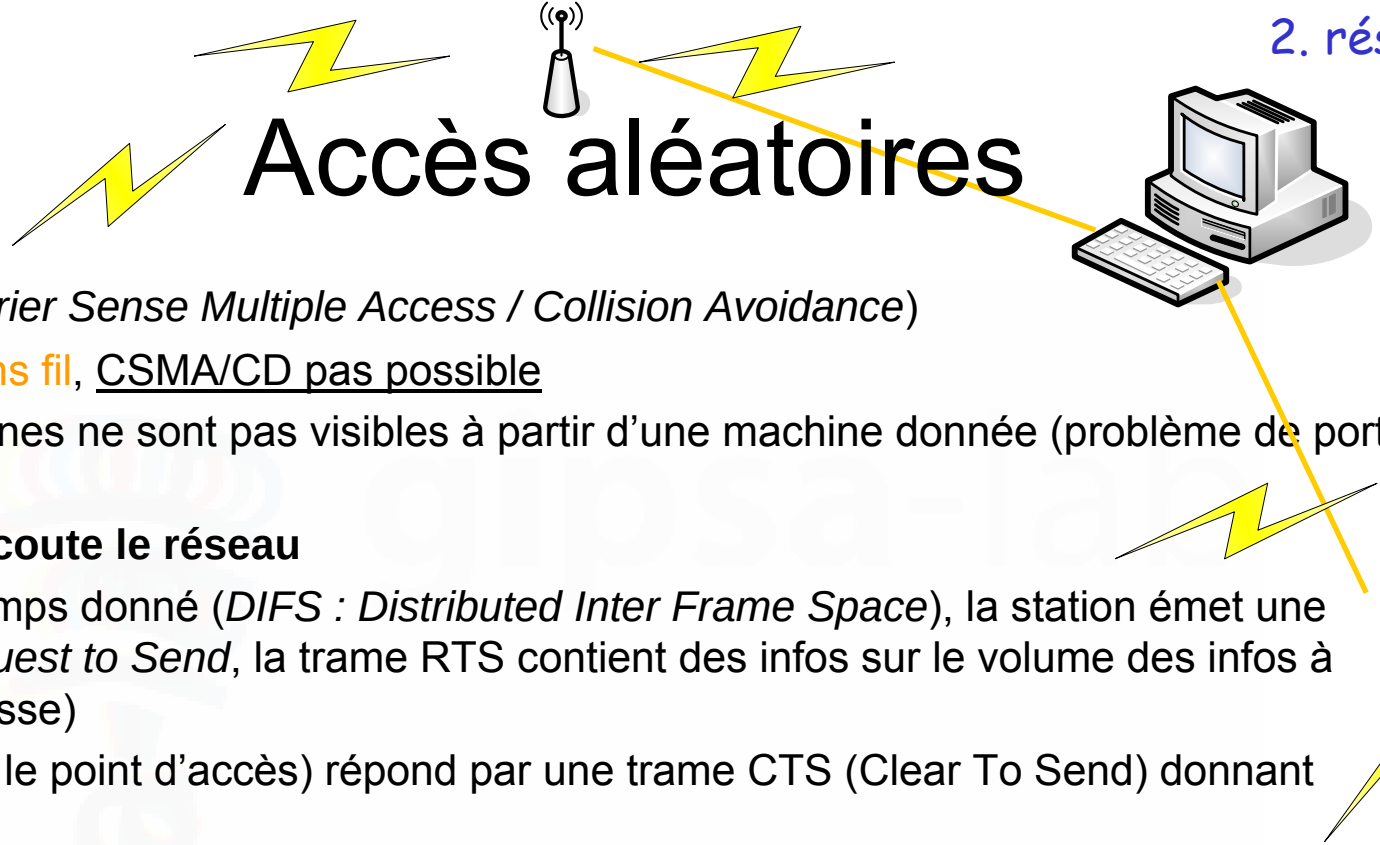
CSMA/AMP
Arbitration by Message Priority

Ordonnancement des messages en fonction de leur priorité

(ex : réseau CAN, Controller Area Network),



Accès aléatoires



- CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*)

Pour les réseaux sans fil, CSMA/CD pas possible

Car toutes les machines ne sont pas visibles à partir d'une machine donnée (problème de portée d'émission)

Station émettrice écoute le réseau

Si libre pdt un temps donné (*DIFS : Distributed Inter Frame Space*), la station émet une trame RTS (*Request to Send*, la trame RTS contient des infos sur le volume des infos à émettre et la vitesse)

Le récepteur (ou le point d'accès) répond par une trame CTS (Clear To Send) donnant l'autorisation

La station émettrice émet ensuite ses données

Lorsque toutes les données sont reçues, le récepteur envoie une trame ACK (*Acknowledgement*)

Les autres stations attendent pendant un certain temps (temps estimé de transmission du volume de données à la vitesse prévue)

- Collision Avoidance (Evitement de collision, ex : Wi-Fi 802.11, Zig-Bee 802.15.4)

Modes d'accès : accès contrôlé

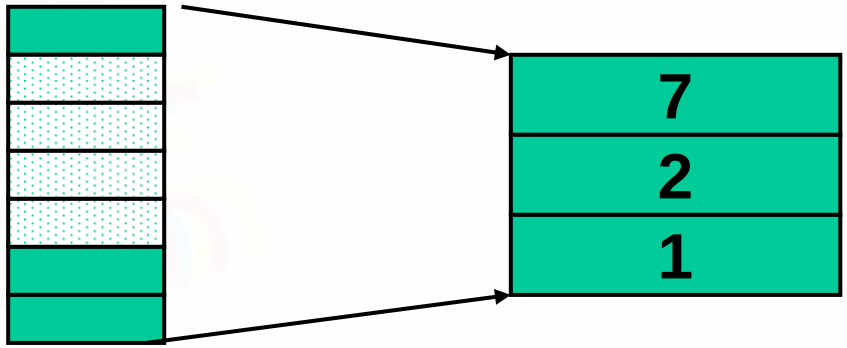
- Attente d'un droit de parole (éviter tout conflit)
  - gestion centralisée :
    1 station contrôlant les accès
  - gestion décentralisée :
    pl. stations contrôlant les accès
- Accès centralisé par "polling" :
  - Chaque abonné peut émettre à tour de rôle selon un ordre prédéfini.
  - Nécessité :
    1. d'un contrôleur des accès
    2. d'une table de scrutation
  - Ex : Réseau WorldFIP
- Accès décentralisé (ex : Token Ring)
  - Création d'un anneau logique dans lequel tourne un jeton
  - Droit de parole et contrôle de l'accès détenu par le possesseur du jeton
  - possession du jeton limité dans le temps
  - Ex : Réseau ProfiBUS

Cas du réseau de terrain

- Objectifs / contraintes / caractéristiques de la communication de terrain :
  - Informations de petite taille
  - Délais d'acheminement réduits
  - Coût des composants réduit
  - Solution généralement retenue :

Simplification du protocole

Simplification du modèle OSI :



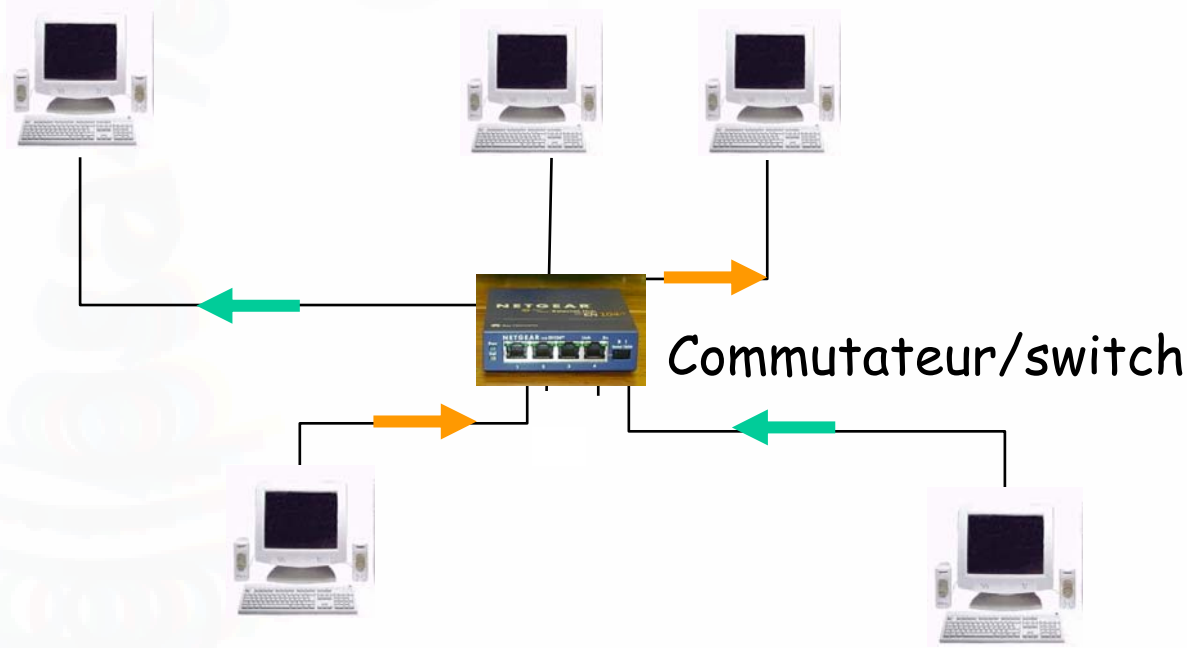
Application
Liaison
Physique

Exemples de réseaux de terrain

- WorldFip (réseau français, Alstom), déterministe
- CAN (automobile, avionique (Airbus)), Arbitration by Message Priority
- Profibus (réseau d'automates, automates et capteurs/actionneurs)
- ASI (réseau de capteurs-actionneurs)
- …

Ethernet commuté

- Ethernet = collisions
- Commutateur : délimite des zones « libres de collisions »



Réseaux de terrain vs. réseau ethernet commuté

- Ethernet : communauté universitaire
  - [J.D. Decotignie] (interopérabilité avec ethernet, utilisation d'éléments standards, réseau « multi-media »)
  - Origine : 10 Mb/s
  - FastEthernet : 100 Mb/s
  - GigaEthernet: 1 Gb/s
- CAN (Avionique/[FeT])
  - Compatibilité avec des éléments répandus dans l'industrie (notamment industrie automobile)
  - De 250 kb/s à 1Mb/s

Réseaux sans fil

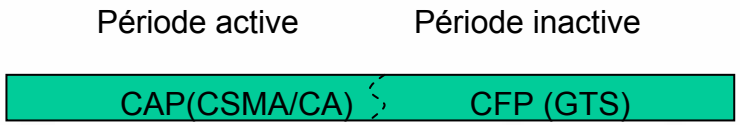
ZigBee	Wi-Fi
IEEE 802.15.4	IEEE 802.11b
2.4-2.4835 GHz (world), 902-928 MHz (USA) and 868-870 MHz (Europe)	2,4 GHz,
from 10 to 75m	46 m indoor, 92 m outdoor
250 kb/s (2.4 GHz), 40 kb/s (915 MHz), and 20 kb/s (868 MHz)	1, 2, 5.5, 11, 54 Mb/s
2^{16}=65536 Nombre de noeuds	32
100-1000+ Durée de vie des batteries	0,5-5
30 ms Temps pour trouver un nouveau nœud dans le réseau	Up to 3s
Reliability, low Power, low Cost	Speed, Flexibility
Home, building, industrial monitoring and control (for small, cheap microprocessors, low rate control networks)	Web, Email, Video. (for PCs, laptops, PDAs)

Réseaux sans fil longue distance

- Wimax
- IEEE 802.16
- Range: 5 GHz, 2-11 GHz, 10-66 GHz => d'autres fréquences (3,5 GHz – 2,6 GHz) pourraient être utilisées
- Distance : 50 km, practically 5 - 8 km
- Débits : pouvant aller jusqu'à 70 Mb/s
- Intérêt : Wide-Range
- Broadband access, "last mile" broadband connections
- Autre réseau sans fil grande distance : WRAN (Wireless Regional Area Network) IEEE 802.22

Réseaux sans fil et temps réel (temps critique)

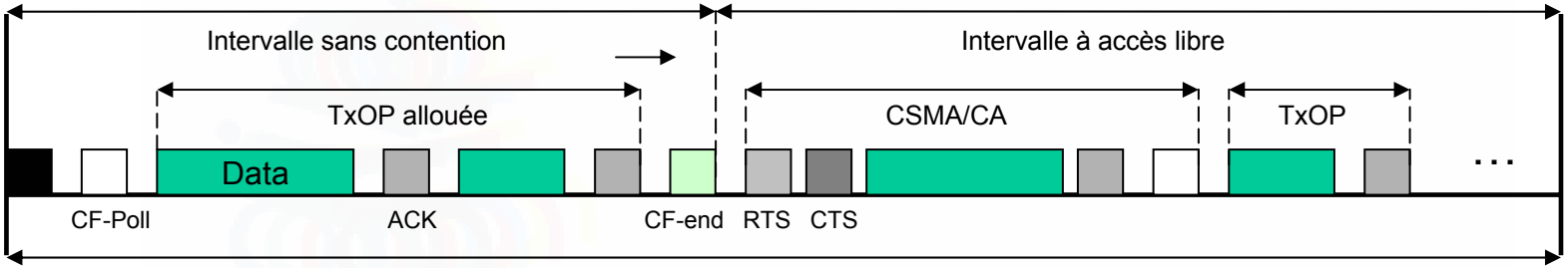
- Zig-Bee
  - Supertrames :



Supertrame

CAP (Contention Access Period) : tous les nœuds peuvent transmettre d'une façon aléatoire en respectant la durée d'un slot CSMA/CA
CFP (Contention Free Period) : Permettent de garantir l'accès au canal à un nœud pendant une durée déterminée en nombre de slots GTS
GTS (Guaranteed Time slots) : Ce sont des slots temporels dédiés (le coordinateur pourra allouer un ou plusieurs slots à un nœud en particulier pour offrir certaines garanties temporelles).

