Administration systèmes et réseaux

Sûreté de fonctionnement

Nicolas Hernandez

Cours de DUT informatique – 2ème année
IUT de Nantes – Département Informatique
2006 – 20??

Nantes, le February 4, 2018

Sûreté de fonctionnement – Sommaire

Définitions

Définition

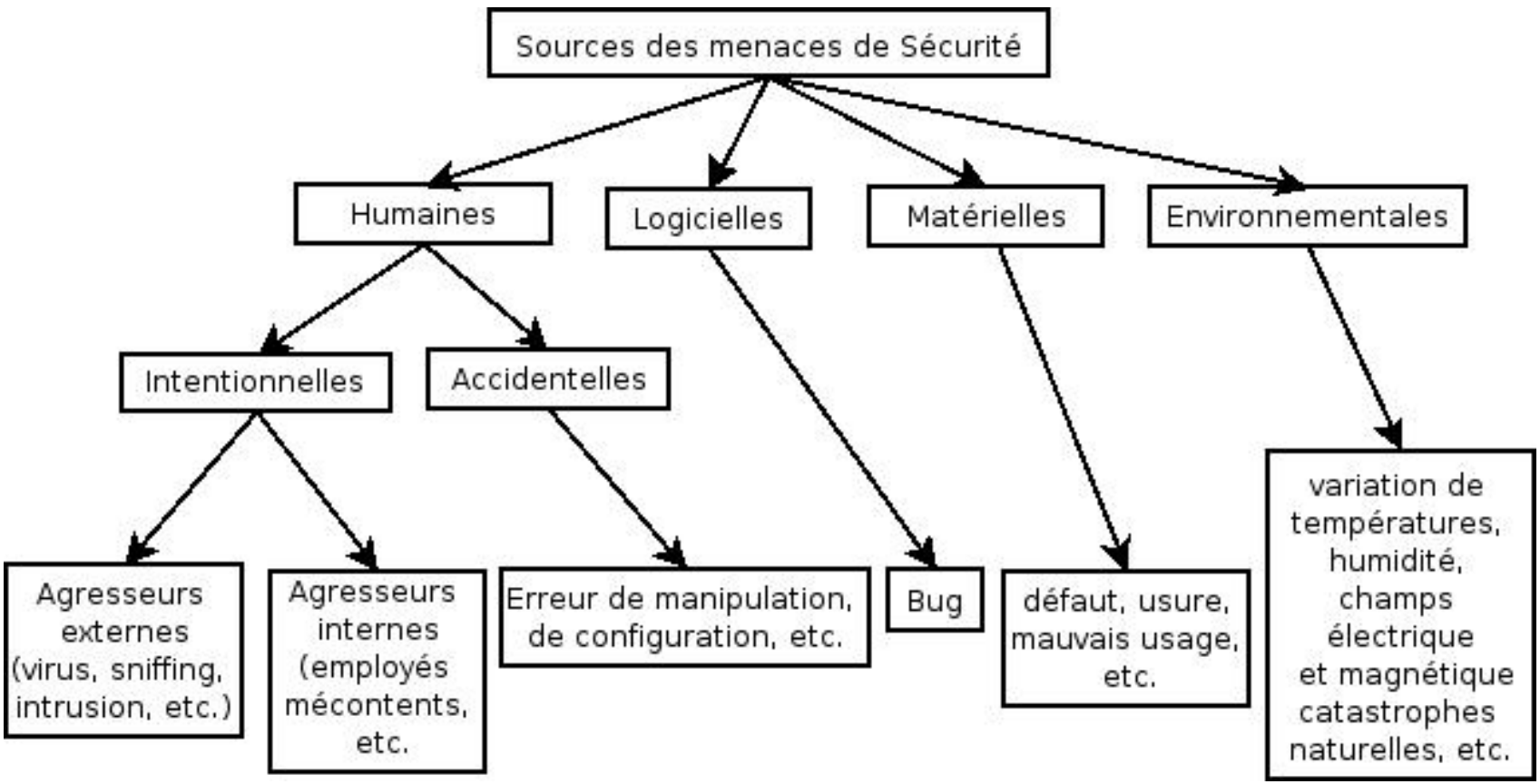
Sécurité regroupe tous les moyens et les mesures prises pour mettre le système[1] d'information à l'abri de toute agression

Définition

Sûreté de fonctionnement concerne l'ensemble des mesures prises et des moyens utilisés pour se prémunir contre les dysfonctionnements des équipements

[1] Dans le contexte de sûreté, on emploie souvent le terme *système* pour désigner un *(ensemble d') équipement(s)* et non *système d'exploitation*

Typologie des risques (i.e. des sources des menaces)



