École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

Paramètres *significatifs* dans le processus de modélisation de la disponibilité

Ahmed Bouabdallah, Nora Cuppens-Boulahia et Frédéric Cuppens

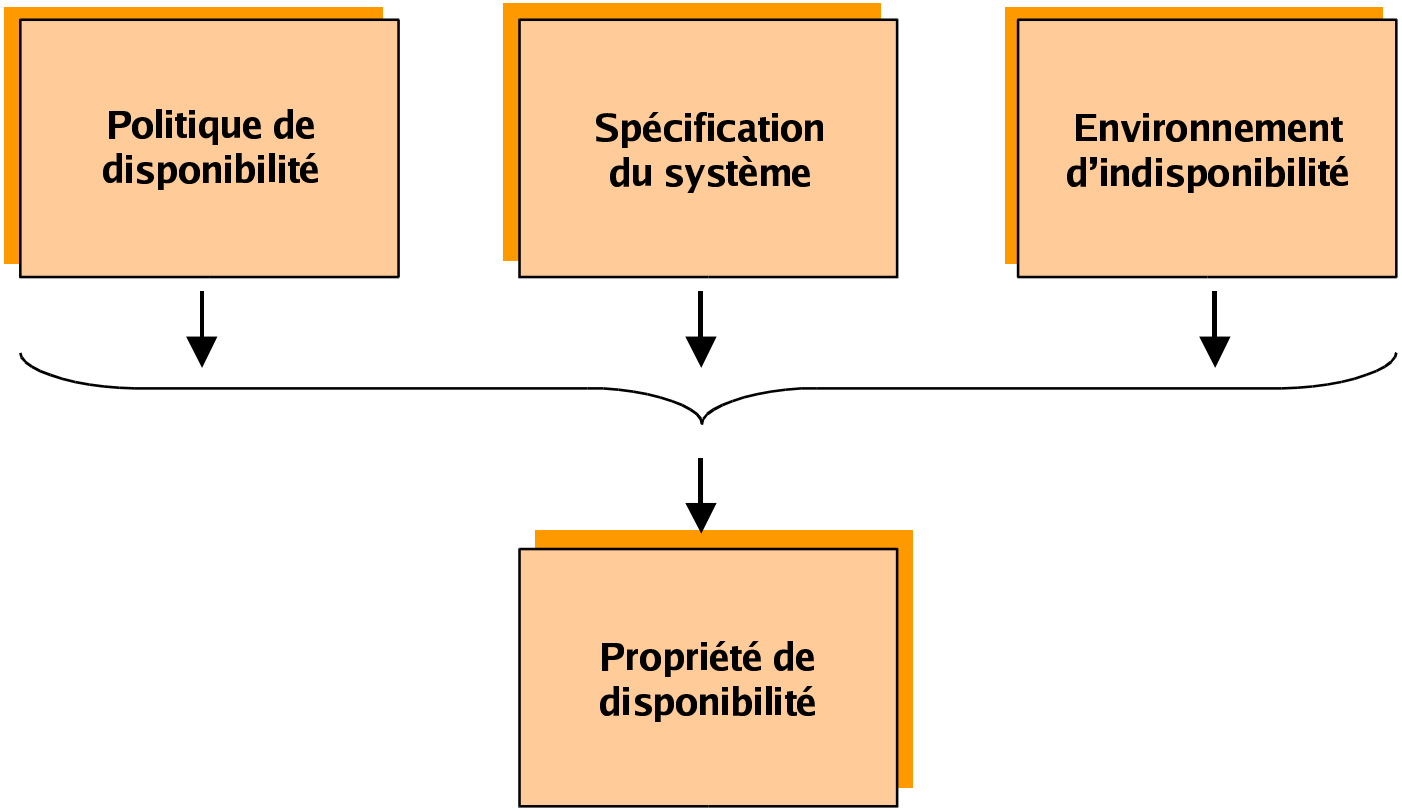
Rennes le 24 mars 2004

get

Plan

- Problématique
- Politique de disponibilité
- Environnement d'indisponibilité
- Spécification du système
- Propriétés de disponibilité
- Modélisation de la disponibilité
- Étude de cas
- Conclusion