- Wi-Fi 802.11e



Supertrame

Conclusion sur les réseaux

- Qualité du protocole
  - %age du temps pour émettre des données
  - Besoin de réémissions ?
  - Trafic de service important…
- Déterminisme
  - impossible en sans fil
  - Nécessite un réseau « fermé »
- « perturbations »
  - Négligeable en filaire
  - Important en sans fil => besoin d'applications robustes au réseau…
    - Mise en place de redondances (multi-bursts, multi-canal, multi-stations…)

3. Réseaux et sûreté de fonctionnement

« Défauts » des réseaux

- Défauts réseaux
  - Retards : Certaine tolérance (gigue)
  - Pertes : (réémission, régénération, tolérances aux fautes)
    - [Kim, 1988]. CSD (control system deadline),
    - [Babak, 2003] [Zhang, 2001] stabilité des systèmes distribués en présence de pertes
  - Altérations
    - Détection de l'altération par code détecteur d'erreur
    - Correction d'erreurs (si code correcteur)
    - Fonctionnement tolérant aux fautes (reconstruction de la (des) donnée(s) manquante(s))
  - Désynchronisation (protocole d'horloge, horloge externe)
  - Perturbations électromagnétiques
  - Surcharge due au réseau partagé (protocole)

Retard

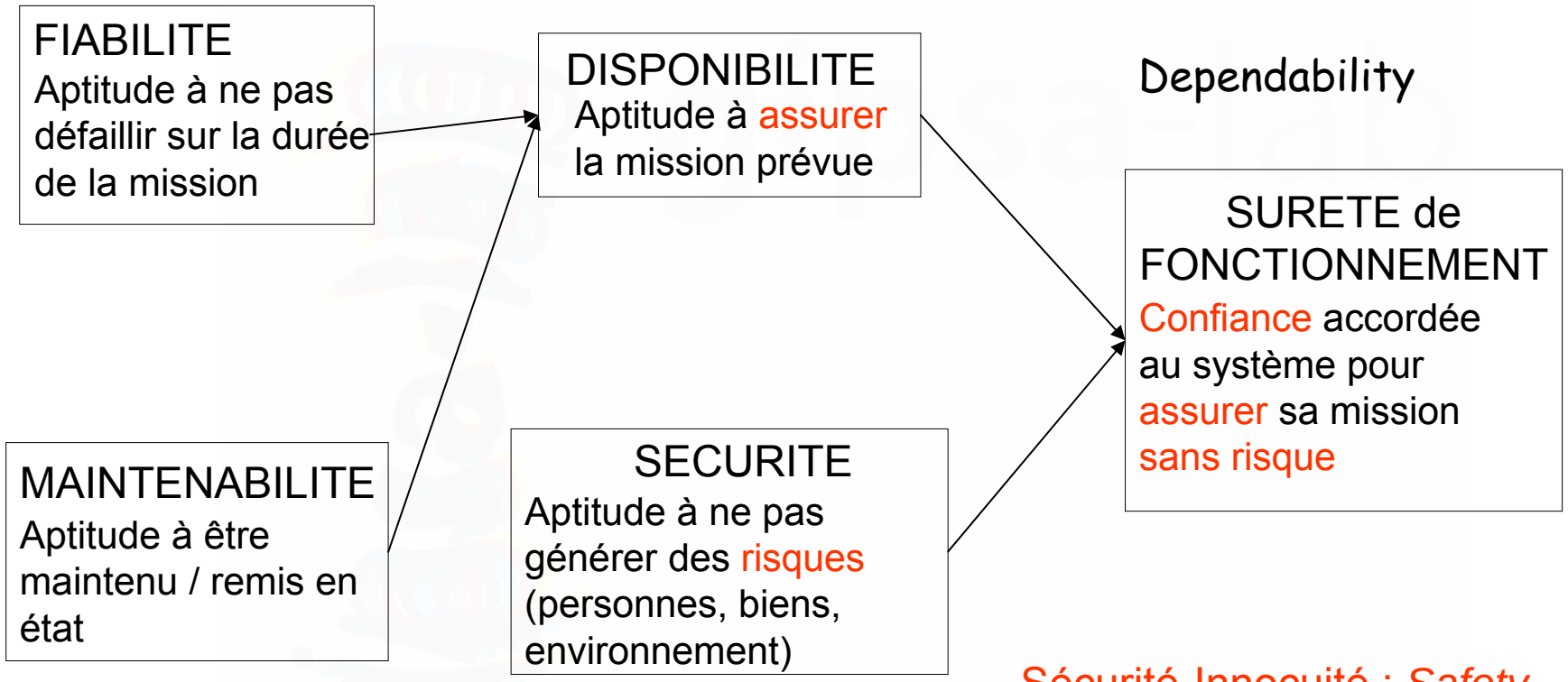
- Réseau déterministe (accès contrôlé)
  - Tâche 1 : tous les T=0,01 s.
  - Tâche 2 : tous les T=0,02 s.
  - Tâche 3 : tous les T=0,01 s.
- 1 3 2 1 3 1 3 2 1 3 1 3 2 1 3
  - Tâche 2 périodique
  - Tâches 1 et 3 périodiques avec de la « gigue »
- Retards dus
  - Aux temps de transferts
  - A la politique de synchronisation (time-driven, event-driven,…)
  - Au mode d'accès (aléatoire, contrôlé)
- Types de retards
  - Retard moyen (borné, non borné)
  - « pire » Retard (retard dans le pire cas)
- Réseau non déterministe (accès aléatoire)
  - Priorité
  - Réémission de tâches suite à la détection d'erreurs

Réseaux sans fil

- Même problèmes que les réseaux filaires +
- Perturbations électromagnétiques (plus sensible)
- Réseau pas toujours disponible (fonctionnement normal)
  - Non visibilité, retards dus aux réflexions (réception non directe)
  - Pas toujours « on » à cause de la gestion de l'énergie (système embarqué)
- Perturbations liées à la mobilité
  - Distance émetteur-récepteur
  - Obstacles entre émetteur et récepteur
  - Nécessité d'avoir du trafic de service (connexion, év. routage…)
- Topologie du réseau évoluant au cours du temps (stations mobiles, communication entre un mobile et plusieurs stations au sol), (hand-over, roaming)
  - CONSEQUENCES
- Diminution du débit
- Perte de la communication (perte « non négligeable » de trames)
- Plus grande sensibilité au "piratage"

Sûreté de fonctionnement

RAMS : Reliability, Availability, Maintainability, Safety



Sécurité-Innocuité : *Safety*
Sécurité-Intégrité… : *Security*

Niveau intégré de sûreté (*SIL*)

- Norme générique CEI-61508

Sécurité fonctionnelle des systèmes électriques / électroniques programmables relatifs à la sécurité

- SIL (*Safety Integrated Level*)

Prescriptions du système de sécurité et niveaux SIL correspondants		
SIL	Fonctionnement à la demande Probabilité moyenne de défaillance sur sollicitation Taux de défaillance par an	Fonctionnement en continu λ Taux de défaillance par heure
SIL4	$10^{-4} < PFDavg < 10^{-5}$	$10^{-8} < \lambda < 10^{-9}$
SIL3	$10^{-3} < PFDavg < 10^{-4}$	$10^{-7} < \lambda < 10^{-8}$
SIL2	$10^{-2} < PFDavg < 10^{-3}$	$10^{-6} < \lambda < 10^{-7}$
SIL1	$10^{-1} < PFDavg < 10^{-2}$	$10^{-5} < \lambda < 10^{-6}$

Réseaux de sécurité

- **Safety-Bus p**, un des premiers réseaux avec un objectif de sécurité
- 2 protocoles de sécurité basés sur les couches basses de CAN : **CANopen-Safety** et **TTP** (Time-Triggered Protocol),
- **FlexRay**, conçu pour des applications automobiles sûres de fonctionnement,
- ProfiBus qui est devenu **ProfiSafe**, grâce à son extension sécurisée,
- **ASI Safety at Work**, extension de sécurité du réseau de bas niveau ASI.

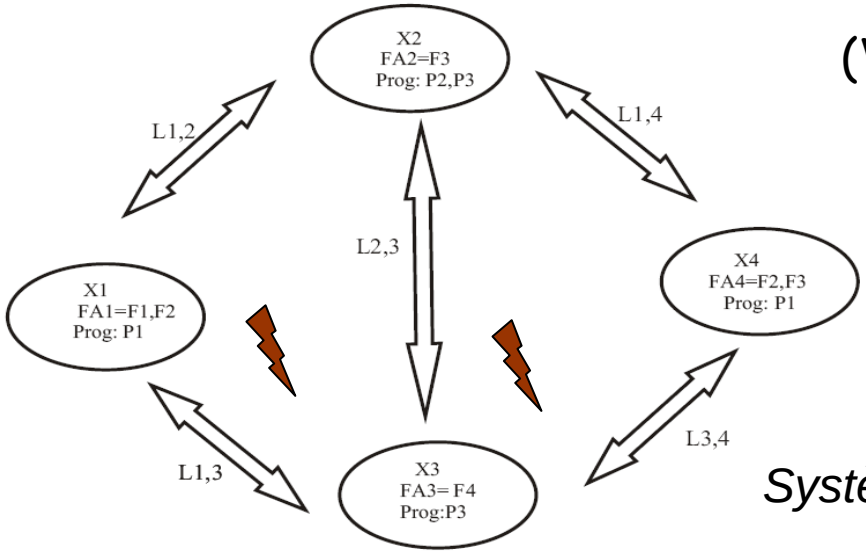
- Trames périodiques
- Redondances (câbles, transmission redondante, redondance hétérogène)
- Moniteur de sécurité (ex sur ASI) : Elément passif détectant les suites de 4 zéros consécutifs indiquant un problème
  - un utilisateur a déclenché un système de sécurité et pressé un arrêt d'urgence
  - des défauts ont été détectés sur le bus de communication ou sur l'un des composants
- Communication sécurisée entre des composants de sécurité (CRC, accusé de réception, vérification de la durée de transmission => trames spécifiques à la sécurité)

Sûreté de fonctionnement des réseaux

- Evaluation du réseau « seul »
  - Qualité de service de la communication
  - Sensibilité aux perturbations
- Réseau vu comme un « brin » de communication
- Réseaux vu comme plusieurs « brins » de communication « indépendants »

Intégration de la fonction communication dans l'étude de la fiabilité (système distribué : approches informatiques)

(Wang et al, 2002) et (Lin et al, en 2001)



$FA_1 = \{F_1, F_2\}$ $PRG_1 = \{P_1\}$ $FN_1 = \{F_1, F_2, F_3\}$

$FA_2 = \{F_3\}$ $PRG_2 = \{P_2, P_3\}$ $FN_2 = \{F_1, F_2, F_4\}$

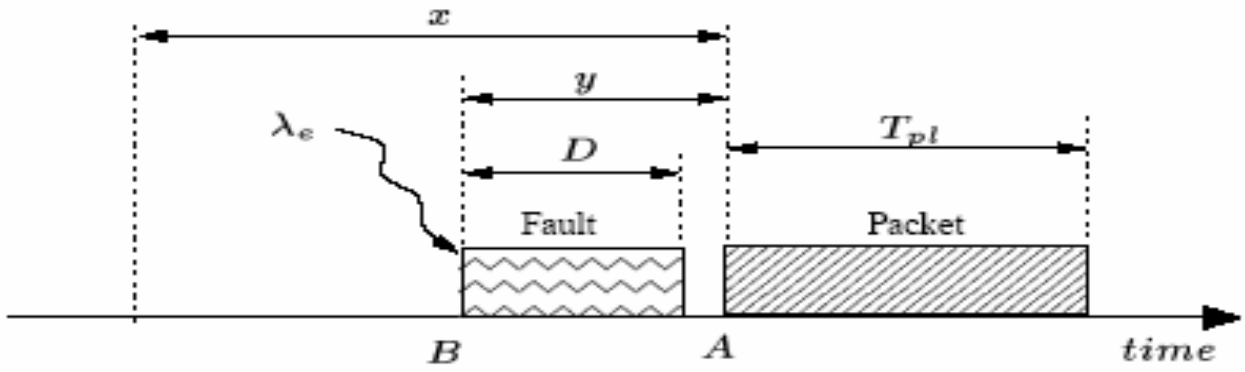
$FA_3 = \{F_4\}$ $PRG_3 = \{P_3\}$ $FN_3 = \{F_1, F_2, F_3, F_4\}$

$FA_4 = \{F_2, F_3\}$ $PRG_4 = \{P_1\}$

Système distribué avec 4 nœuds et 5 liaisons

- Chaque liaison possède deux états: état de marche ou de panne
- Taux de défaillance des liaisons indépendants et exponentiellement distribués
- Taux de réparation des liaisons indépendants et exponentiellement distribués
- Pendant une unité de temps, une seule liaison peut tomber en panne ou être réparée

Intégration de la fonction communication dans l'étude de la fiabilité (approches centrées réseau)



- (Tindell, 1997) temps de réponse en présence de fautes transitoires
- (Navet et al, 2000), (Portugal et al, 2002) probabilité qu'un message manque son délai
  - Un message qui manque son délai → la défaillance de la fonction communication
- [Portugal et Carvalho, 2001] : approche basée sur les chaînes de Markov pour évaluer l'indisponibilité de la fonction communication (fautes permanentes)

- **ces approches tiennent compte seulement de la fonction communication et ne prennent pas en compte l'application qui s'appuie sur ce réseau**
- **un point de vue sur la défaillance**

Conclusion sur la SdF des réseaux

- Approche orientée fonction de communication
- Donne la possibilité de mesurer le niveau de qualité du réseau
- Permet de certifier la communication (par ex : réseaux de sécurité)
- Ne prend pas en compte les interactions avec le système
  - Etat du système
  - Successions de défaillances (ex : bavardage d'un composant)
  - Taux de charge du réseau en fonction des sollicitations
  - Niveau de priorité (criticité) d'information à transmettre en fonction de l'état du système et/ou de son environnement

4. Systèmes et réseaux

4.1 Approches évaluation de la sûreté de fonctionnement

4.2 Approches co-design

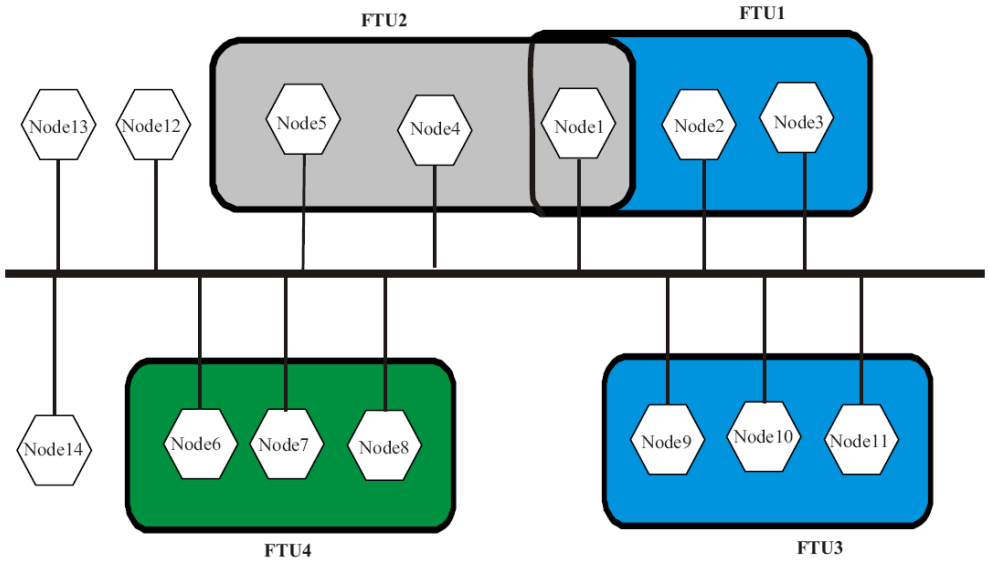
- Approches évaluation de la sûreté de fonctionnement
  - Modèle fonctionnel
  - Modèle dysfonctionnel

- Approches co-design

4.1.1 Systèmes en réseau

Réseau parfait

Comparaison des paramètres de la sûreté de fonctionnement pour plusieurs architectures d'un système distribué



[Pimentel et Salazar, 2002]

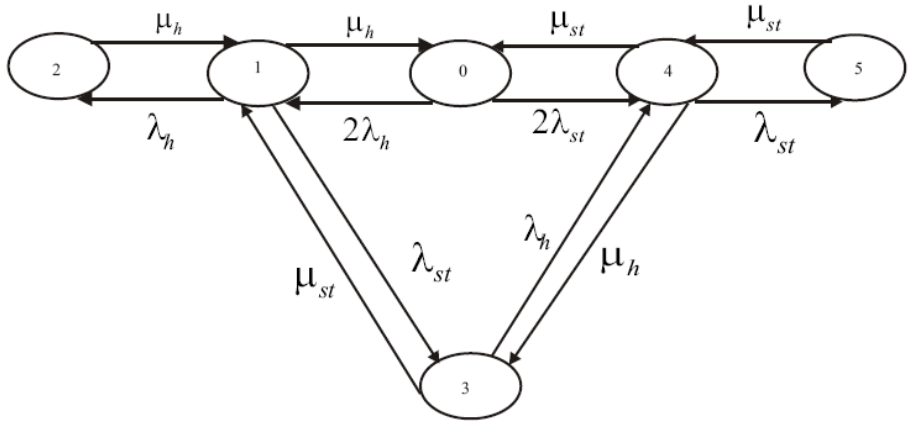
- Plusieurs composants appelés nœuds.
- Les nœuds groupés dans des unités appelées unités de tolérance aux fautes FTU
- une unité FTU est en bon fonctionnement si l'un de ses nœuds est en état de marche
- Le bon fonctionnement du système exige le bon fonctionnement de tous les FTUs (4 dans l'exemple)
- Les paramètres évalués sont la fiabilité et le temps moyen pour la première défaillance (*MTTFF - Mean Time To First Failure*).
- Les seules fautes considérées sont les fautes au niveau des nœuds, le réseau est considéré comme étant toujours fiable.
- L'approche est basée sur la modélisation par réseau de Petri stochastique et les résultats sont évalués en utilisant la simulation de Monte-Carlo

Approche basée sur les chaînes de Markov pour évaluer la disponibilité de tels systèmes

[Lai et al, 2002]

- Hypothèses :
- Tous les sites ont le même taux de défaillance matérielle suivant une distribution exponentielle de valeur moyenne.
- Tous les sites ont le même taux de défaillance logicielle suivant une distribution exponentielle de valeur moyenne.
- états considérés pour le matériel et pour le logiciel
  - (1) état de bon fonctionnement
  - (2) état de panne.