Quelques exemples de menaces de dysfonctionnement

complément à ceux de la figure précédente

- défaillance des équipements de traitement (panne)
- dysfonctionnement des mémoires de masse
- défaut des équipements réseau
- défaillance de la fourniture d'énergie involontaire (panne) ou volontaire (grève)
- agressions physiques comme l'incendie et les inondations

Les équipements à tolérance de panne (*fault tolerant*)

Principe

La fiabilité matérielle est obtenue par sélection des composants mais surtout
par la **redondance des éléments principaux**

Techniques de redondance

Définition

Miroitage (*mirroring*) : l'équipement de secours est maintenu en permanence dans le même état que l'équipement actif

Définition

Duplexage (*duplexing*) : équipement disponible qui prend automatiquement le relais de l'équipement défaillant

Les mémoires de masse : systèmes RAID

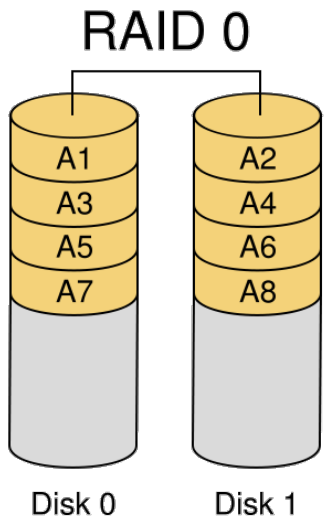
Définition

RAID (*Redundant Array of Independant*[2] *Disk*)

Différentes stratégies de tolérance de panne apportant différents niveaux de fiabilité et de performance

En pratique seuls les niveaux 1 et 5 sont utilisés

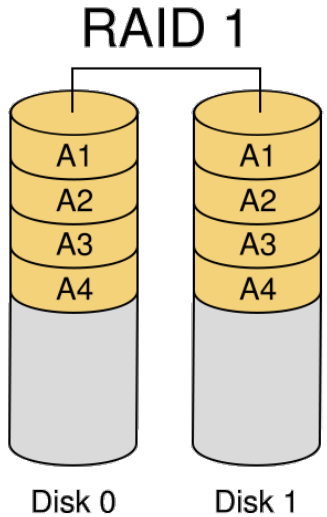
RAID 0, appelé "volume agrégé de bandes de données (*striping*)" ou "entrelacement de disques" : **augmente les performances** de la grappe en faisant travailler *n* disques durs en parallèle.
Chaque disque ne lit et écrit que *1 / n* des données.



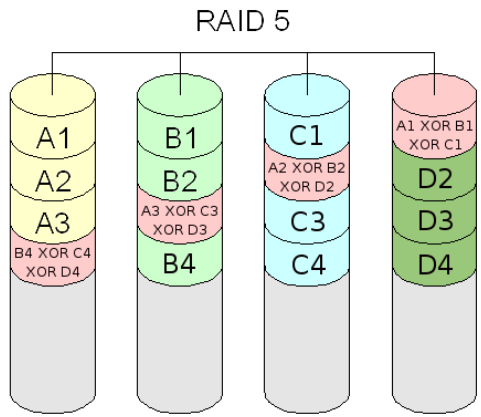
[2] Hist. *Inexpensive* i.e. bon marché et donc peu fiable

Les mémoires de masse : stratégies RAID

RAID 1, appelé "miroitage de disques" : **augmente la fiabilité** en dupliquant simultanément les données sur chacun des *n* disques de la grappe (accepte une défaillance de *n - 1* éléments)
Performance en lecture accrue et aucune incidence en écriture.