Problématique

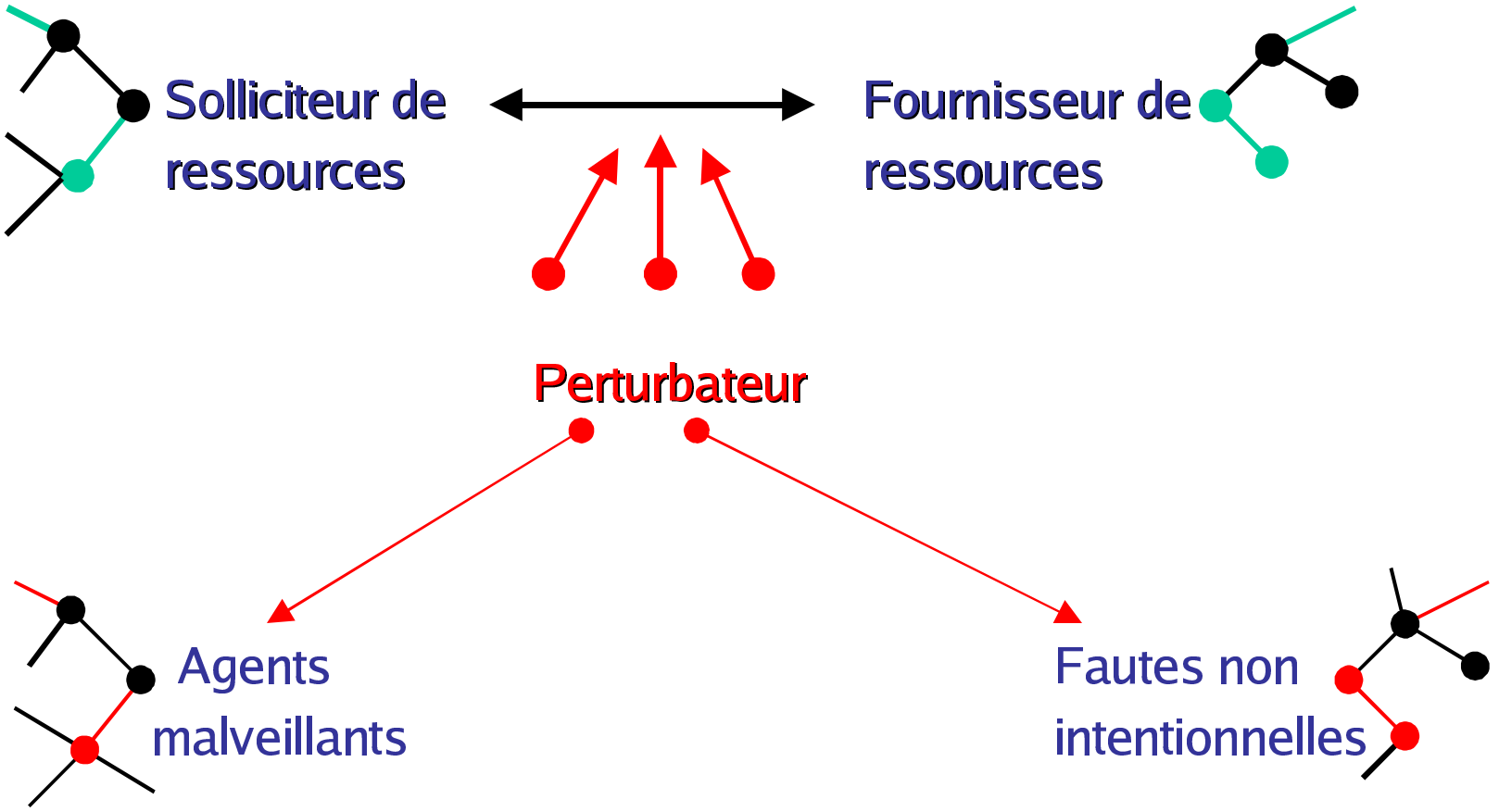


Politique de disponibilité

- Ressources
  - Notion de profil d'une ressource
    - Type
      - CPU, imprimante, segment mémoire, composant logiciel, composant matériel, bande passante réseau, fichier,…
    - Attribut*
      - Taille,type de processeur, largeur,…
    - État
      - Occupée, libre,…
    - Caractéristique
      - Partageable, consommable,…
  - Notion de profil d'utilisation d'une ressource
    - Spécification des conditions d'accès
      - Permissions / quotas

Politique de disponibilité

Rôle



Activité

- Services fournis par le système
- Nécessite de la disponibilité de ressources pour la réalisation

Politique de disponibilité

Permission

- Contrôle d'accès
  - Permission requête acceptée
  - Mais pas de garantie que l'activité pourra être réalisée
  - Insuffisant pour la disponibilité

Politique de disponibilité