  Seules les fautes permanentes sont considérées.
- temps de réparation qui inclut le temps de détection de la défaillance et la réparation
  - loi exponentielle de valeur moyenne pour les composants matériels et pour le logiciel.
- Défaillances supposées indépendantes.
- Un site est en état de marche si le matériel et le logiciel associés sont aussi en bon état



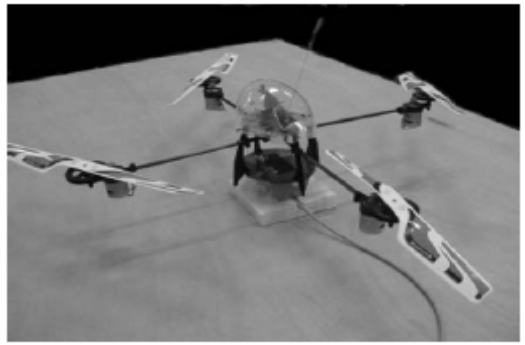
Etat 0 : état initial, tous les composants sont en bon état
Etat 1 : 1 matériel en panne, un site en marche
Etat 2 : 2 matériels en panne, système en panne
Etat 3 : 1 matériel en panne et 1 logiciel en panne, système en panne
Etat 4 : 1 logiciel en panne, 1 site en marche
Etat 5 : 2 logiciels en panne, système en panne

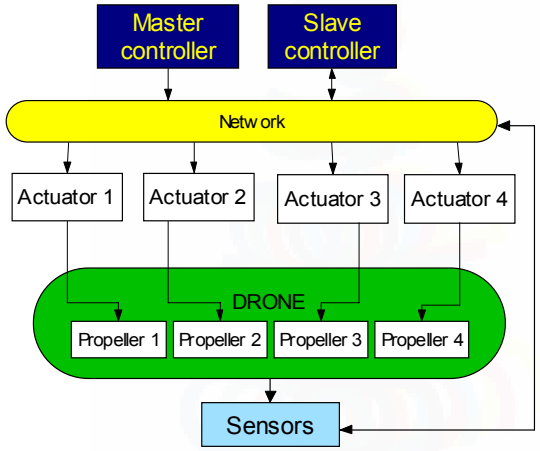
•systèmes à temps souple où les retards de l'envoi de l'information entre les différents composants n'affectent pas trop les performances de l'application

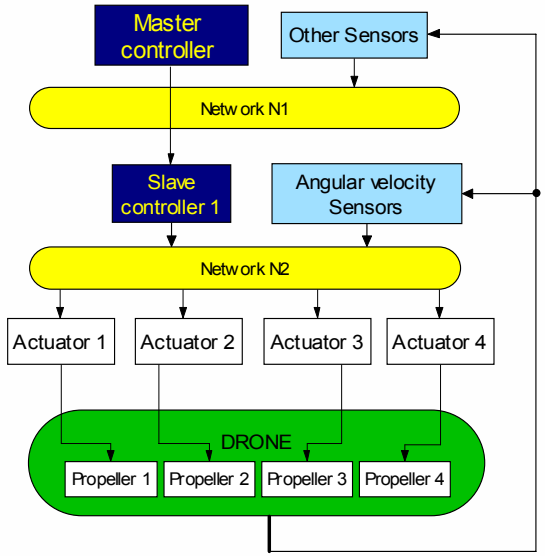
Composants partiellement redondants

[Galdun, 2008]

- Cascade control approach
  - Primary loop – drone control
  - Secondary loop – motors' angular velocity
- SR approach
  - Quasi-redundant controllers/nets
  - Single failure rate change





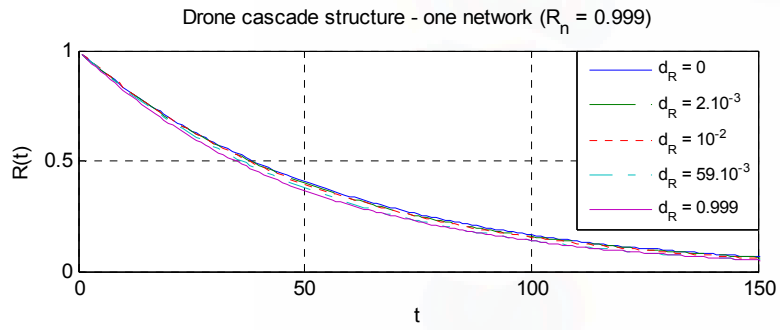


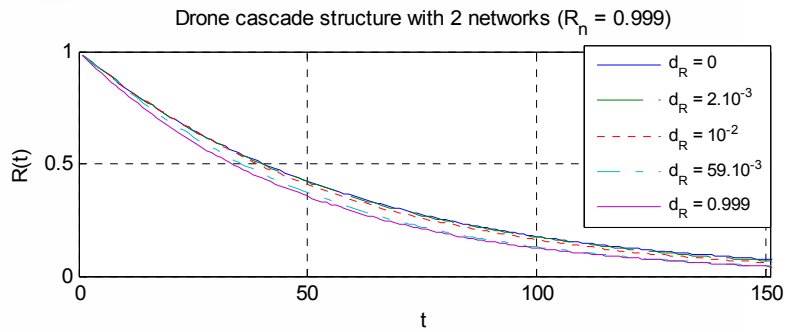
Composants partiellement redondants

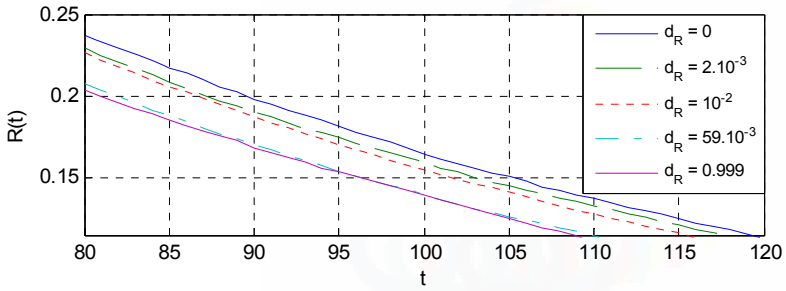
Increased nominal failure rate $\lambda_n = 0.001$ by value d_R	MTTFF [*Tu*] Drone – one net	MTTFF [*Tu*] Drone - two nets
$\lambda' = \lambda_n + d_R =$ 0.003 $(d_R = 2.10^{-3})$	53.81 (8%)	56.2 (18%)
0.011 $(d_R = 10^{-2})$	53.2 (7%)	54.27 (14%)
0.06	50.49	49.18
1 (without redundancy)	49.66	47.6

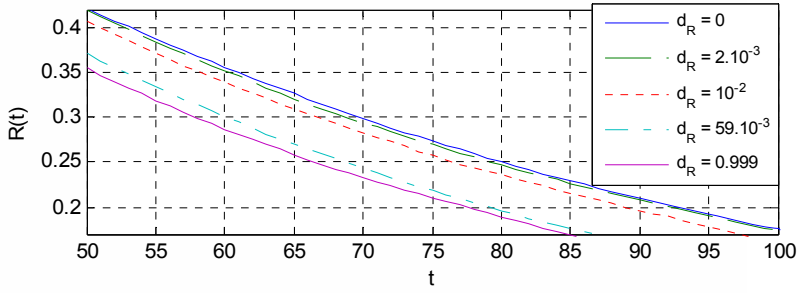
[Galdun, 2008]

Redondance partielle
-Composant
-Réseau





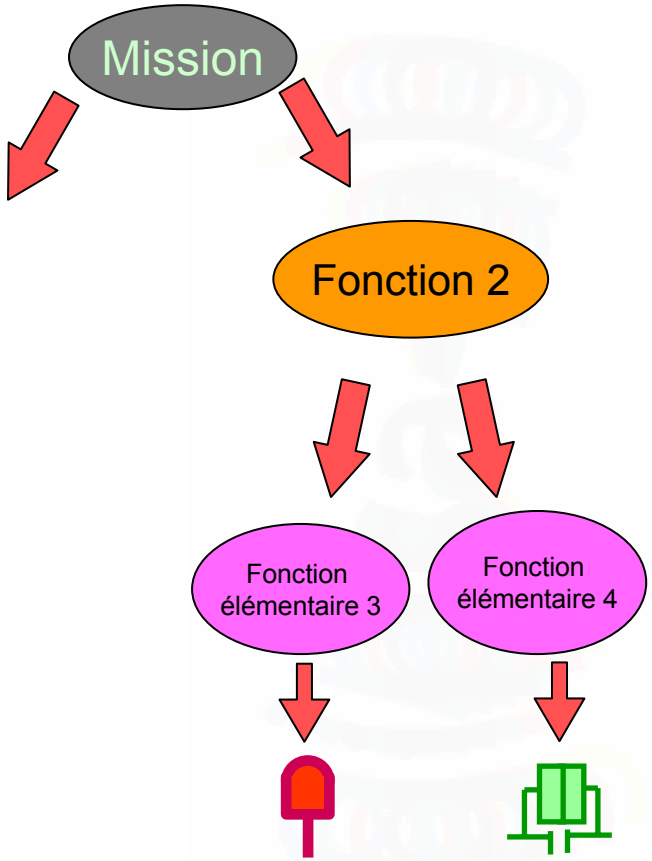




4.1.2 Réseau pouvant défaillir

Approche statique, basée sur l'architecture

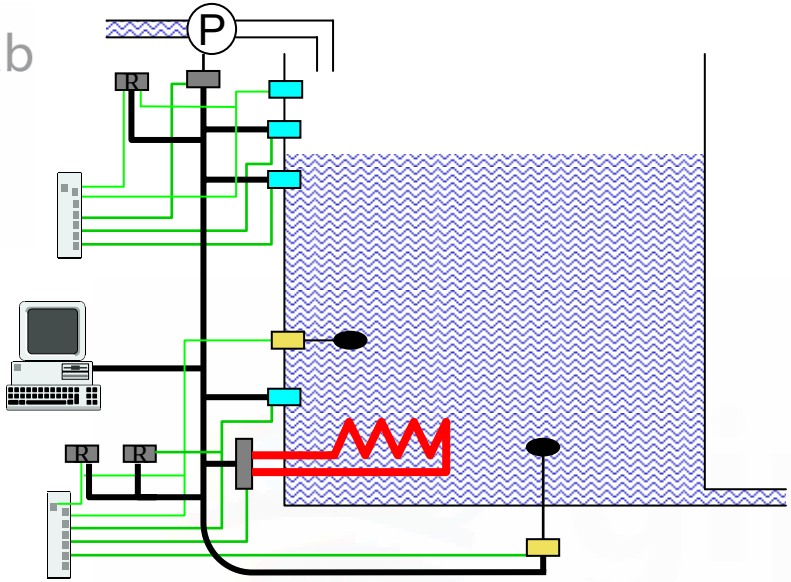
Evaluation du niveau de fiabilité et de disponibilité d'une architecture en réseau



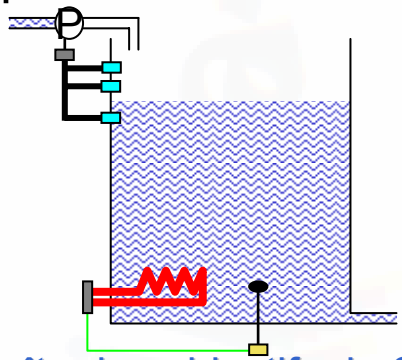
- Etats => disponibilité
- Propagation des défaillances => fiabilité
- Utilisation de diagrammes de décision binaire

[Conrard 2004]

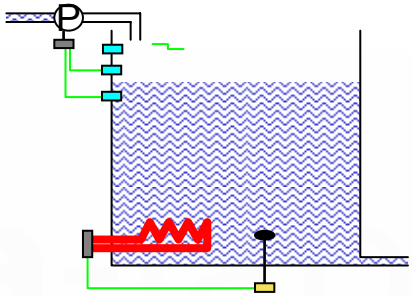
Résultats



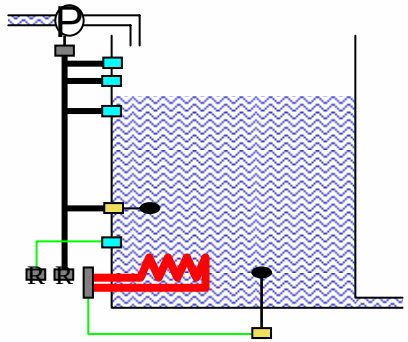
- Architecture matérielle préliminaire



- Accroître les objectifs de SdF
  - Une solution plus sûre (réseaux + composants intelligents)