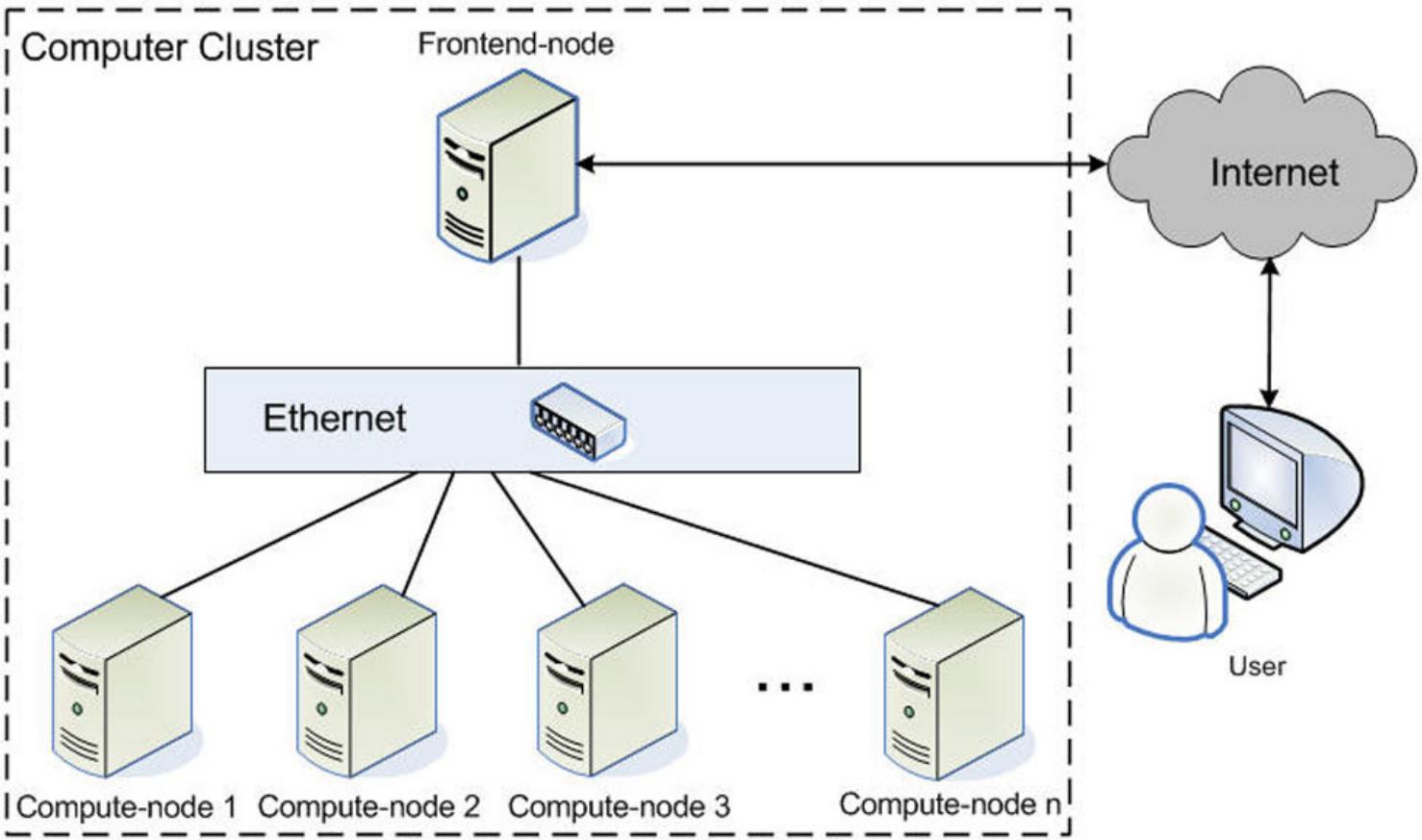
RAID 5, appelé "volume agrégé de bandes à parité répartie" : **cumule fiabilité** (grâce à codes de contrôle de parité répartis sur chacun des disques –en RAID 4 étaient stockés sur un seul disque)
et **bonne disponibilité** (grâce à la répartition de la parité possibilité de reconstruire un disque défaillant à partir des données et des informations de parités contenues sur les autres disques)



Duplexing de serveurs

Définition

Grappes de serveurs (*computer cluster*) : technique permettant une gestion globale d'un ensemble de machines comme un seul système



Duplexing de serveurs

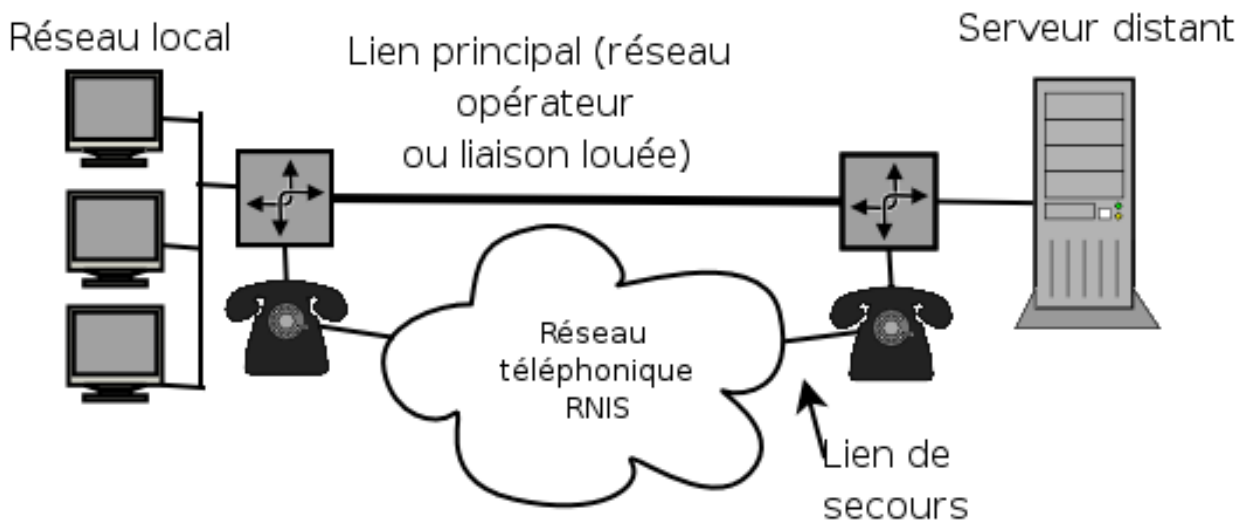
- Des noeuds *esclaves* dirigés par un *maître*
- Interconnectés sur un *FAST* LAN
- En général même *hardware* et même *operating system*
- Cas d'utilisation :
  - calcul scientifique intensif,
  - soutien de la disponibilité d'un service métier (e.g. web) par répartition des charges (*load balancing*)
- Distribution des requêtes sur différents serveurs selon différents algorithmes : Round-Robin (à tour de rôle), moins de connexions...