Droit = Permission + obligation

- Permission pour le solliciteur d'accéder aux ressources
- Obligation pour le fournisseur de garantir que le solliciteur pourra réaliser son activité

- *on y revient plus loin*

Politique de disponibilité

- Contraintes pour le fournisseur
  - Priorité entre les droits
  - Délais de satisfaction des droits
- Contrat fournisseur/solliciteur
  - Taux et fréquence d'utilisation des droits
- Gestion des violations
  - *Légitimité du déni de service*
  - Gestion de listes noires

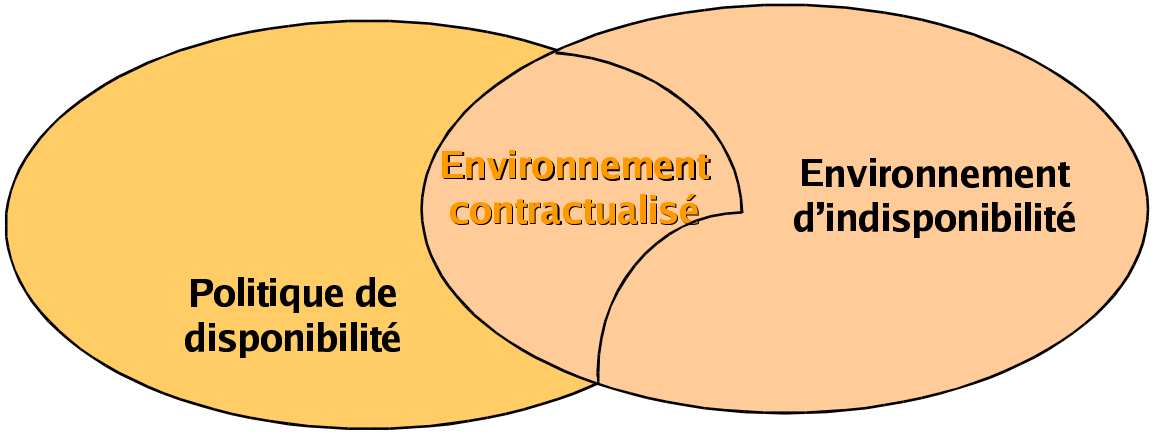
Environnement d'indisponibilité

- 3 parties
  - Environnement contractualisé
  - Environnement de fautes
  - Environnement de malveillances

Environnement d'indisponibilité

Environnement contractualisé

- Contrat entre le fournisseur et le solliciteur de ressources
- Obligation / interdiction pour le solliciteur de ressources
- Obligation / interdiction pour le fournisseur