- En accord avec les objectifs de SdF
  - la solution la plus économique



- Accroître les objectifs de fiabilité
  - Une solution encore plus sûre

4.1.3 interaction réseau-système

Evaluation dynamique de la sûreté de fonctionnement

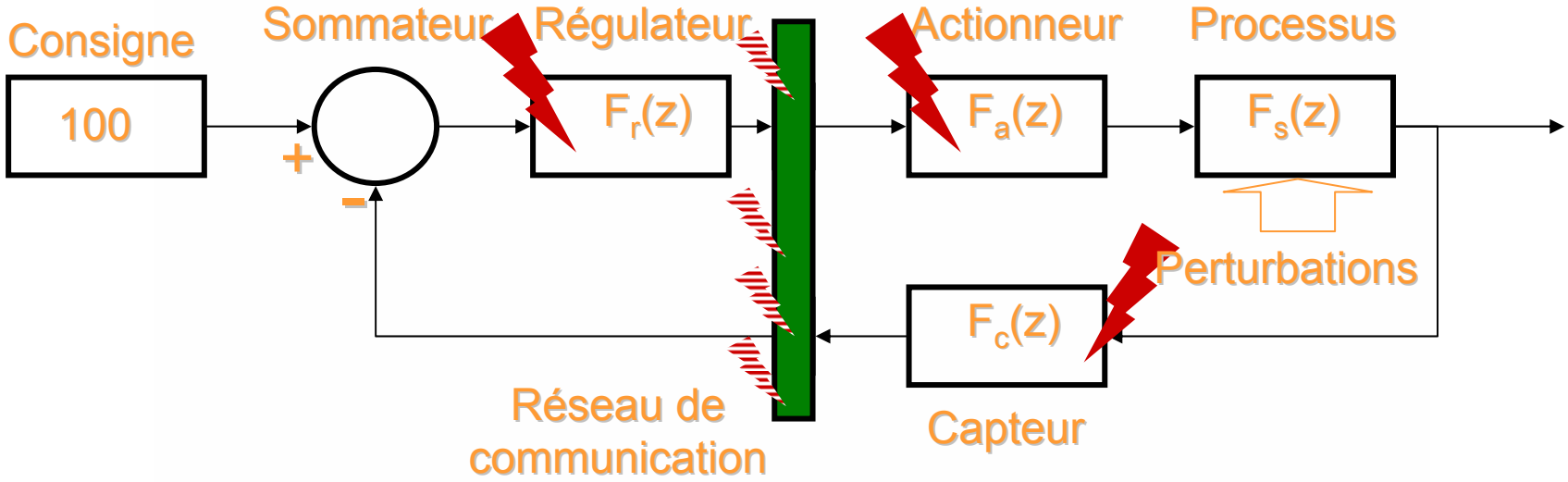
Etape - Modélisation ✓

Modèle fonctionnel des composants ✓

→ Modèle dysfonctionnel des composants ✓

→ Modèle unifié des composants ✓

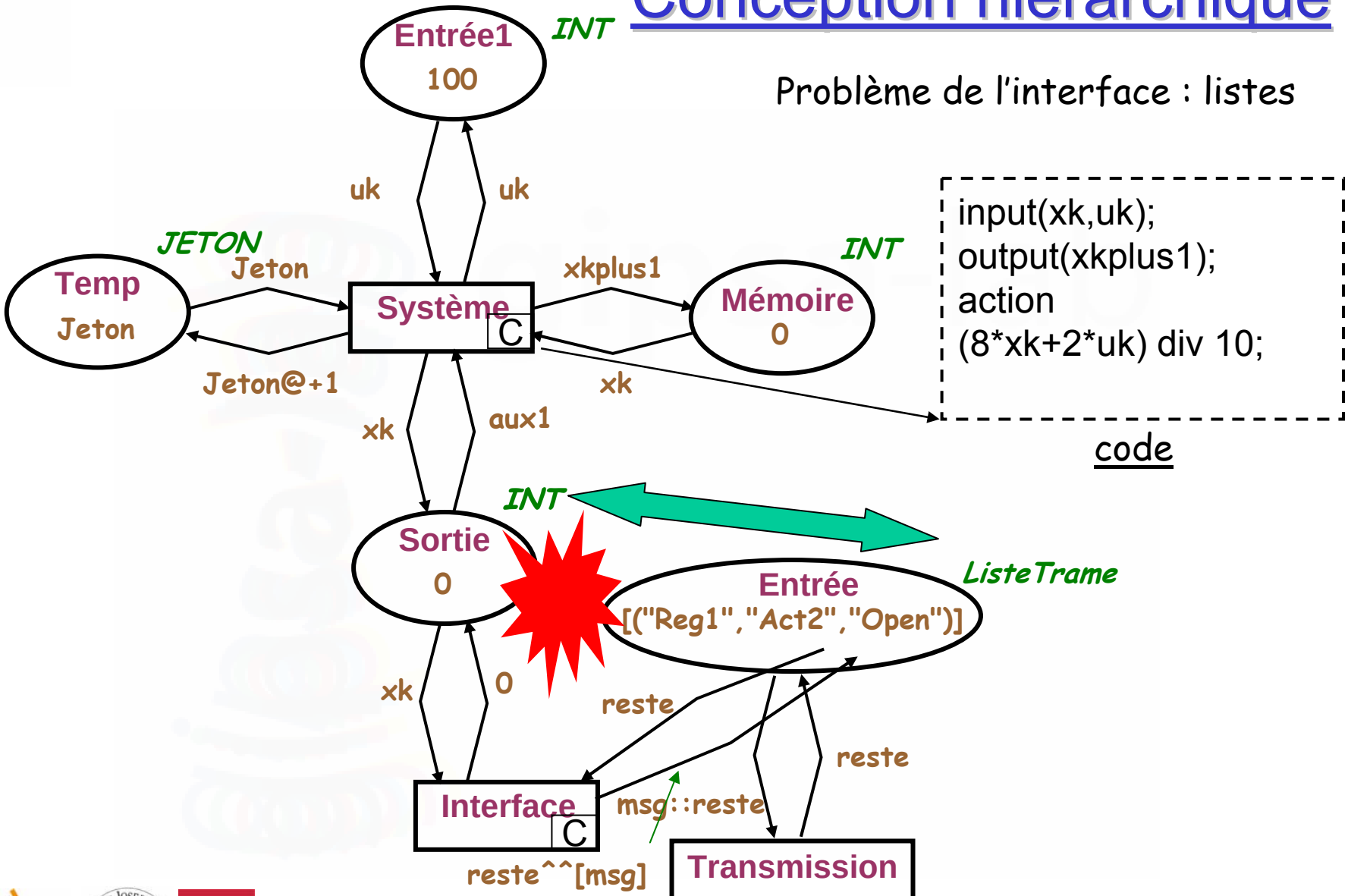
→ Interconnexion des composants ✓



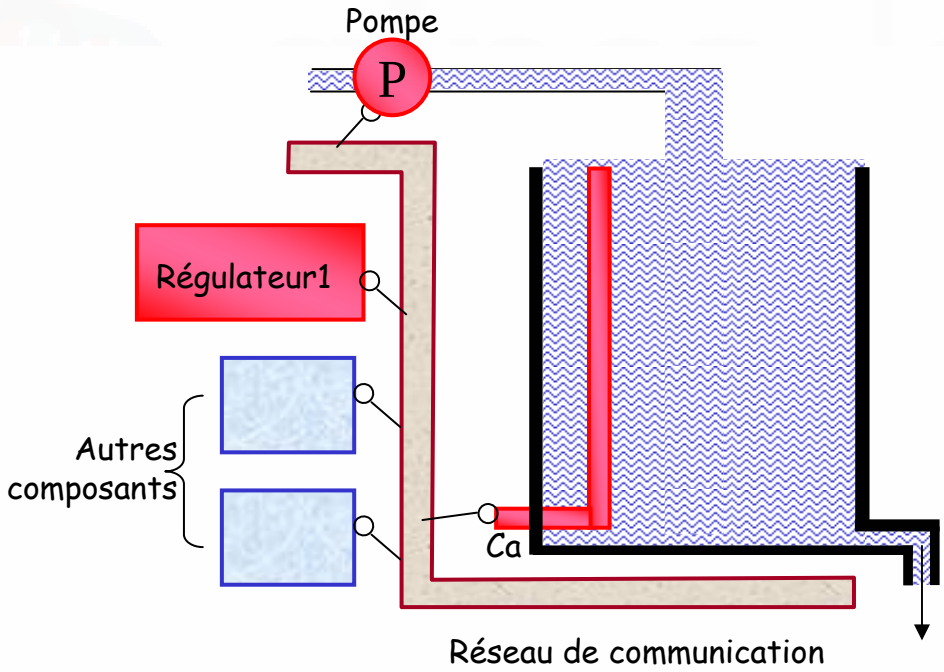
Design/CPN [Jen 97]

Conception hiérarchique

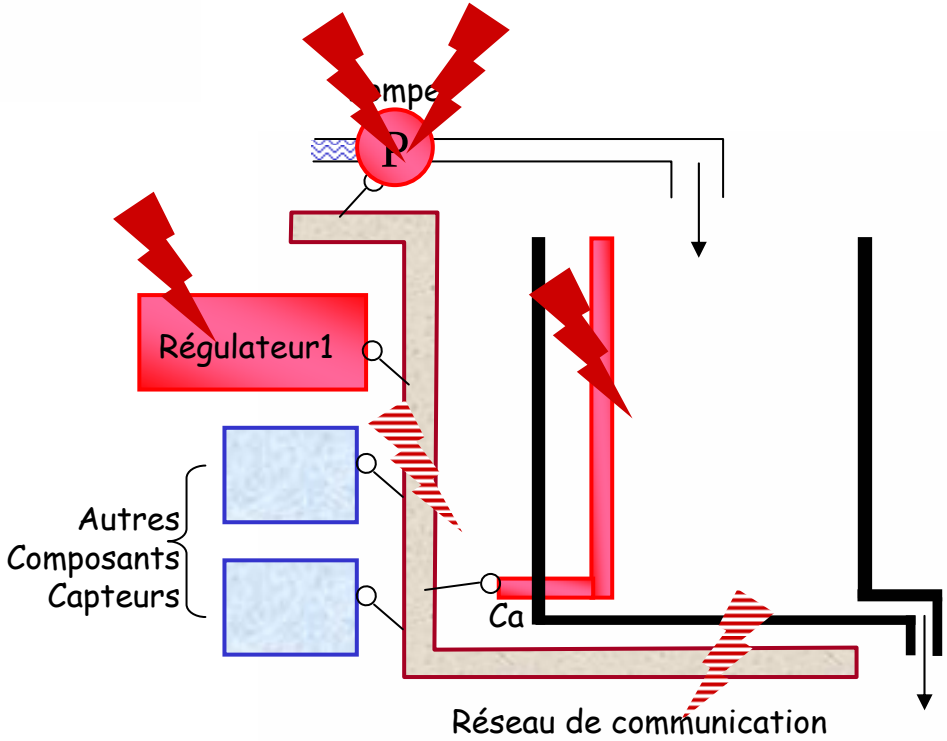
Problème de l'interface : listes



Présentation du système



Défaillances



6 événements :

1. Défaillance du régulateur
2. Défaillance du capteur

Défaillances de l'actionneur

3. Usure
4. Blocage

Erreurs du réseau

5. Perte d'une trame
6. Altération d'une trame

[Barger 2003]

Mission		Mode de défaillance
1. Remplir la cuve	➔	Ne remplit pas
2. Maintenir le niveau	➔	Ne maintient pas

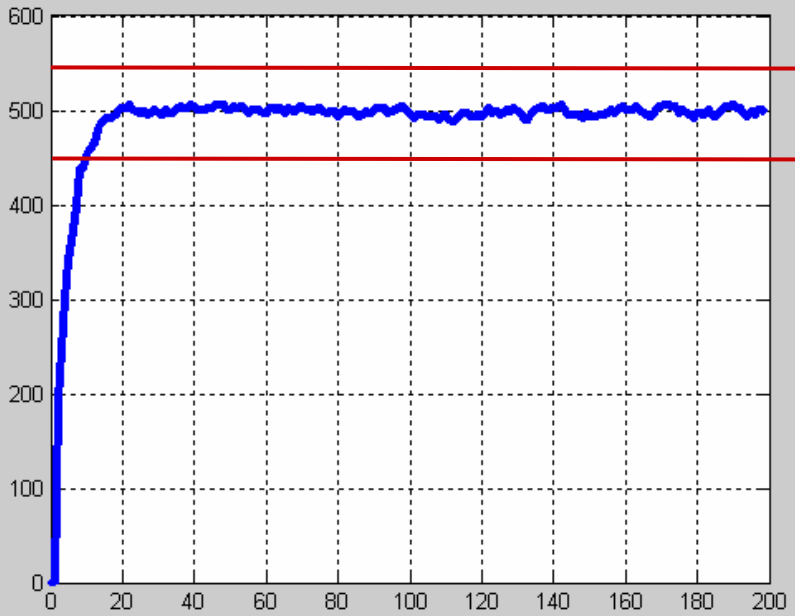
Scénarios

Défaillances

6 événements	Probabilités
Défaillances en fonction de temps	
Défaillances de l'actionneur	
1. Défaillance du régulateur	1/(100 Te)
2. Défaillance du capteur	1/(100 Te)
3. Usure	1/(50 Te)*
4. Blocage	1/100 démarrages
Défaillances en fonction des sollicitations	
Erreurs du réseau	
5. Perte d'une trame	1/20 trames
6. Altération d'une trame	1/20 trames

*pendant le fonctionnement

Simulation Monte Carlo



11% Ne maintient pas

83% Réussie

6% Ne remplit pas

Résultats

Total simulations	Simulation finie comme		
	Ne remplit pas	Réussie	Ne maintient pas
6734	389	5620	725
100%	6%	83%	11%

L'importance d'un scénario

Conclusion cas statique

Evénements réseau et leur influence cumulée peu importants ➔ débordement est dû aux autres événements

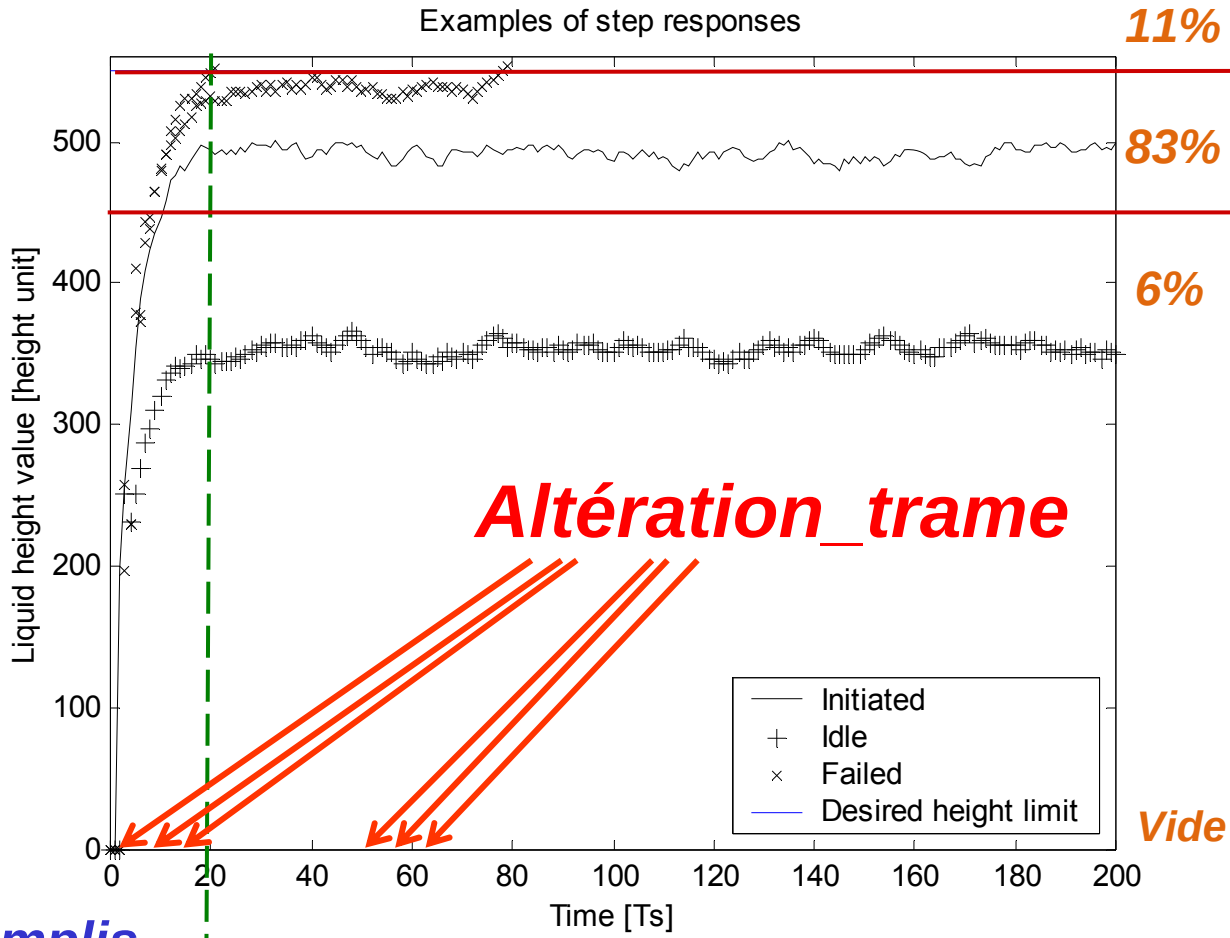
Problème: 50% des scénarios menant au débordement ne contiennent que des problèmes dus au réseau de communication