Environnement d'indisponibilité

- Environnement de fautes
  - Fautes accidentelles
- Classification
  - Communication
    - erreur de routage, liaison défectueuse
  - Système
    - Panne courant, défaillance matérielle
  - Application
    - bogue de programmation
- Solutions connues
  - Redondance matérielle
  - Redondance logicielle
  - Réplication active, passive ou semi-active

Environnement d'indisponibilité

- Environnement de malveillance
  - Non respect des contrats
  - Attaques
- Attaque
  - Source, objectif, moyen, conséquence
- Exemples d'attaques
  - Virus, Ver,
  - Cheval de Troie, Bombe logique,
  - Buffer overflow,
  - DOS, DDOS

Environnement d'indisponibilité

- Classification des malveillances contre la disponibilité
  - Communication
    - Inondation
      - syn-flooding, smurfing,…
  - Système
    - DOS & DDOS
      - teardrop, land, Winnuke,…
  - Applicatif
    - Ver + Buffer overflow
      - Code red, Slammer,…

Environnement d'indisponibilité

- Catalogue de solutions
  - Communication
    - Partitionnement des ressources réseau
    - Filtrage
  - Système
    - Redondance passive
    - Diversification fonctionnelle
  - Applicatif
    - Preuve de programme
    - Redondance active
    - Déverminage

⇒ Objectifs

- Intégrer ces solutions dans une architecture de sécurité
- Prouver que des propriétés de disponibilité sont garanties
- Faire/trouver les hypothèses d'environnement nécessaires à la preuve

Spécification du système

Objectifs

- Décrire une architecture réseau et son environnement d'indisponibilité
- Décrire les composants de l'architecture
- ?? Spécifier les performances du système

Comment ?

- Automate,
- Chronique,
- Machine abstraite ou schéma Z,
- Logique temporelle,
- Tribu de Mona,
- ...

Propriétés de disponibilité

- Contraintes temporelles
  - Temps fini
  - Temps borné
- Respect des droits
- Respect de l'environnement contractuel

⇒ Objectif : prouver qu'un système donné garantit ces propriétés compte tenu d'un certain environnement d'indisponibilité

Modélisation de la disponibilité *(Réflexion en cours)*

$[Droit]_{dispo} = [Permission + obligation]_{Contrat}$

Matrice contrôle d'accès & matrice de transition entre domaines

Domaine sujet,
Type sujet ou objet

Contrôle des Permissions, contrôle de flux
Type et moyen d'accès

Politique accès

Matrice de contrôle de la disponibilité

Domaine demandeur,
Type ressource

Contrôle du profil de disponibilité
Priorité, taux, délais, quotas…

Politique dispo

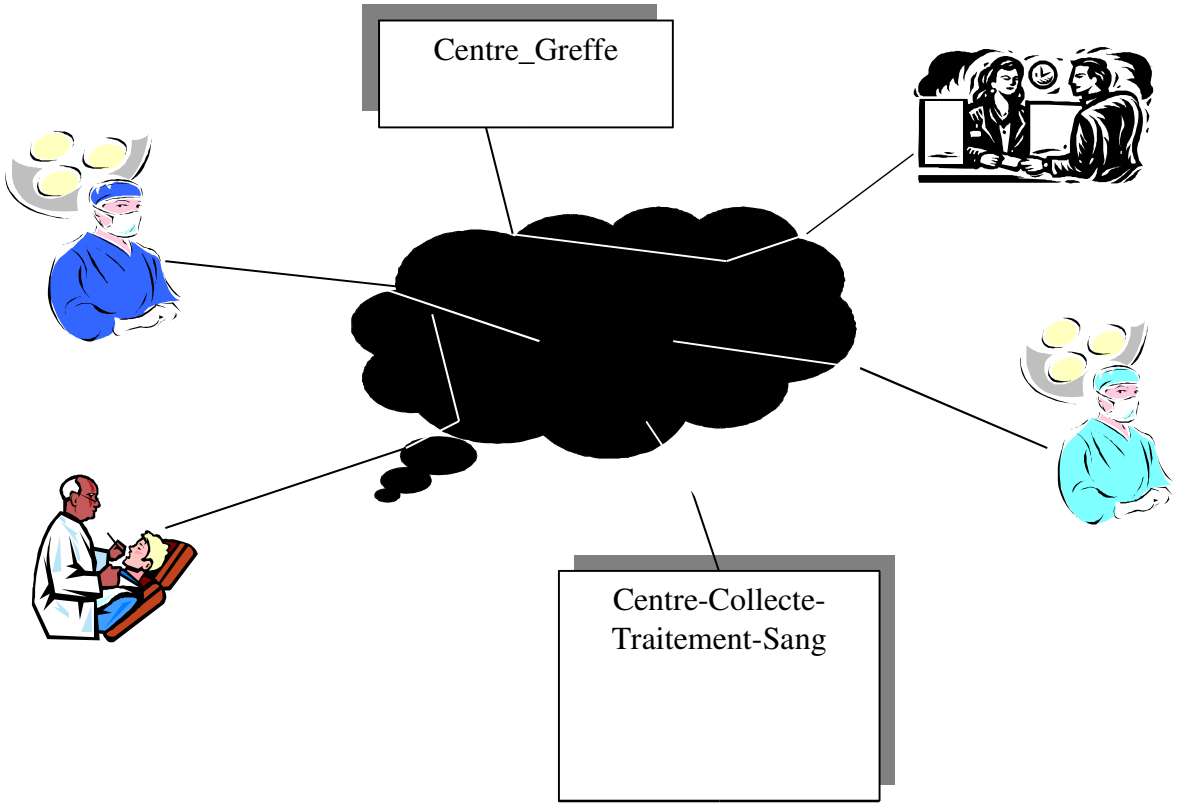
Dispo_Properties

Ψ [Propriétés confidentialité intégrité, Propriétés *contractuelles*]

Organisation(permissions, rôles, activités, vues) ←Or-BAC→ Organisation(Contexte)