➔besoin d'une autre approche d'analyse:
analyse dynamique

L'importance d'une erreur réseau dépend de l'état* du système

*Etat au sens de l'automatique, variable interne (niveau) intégrant en elle l'historique fonctionnel et dysfonctionnel du système

L'importance d'un scénario : Cas dynamique



11% **Ne maintient pas**

83% **Désiré**

6% **Non rempli**

Vide

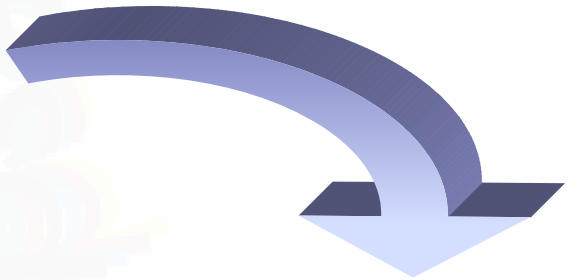
Altération_trame

Remplis-sage

Maintien

Fiabilité des systèmes commandés

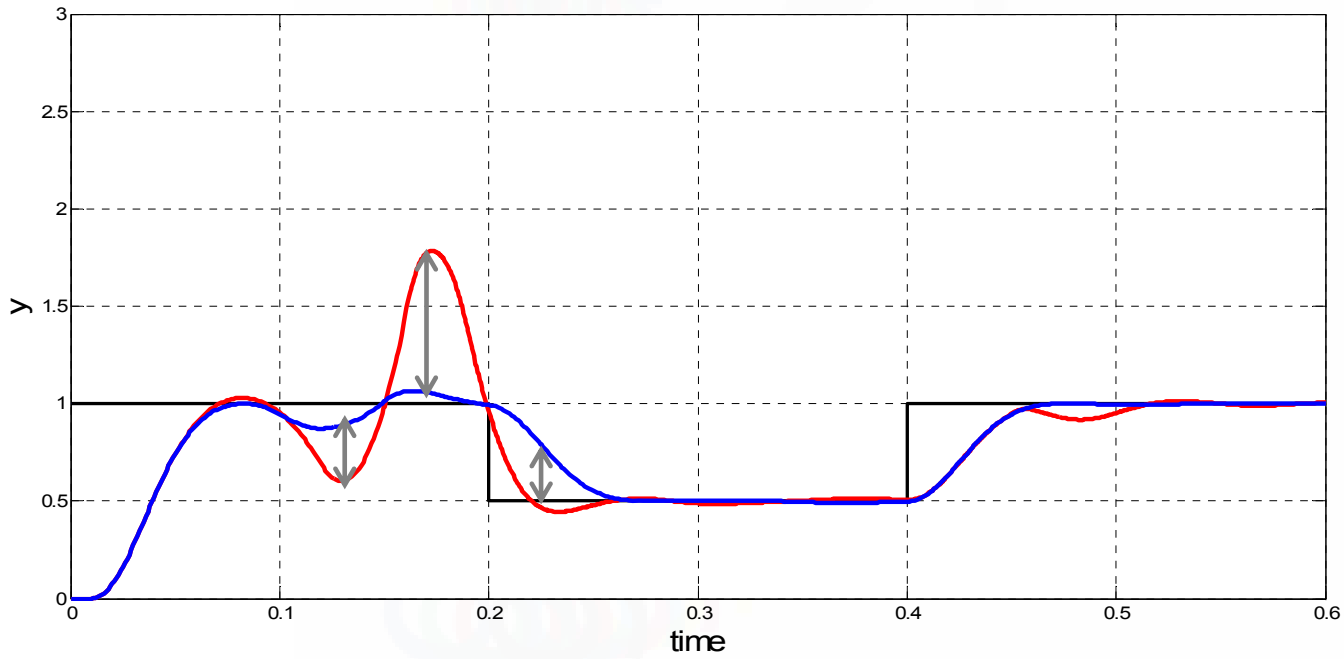
- **Recherche des Scénarios critiques [Moncelet, Sadou]**
  - Recherche des séquences des événements redoutés et l'estimation de leurs probabilités
- **[Barger, 2003]**
  - Parmi les premiers travaux qui ont considéré des fautes au niveau du réseau (probabilités de perte sur les messages)
  - Système commandé → système dynamique par rapport à la SdF
  - Approche basée sur les réseaux de Petri pour prendre en compte l'aspect dynamique



dans la suite de ces travaux
il convient de mieux prendre
en compte les fautes transitoires représentatives d'un réseau

Example

- Impact of lost messages on the system reliability
  - How we detect a failure situation?

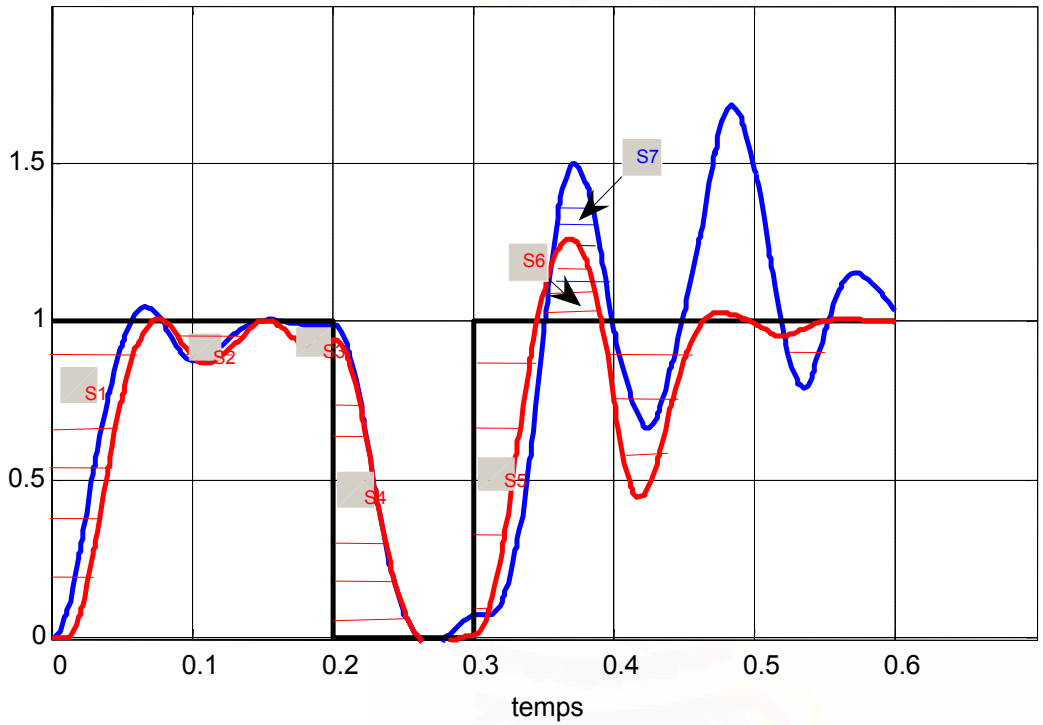


Actual output

output error

Reference output

Réponse à une sollicitation tout ou rien



- En noir, consigne
- En rouge, 10 % de pertes d'information
- En bleu, 20 % de perte d'information

SAN/Truetime

Fiabilité en fonction du taux de perte et de de l'erreur de sortie permise

MonteCarlo approch
1000 trial for
Each case

			Loss probability			
			0.5%	1%	5%	10%
OUTPUT ERROR	0.4	Truetime	~1	0.9993	0.8833	0.7167
		Mobius	~1	0.9989	0.8981	0.7192
	0.3	Truetime	0.9999	0.9909	0.8533	0.6821
		Mobius	0.9972	0.9918	0.8538	0.6832
	0.2	Truetime	0.9556	0.6933	0.2233	0.0120
		Mobius	0.9514	0.6919	0.2187	0.0115
	0.1	Truetime	0.9431	0.6433	0.1900	0.0059
		Mobius	0.9392	0.6429	0.1923	0.0052

Normalized

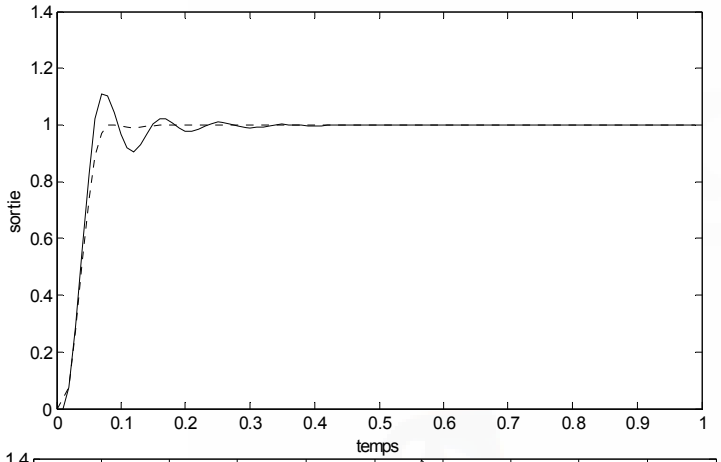
<u>SAN</u>
+ widely used for dependability evaluation
+ analytical and simulation solutions

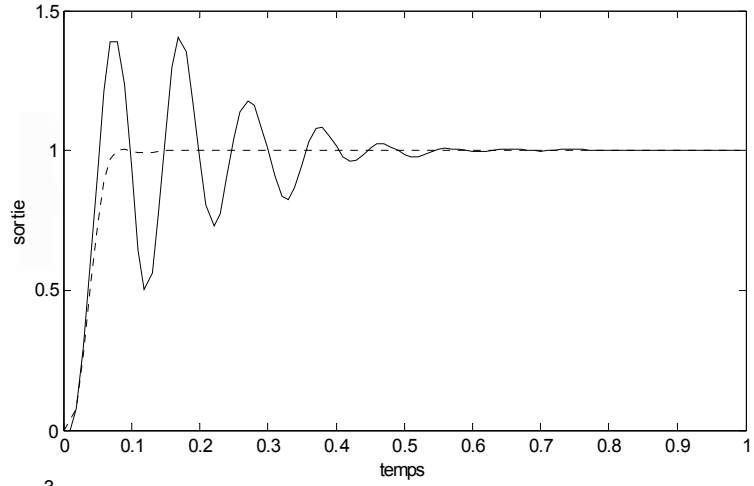
<u>Truetime</u>
-never used for reliability evaluation
-Only simulation solution
+ the use of already simulink model

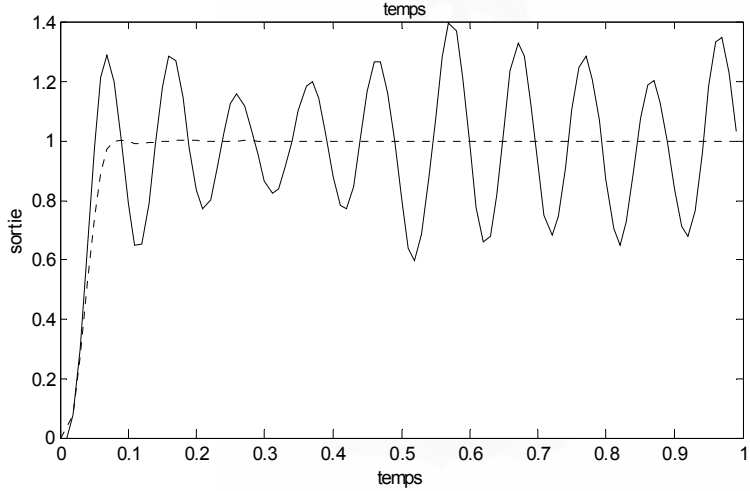
Modélisation d'un SCR classique

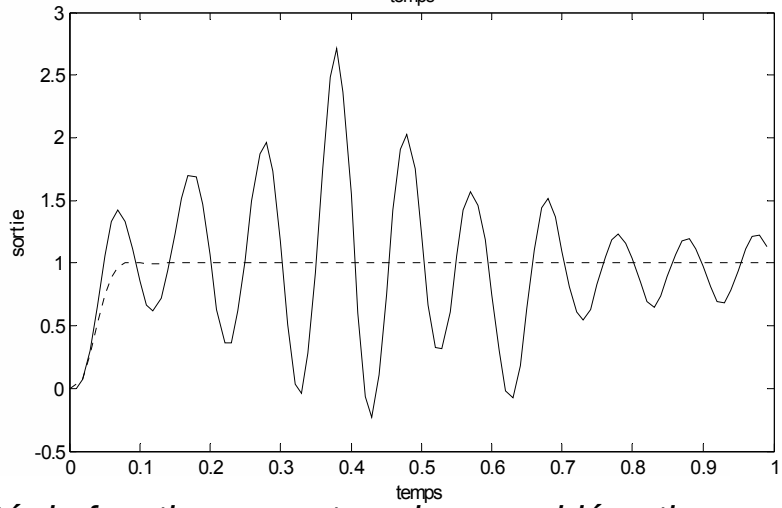
Modèle composé

Process=1000/s(s+1) Te=0.01s
retard uniformément distribué entre 0%Te et 60%Te









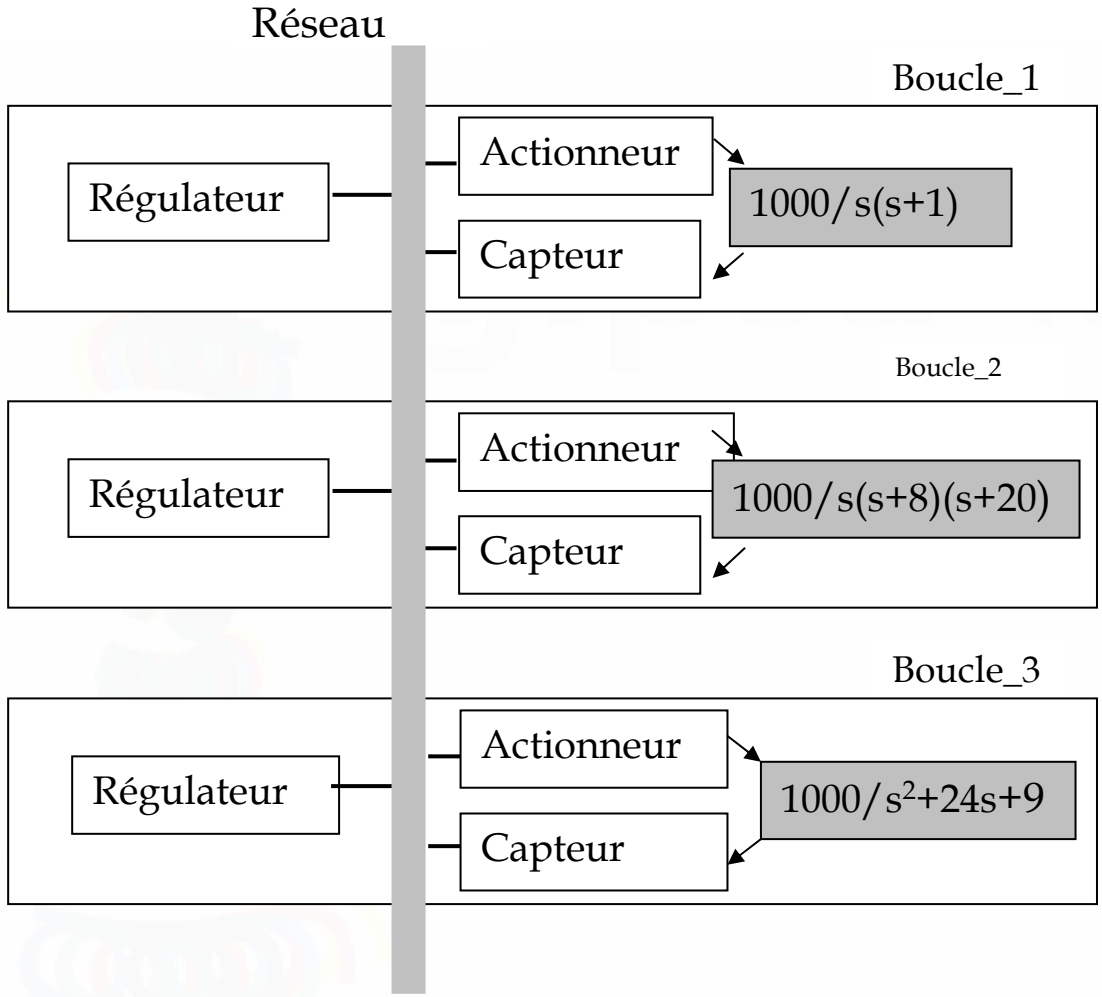
Modes de défaillance

- défaillance par dépassement
- défaillance par temps de réponse
- défaillance sur la stabilité

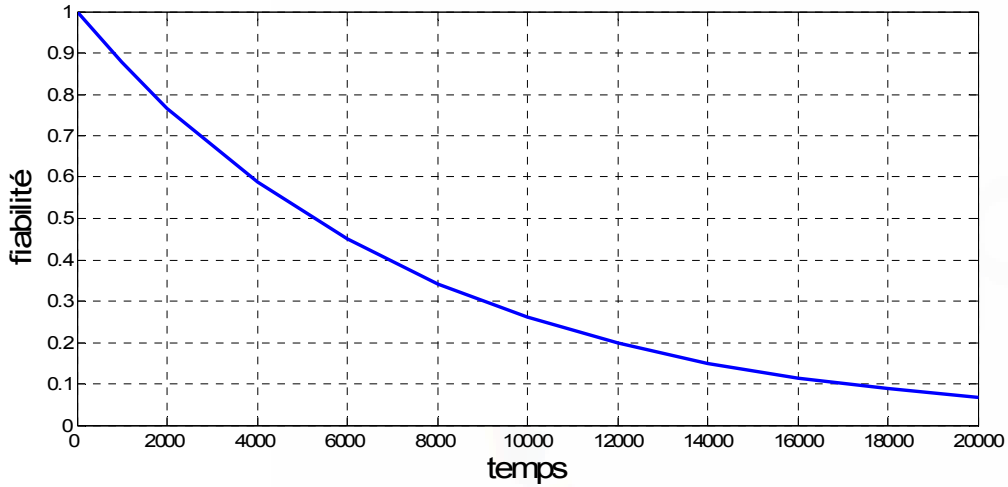
Connaissance sur les probabilités de fautes transitoires (retard variable, perte des messages)

Probabilité de défaillance du système

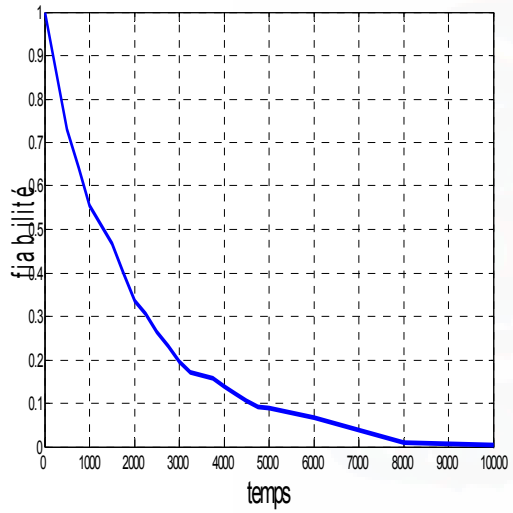
Système à trois boucles



Trois boucles partageant le même medium



Cas 1 : la boucle_1 possède la plus grande priorité



Cas 2 : boucle_2 possède la plus grande priorité

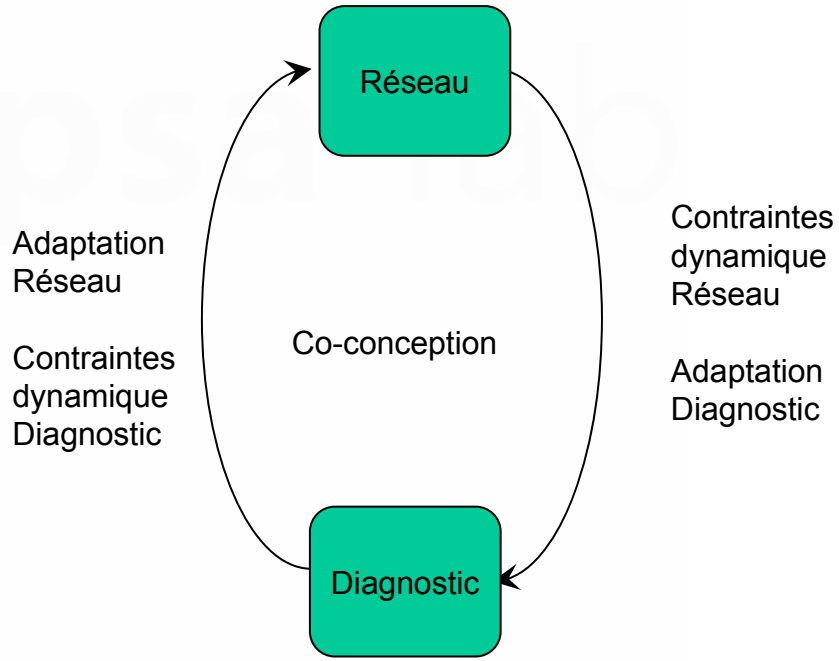
Conclusions

- Modèle du réseau
- Modèle du système
- Temps continu
- Aspects événementiels
- Combinaison de ces aspects
- Analyse de sensibilité des paramètres

4.2 Co-design, exemples de travaux en cours

Introduction

- Schéma co-design
- Approche réseau en fct des contraintes systèmes
  - Contrôle du réseau
- Approche système en fct des contraintes réseaux
  - Contrôle/diagnostic via le network



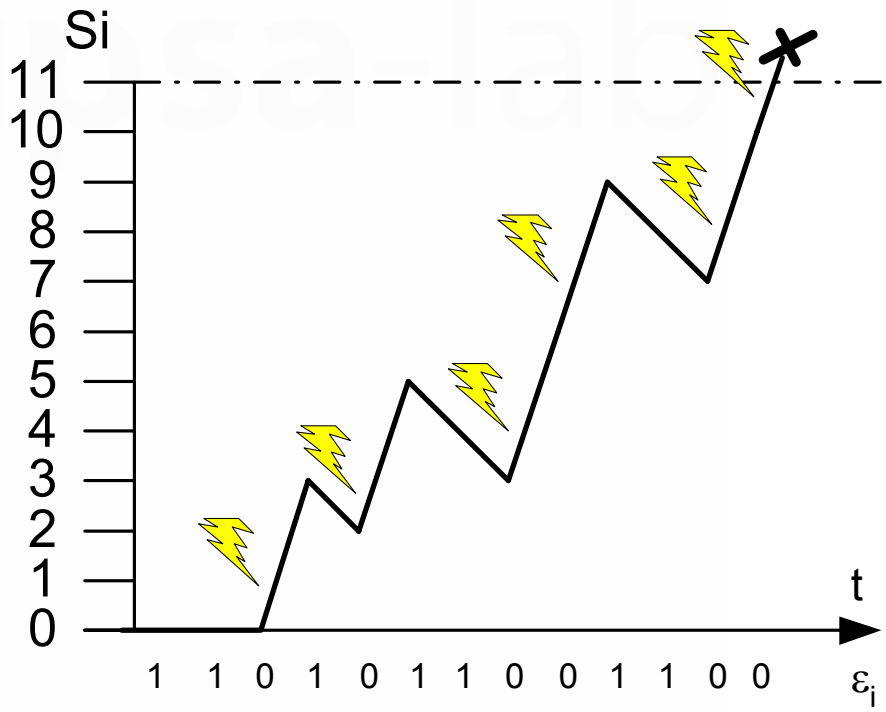
Diagnostic ⇔ sûreté de fonctionnement

Influence de scénarios de défaillances sur la sdf du système

- séquencement d'événements
- Durée entre événements

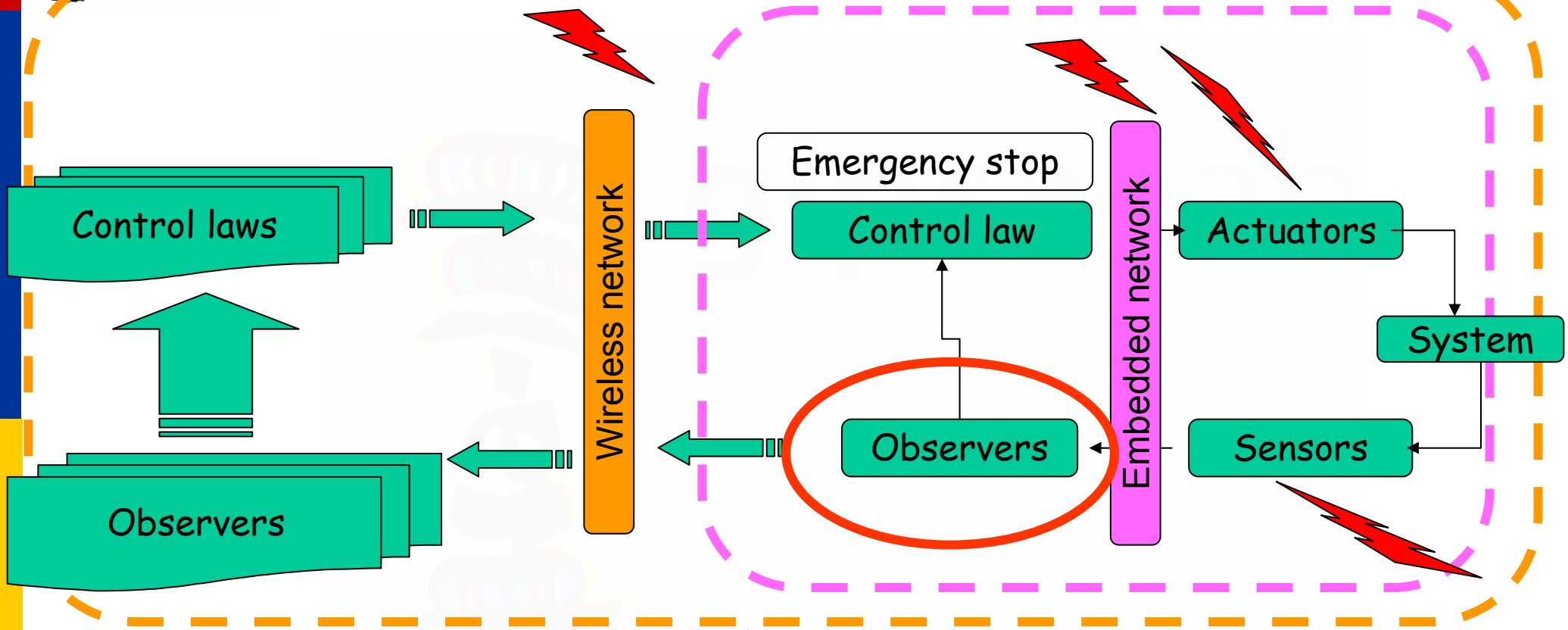
- Avalanche de fautes
- Etude à partir d'une chaîne de Markov

[Jumel 2003]