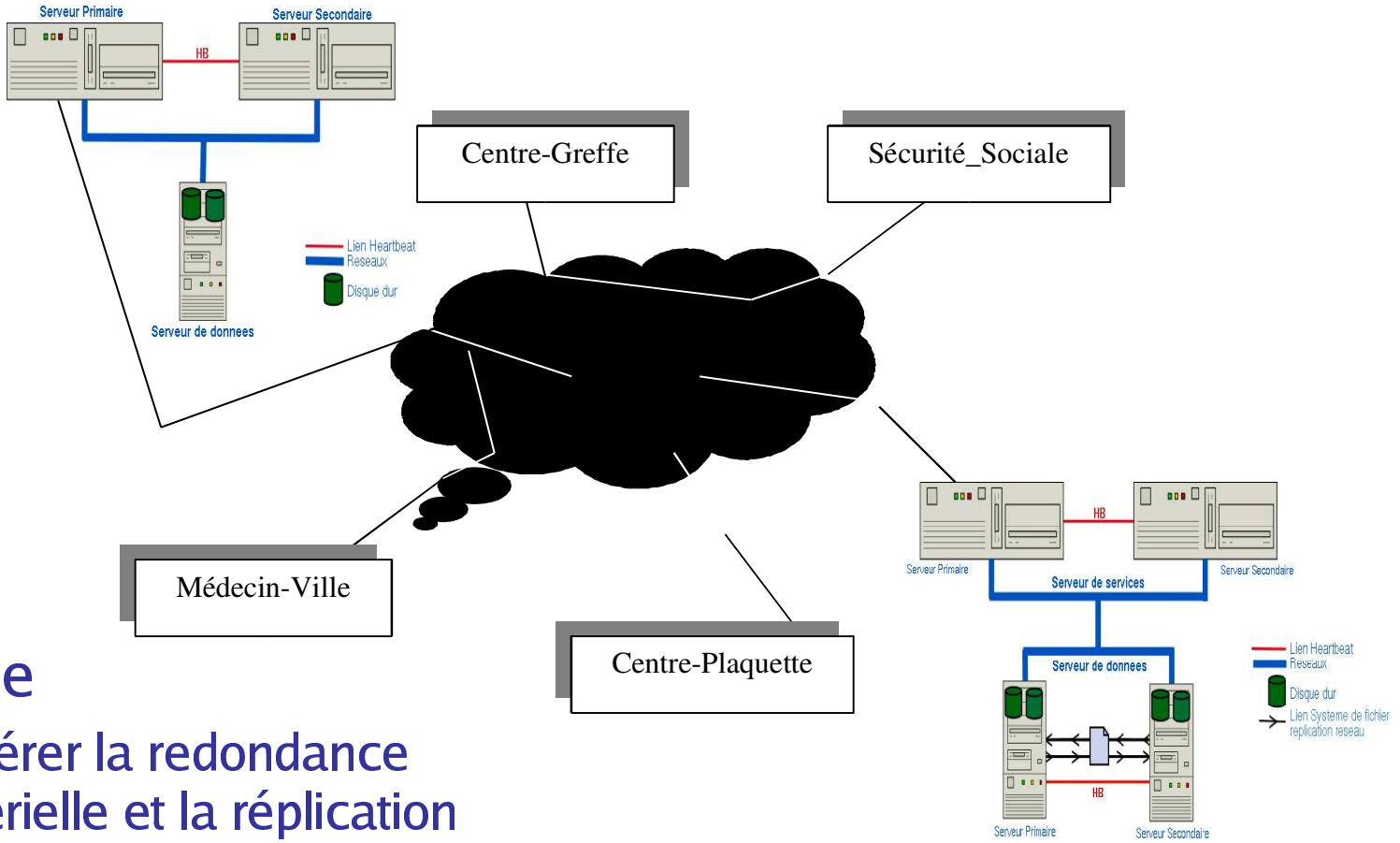
Étude de cas *(En cours d'élaboration)*

- Objectif
  - Assurer la disponibilité dans un tel réseau
- Notion de composabilité des propriétés de disponibilité



Étude de cas

Solutions de partage et de réplication dans le réseau de santé



- Hypothèse
  - Considérer la redondance matérielle et la réplication logicielle

Politique de sécurité du réseau de santé

- Les ressources
- Les rôles (clients) potentiels
- Politique d'accès
- Politique de disponibilité

?? Au niveau du réseau globale et au niveau de chaque entité

à développer…

- Environnement contractualisé du réseau
  - Contrat non respecté (abus) → Déni de service (sanction)
  - Contrat non respecté → possibilité de réponse (temps non borné)
- Environnement hostile
  - Vulnérabilités connues au niveau du réseau, système, application
- Environnement de fautes
  - Pannes des serveurs des entités du réseau et possibilité de reconfiguration

Conclusion

- Variante du modèle de disponibilité FCCS
  - Les éléments temporels « de granularité fine » sont dérivés de la politique de disponibilité et exprimés dans les propriétés de disponibilité à prouver
- Investigation du domaine de tolérance aux intrusions
  - Dériver des architectures de tolérance aux fautes
  - Les utiliser pour raffiner l'étude de cas
- Structurer les environnements
- Modéliser la politique de disponibilité

Conclusion

- Choix ouvert
  - Système de contrôle du trafic aérien
    - Le Coordinateur Automatique trafic aérien
      - Traitement du plan de vol
      - Traitement des données du radar
  - Protocole de transfert de données numériques
    - Transfert de données numériques entre les éléments de systèmes avioniques
    - Terminaux connectés au réseau
      - transmission et réception de données numériques en utilisant un protocole standard
      - Protocoles de bus de données avioniques
  - Système (algorithme) d'allocation de ressources
  - Et Banque.