Drone-hélicoptère

Purpose: Networked Control



GROUND STATIONS

Wireless loop

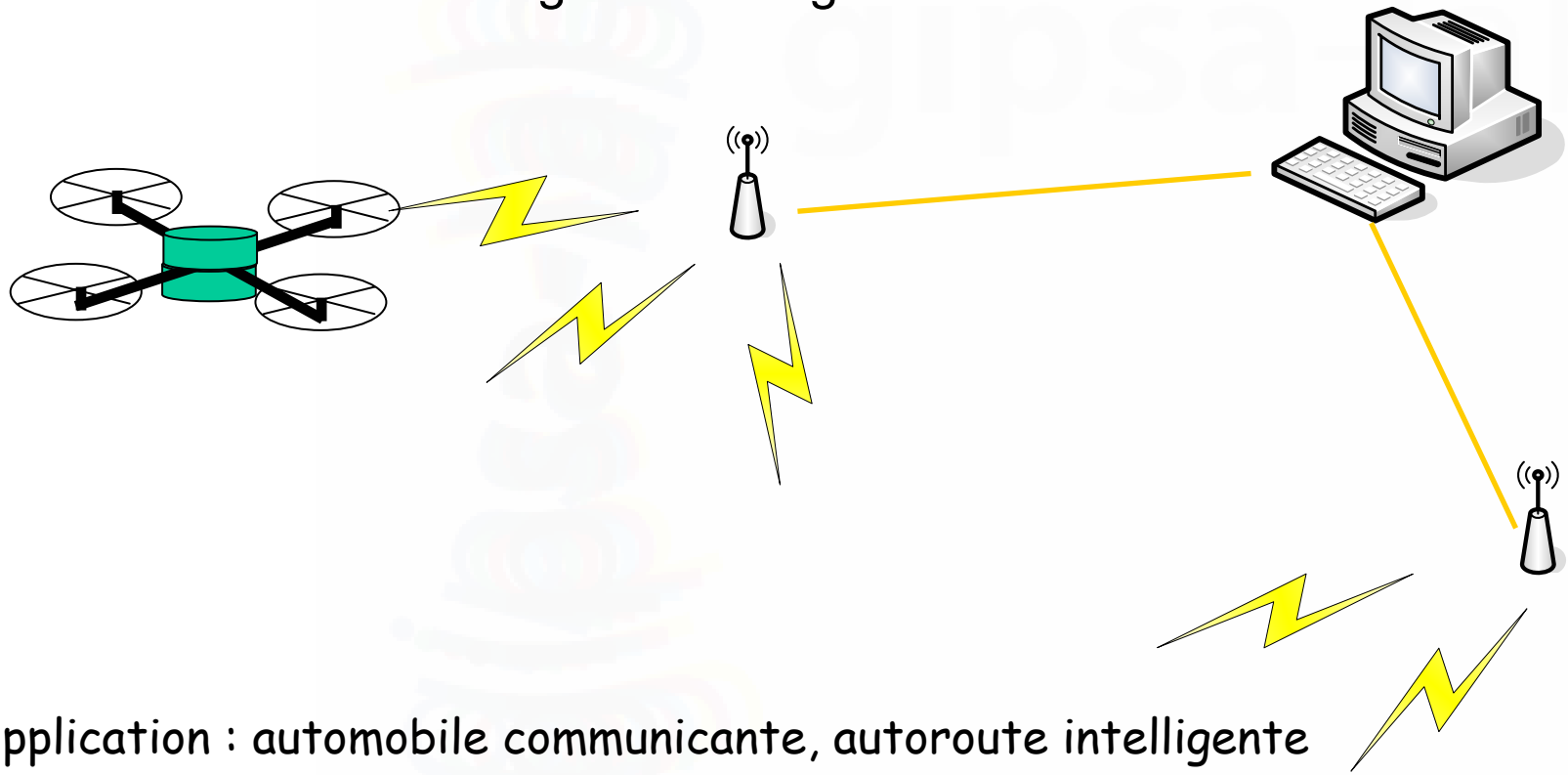
Drone-Ground stations communication

EMBEDDED (communication)

Embedded local loop

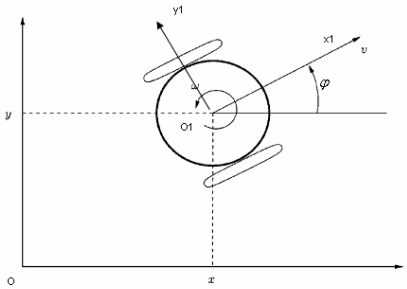
The roaming in ZigBee network

- Roaming – switching between different stations

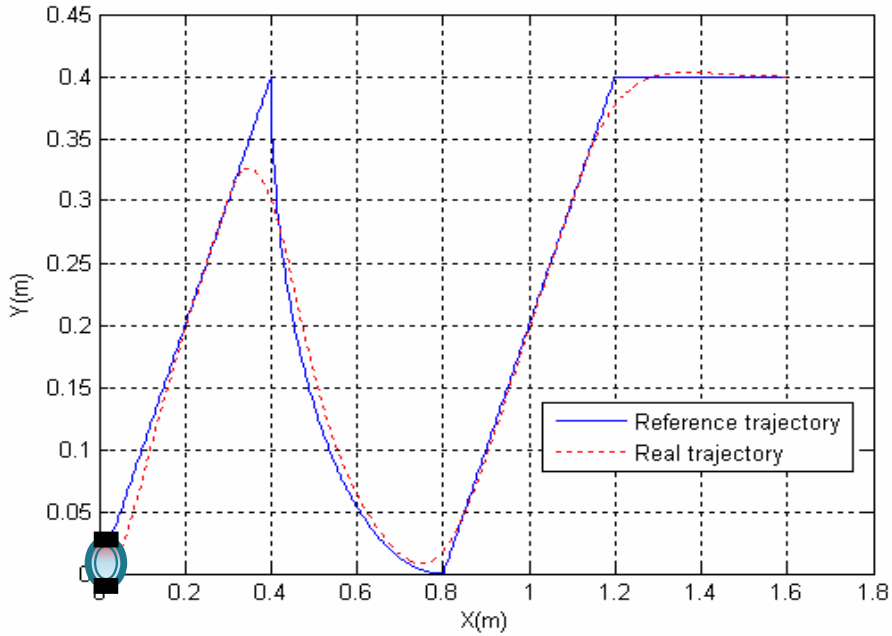


Application : automobile communicante, autoroute intelligente

Suivi de trajectoire, application robot



Robot Khepera



Trajectory of the robot

Initial position

$(X_0, Y_0, \varphi_0) = (0,0,0)$

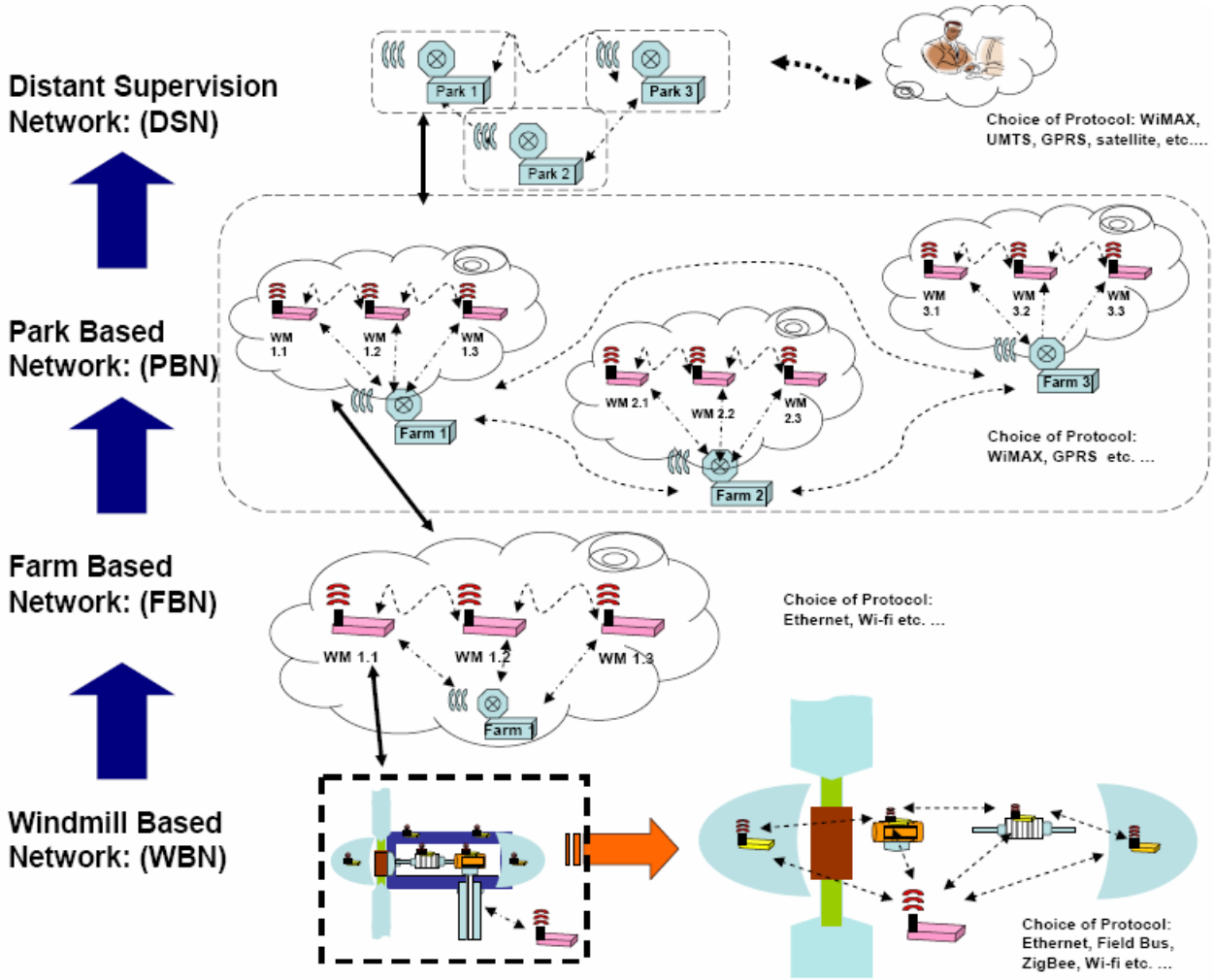
Reference:

A Time trajectory

Global Heterogeneous Architecture

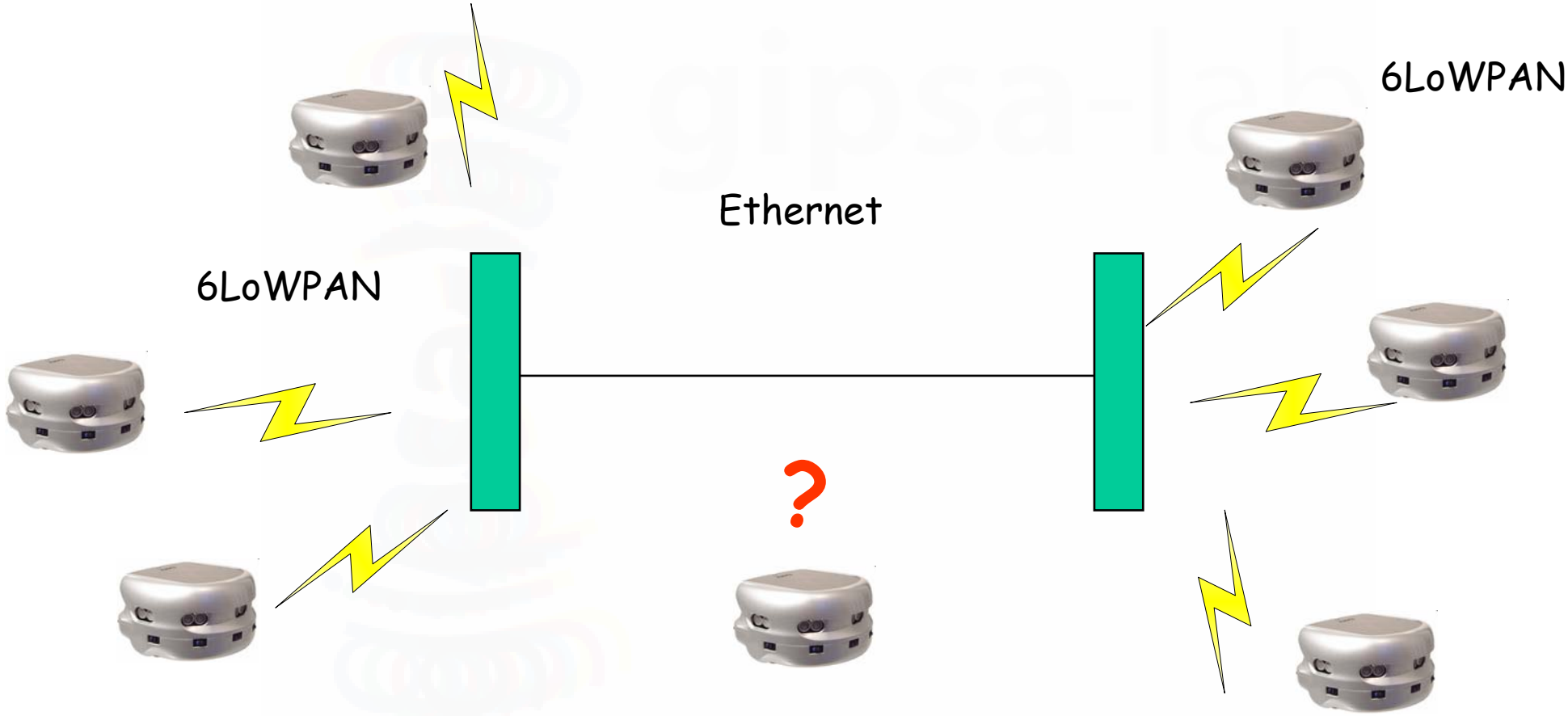
long distance

Short distance

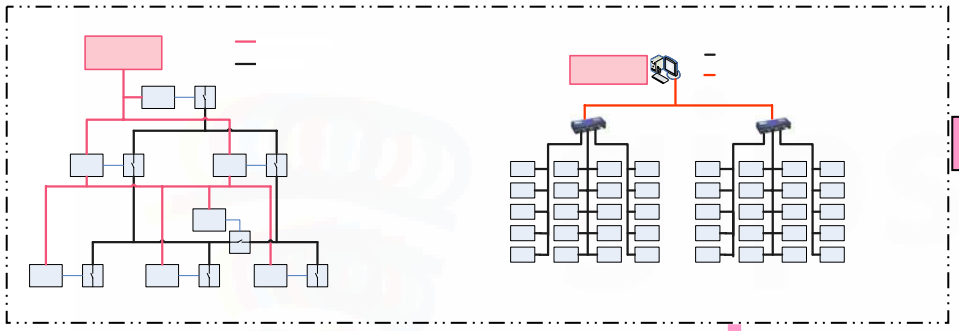


Trafic temps réel-temps critique sur réseau hétérogène IP bout en bout

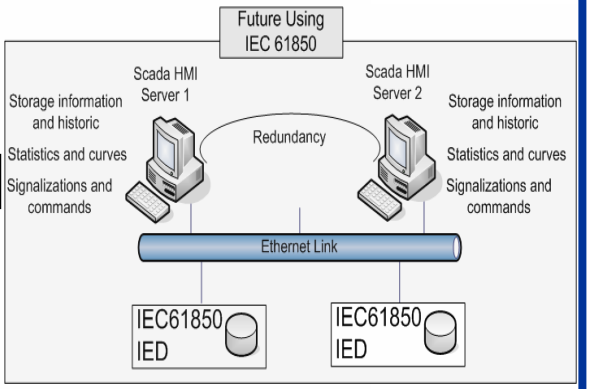
Assurer une mission commune (extinction d'incendie…), réussir la mission ?



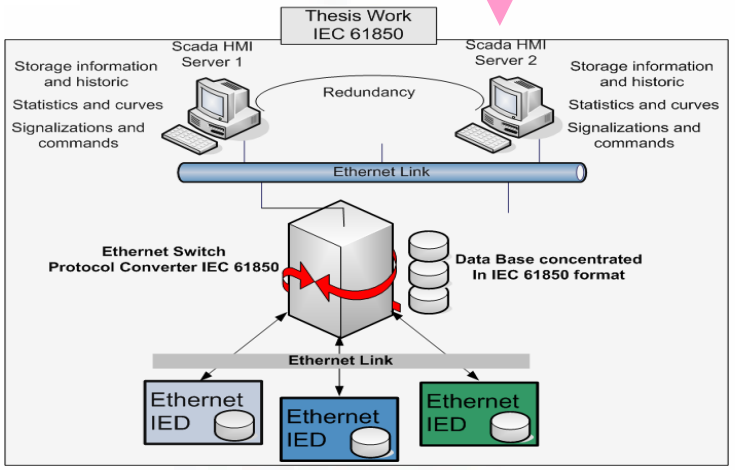
Evolution of architectures respecting IEC 61850 & new propositions

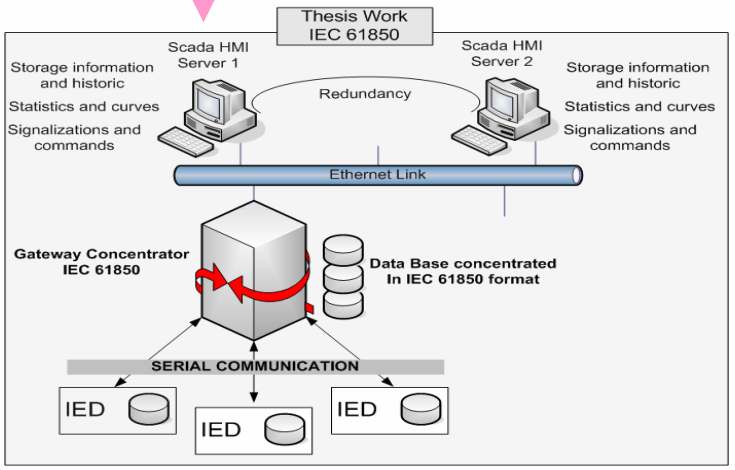


constructe urs



Architectures EURO SYSTEM





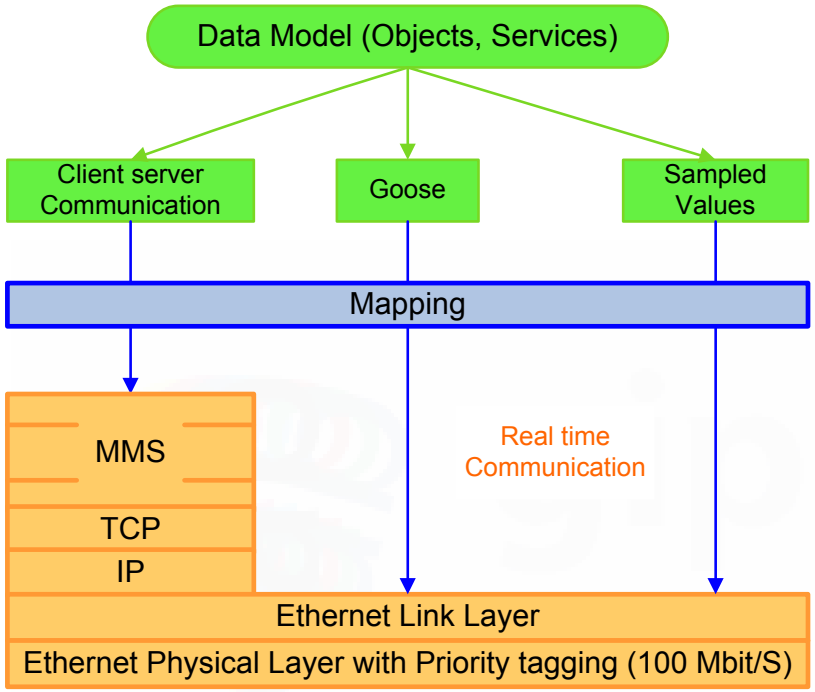
ETH

SCADA

BUS

IED

IEC 61850



- Satisfying real time performance by the standard in developing extension cards that can transmit critical real-time signals at serial network level
- Development of a new appliction layer allowing to track the dialogue according to the IEC 61850 standard
- New equipment design playing the role of Ethernet switch/ IEC 61850 converter and data concentrator

Conclusions et perspectives

Conclusions

- Evaluer la fiabilité d'un système commandé en réseau avec la prise en compte des aspects dynamiques
- Méthode de conception prenant en compte en particulier les informations critiques
- proposition d'une approche de modélisation et de l'analyse
  - composants divers (hybrides, défaillants)
  - leur intégration
  - le comportement dynamique
  - un seul outil, ou des systèmes hybrides (hardware in the loop ?)
- Pas de formule magique, mais un rapprochement
- A approfondir les aspects plus formels tant pour la modalisation que l'évaluation => non trivial

Conclusion

- **Réseau**
  - Topologie, méthode d'accès, priorités, routage…
  - Pbs des réseaux filaires
  - Pbs des réseaux sans fil
- **SdF**
  - Sdf de réseaux
  - Sdf vision système (NCS)
- **Problématique importante**

Des projets

- nationaux (ANR [Cran, Laas, Inria Rhone alpes, Loria, GIPSA-Lab],
- GIS [UTT, UTC, LAGIS, LAMIH, Crestic, CRAN, LORIA, EDF, CEA]
- européens Necst, (avec un nouvel appel à projets en ICT Information and Communication Technologies [Network, embedded system, Control]

Des acteurs, pluridisciplinarité

Un groupe de travail sur cette thématique : Ciame (Constituants Intelligents pour l'automatisation et la mesure) réunion régulière sur Paris

- Sortie d'un ouvrage sur la Sdf des systèmes intégrant un réseau de terrain
- Une session proposée à CIFA 08 et au World IFAC

Réseaux de capteurs et MANET (Mobile ad hoc networks)

- Ensemble de « micro- » capteurs autonomes communicants distribués
  - Échange d'informations
  - Elaboration d'une stratégie globale (mesure, reconnaissance, validation)
  - Coopération des éléments (« intelligence distribuée »)
- Topologie et organisation dynamiques
  - Objets entrants et sortants du réseau à tout moment
  - Eventuellement objets mobiles
- Aspects routages dynamique
- Aspects « low cost » et faible énergie (mise en veille)

Modélisation de réseaux

- Méthodes & Outils, de type graphes
  - Automates
  - Files d'attente
  - Réseaux de Petri (MocaRP, DesignCPN,…) et extensions (Réseaux d'Activités stochastiques (Möbius)
  - Simulateur de réseaux (OpNet, Network Simulator)
- Approches probabilistes
  - Chaînes, graphes de Markov

Outils-méthodes ?

- Réseaux de Petri
  - Colorés, Stochastiques, Temporisés, à jetons vieillissants
  - Etude des graphes de marquage ou d'occurrences
    - Mise en évidence d'états catastrophiques
    - Recherche des scénarios conduisant à ces états
- Réseaux d'Activités Stochastiques
- True-Time
- Réseaux bayésiens dynamiques
- Simulation de Monte-Carlo
- ???

Simplifications des modèles

- Isoler des ensembles cohérents communicants (avec des interfaces d'entrées-sorties)
- Puis composer ces sous-ensembles afin d'obtenir un modèle global
  - synchronisation entre les modèles des différents sous-systèmes
  - messages
  - variables partagées
- Aspect réseau partagé difficile, mais simplifié
  - Si réseau déterministe (TDMA) => permet de garantir un taux de communication (difficile en sans fil)
    - La sensibilité aux perturbations e.m. demeure (cause commune)
  - Si protocole de réseau de type (m,k)-firm (garantit un nombre de trames lié à une tâche sur une fenêtre temporelle) [Y. Q. Song]
  - Mais toujours dépendance
- Utilisation de méthodes de Monte-Carlo sur des cas – types
  - Analyse de sensibilité de certains paramètres (retards, pertes)
  - Généralisation

Aspects sûreté de fonctionnement dynamique

- Communauté fiabilité dynamique
- Sûreté de fonctionnement a priori d'une mission
  - Fonction de la mission (ex : niveau de dynamique d'un drone
  - Probabilité de passer dans un environnement perturbé ai niveau des communications (perturbations e.m., géographiques)
- Sûreté de fonctionnement dynamique
  - Elaboration « on-line » de la SdF en fonction de l'état du système, de l'évolution de la mission…

Références bibliographiques

- M. A. Azgomi & A. Movaghar – Definition and analysis of cloured stochastic activity networks – Technical report, Dept. Of Computer Engineering, Sharif University of Technology, Tehran, Iran, 2004.
- P. Barger – Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique – thèse de l'Université Henri Poincaré Nancy 1, 15 décembre 2003.
- M. Bayart – *Instrumentation intelligents, systèmes automatisés de production à intelligence distribuée* – Habilitation à Diriger des Recherches, USTL, Lille, 21 décembre 1994.
- A. Cervin, D. Henriksson, B. Lincoln, J. Eker, K.E. Årzén – How does control timing affect performance? – IEEE Control Systems Magazine, JUne 2003, Vol. 23, N.3
- Groupe CIAME – Réseaux de terrain, description et critères de choix – Hermes, Paris, 1999.B. Conrard – Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception – thèse de l'Université Henri Poincaré Nancy 1, 24 septembre 1999.
- Blaise Conrard, Jean-Marc Thiriet, Michel Robert – Problems of precision for control loops implanted on Distributed Automation System – CESA'98 (Computational Engineering in Systems Applications)/IMACS/IEEE, Hammamet/Nabeul (Tunisie), avril 1998, pp. 180-185, vol. 1.
- M. Conti, S. Giordano – Multihop ad hoc networking: the theory – IEEE Communications, Vol 45, n°4, p.78, avril 2007.
- R. David, H. Alla – Du Grafcet aux réseaux de Petri – Hermes, Paris, 1992, 1997.
- M. Diaz – Les réseaux de Petri, modèles fondamentaux – Hermes, Paris, 2001.
- JP Georges – Systèmes contrôlés en réseau : évaluation de performances d'architectures ethernet commutées – thèse UHP-CRAN, Nancy, 2005.
- W. Hu, D. Willkomm, G. Vlantis, M. Gerla, A. Wolisz – Dynamic frequency hopping communities for efficient IEEE 802.22 operation – IEEE communications, vol 45, n° 5, mai 2007, p. 80

Références bibliographiques

- K. Jensen – Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use – Monographs in Theoretical Computer Science, Springer-Verlag, 2nd corrected printing 1997.
- Guy Juanole – Réseaux de communication et automatique – *Journées "Automatique et Communication"*, 13-14 mars 2001.
- G. Juanole, I. Blum – Quality of service of real time networks and performances of distributed applications – LAAS report 99166, avril 1999.
- F. Jumel, J.M. Thiriet, J.F. Aubry, O. Malasse - "Towards an information-based approach for the dependability evaluation of distributed control systems" - 20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC2003), Vail (Colorado, United States), 20-22nd May 2003, pp. 270-275.
- P. Kleinschmidt, F. Schmidt - How many sensors does a car need ? - Eurosensors V, Roma, 2 October 1991, pp.1-13.
- P.R. Kumar – New technological vistas for systels and control – IEEE Control Magazine, February 2001
- M.J. Lee, J. Zhang & al. – A new taxonomy of routing algorithms for wireless mobile ad hoc networks: the component approach – IEEE p. Communications, Vol. 44, N° 11, novembre 2006, 116
- K. Lu, Y. Qian – A secure and service-oriented network control framework for WIMAX network – IEEE Communications, Vol 45, N° 5, p. 124, mai 2007
- Stéphane Mocanu – Cours de réseaux, ENSIEG, 2005
- R. M. Murray, K.J. Åström, S. P. Boyd, R. W. Brockett, G. Stein – Future directions in control in an information-rich world, IEEE Control Magazine, April 2003, Vol. 23, n. 2
- Natale, O.R.; Sename, O.; Canudas-de-Wit, C.; - Inverted pendulum stabilization through the Ethernet network, performance analysis - American Control Conference, 2004. Proceedings of the 2004 - Volume 6, 30 June-2 July 2004 Page(s):4909 - 4914 vol.6
- Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang – Investigation of bandwidth request mechanisms under point-to-multipoint mode of Wimax networks – IEEE Communications, Vol 45, N° 5, p. 132, mai 2007

Références bibliographiques

- S.I. Niculescu – Systèmes à retard, aspects qualitatifs sur la stabilité et la stabilisation – Diderot éditeur, Paris, 1997.
- D. Niyato, E. Hossain – Integration of WImax and Wifi: optimal pricing for nadwidth sharing – IEEE Communications, Vol 45, N° 5, p. 140, mai 2007.
- L. Pelusi, A. Passarella, M. Conti – Opportunistic networking: data forwarding in disconnected mobile ad hoc network, IEEE Communications, Vol. 44, N° 11, novembre 2006.
- S.A. Reinemo, T. Skeie, T. Sodring, O. Lysne, O. Torudbakken – An overview of QoS capabilities in InfiniBand, Advanced Switching Interconnect, and Ethernet – IEEECommunications, Vol 44, n° 7, juillet 2006, page 32
- M. Robert, M. Marchandiaux, M. Porte – *Capteurs Intelligents et Méthodologie d'Evaluation* – Hermès, 1993.
- D. J. Smith & K. G. Simpson – Functional safety (second edition) a straightforward guide to applying IEC 61508 and related standards – Elsevier, 2004.
- Y. Q. Song – performance analysis and improvement of zig-bee routing protocol – Fet, 2007, Toulouse.
- J.M. Thiriet - Habilitation à Diriger des Recherches de l'Université Henri Poincaré Nancy 1 en Automatique : "Sûreté de fonctionnement de Systèmes d'Automatisation à Intelligence Distribuée" - CRAN-UHP, Nancy, 16 décembre 2004.
- Törngren M. – Fundamentals of implementing real-time control applications in distributed computer systems, Real-Time Systems Journal, Volume 14, Number 3, May 1998.
- V. Volovoi – Modeling multiphased missions using stochastic Petri nets with aging tokens – RAMS'04, Annual Reliability and Maintainability Symposium, Los Angeles, janvier 2004.
- G.C. Walsh, H. Ye – Scheduling of networked control systems – IEEE control Magazine, février 2001.
- Witrant, E.; Canudas-De-Wit, C.; Georges, D.; Alamir, M.; - Remote stabilization via time-varying communication network delays: application to TCP networks - Control Applications, 2004. Proceedings of the 2004 IEEE International Conference on - Volume 1, 2-4 Sept. 2004 Page(s):474 - 479 Vol.1
- J. Zaytoon – Systèmes dynamiques hybrides – traité ic2 série systèmes automatisés, Hermes, 2002.
- W. Zhang, M.S. Branicky, S.M. Philips – Stability of networked control systems – IEEE control Magazine, février 2001.

Remerciements

- C. Aubrun (CRAN, Nancy)
- JF Aubry (CRAN, Nancy)
- P. Barger (Heudiasyc, Compiègne)
- M. Bayart (LAGIS, Lille)
- C. Berbra (GIPSA-Lab, Grenoble)
- L. Cauffriez (LAMIH, Valenciennes)
- P. Charpentier (INRS, Nancy)
- J. Ciccotelli (INRS, Nancy)
- B. Conrard (LAGIS, Lille)
- J. Galdun (Univ. Kosice, Slovaquie)
- D. Genon-Catalot (LCIS, Valence)
- S. Gentil (GIPSA-Lab, Grenoble)
- R. Ghostine (CRAN, Nancy)
- M. Haffar (GIPSA-Lab, Grenoble)
- Z. Khan (GIPSA-Lab, Grenoble)
- S. Lesecq (GIPSA-Lab, Grenoble)
- J. Ligus (Univ. Kosice, Slovaquie)
- A. Mechraoui (GIPSA-Lab, Grenoble)
- M. Robert (CRAN, Nancy)
- E. Rondeau (CRAN, Nancy)
- C. Simon (CRAN, Nancy)
- MC Suhner (CRAN, Nancy)
- M. Wahl (INRETS, Villeneuve d'Ascq)
- P. Weber (CRAN, Nancy)
- …

Merci à tous pour votre attention !