La sûreté des moyens de transport

Réalisée par la redondance des liens obtenue par le **maillage du réseau** ou par le **doublement des raccordements au réseau de l'opérateur**

Dans le second cas, en fonctionnement normal les charges sont équilibrées sur les deux liens

Compte tenu des coûts, les connexions de secours sont établies à la demande en utilisant généralement le réseau téléphonique



L'alimentation électrique

Définition

Onduleur : équipement qui fournit à partir de batteries le courant électrique d'alimentation du système

Deux types :

- **off-line** : relais en cas de défaillance du réseau d'alimentation sur des batteries chargées en continu
- **on-line** : intermédiaire permanent avec le réseau public, qui stabilise le courant en amplitude et en fréquence ; bascule sur le réseau public en cas de panne

L'autonomie de batterie étant généralement fixée à 20 minutes, un **générateur (groupe électrogène)** peut se substituer au réseau d'énergie public

Les contraintes thermiques

- **climatisation** des locaux informatiques entre 20 à 23°C
- **ventilation avec taux de poussière maximale** de $200\mu g/m^3/24$ heures
- **degré hygrométrique (humidité atmosphérique) correct** entre 40% et 85%

Définitions

Définitions

Disponibilité caractéristise le fait de fournir un service continu et non altéré (réseau, données, logiciel...)

Fiabilité probabilité pour que le système fonctionne correctement pendant une durée donnée dans les conditions définies (i.e. proba. de disponibilité)

Maintenabilité probabilité de retour à un bon fonctionnement dans un temps donné

Définitions

MTTR (*Mean Time To Repair*) : temps moyen de toute répération/remise en état du système

MTBF (*Mean Time Between Failure*) : temps moyen de bon fonctionnement (entre deux pannes successives)

Relations entre Disponibilité et MTTR–MTBF

La **D**isponibilité est définie par :

$$D = \frac{MTBF}{MTBF + MTTR}$$

L'**I**ndisponibilité comme son complément :

$$I = 1 - D = \frac{MTTR}{MTBF + MTTR}$$

On a donc :

$$\frac{I}{D} = \frac{MTTR}{MTBF}$$

Pour rendre un système efficace on peut :

- augmenter le MTBF mais les composants réseaux seront plus onéreux
- diminuer le MTTR mais la maintenance sera plus coûteuse

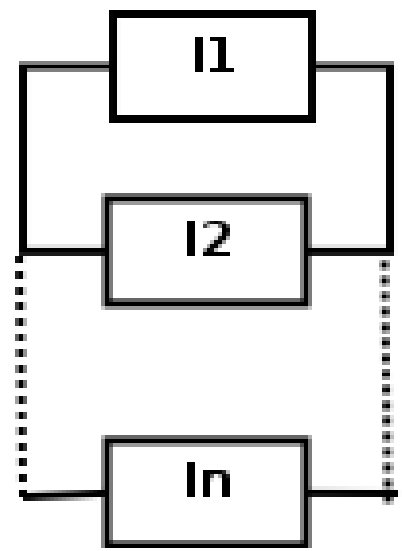
Les structures de fiabilité

Propriété

La mesure de la disponibilité totale d'un système dépend de sa structure.

Deux structures élémentaires :

La structure parallèle



La structure série

Les structures de fiabilité

La structure série : la **D**isponibilité totale est plus petite que celle du composant qui a la plus faible disponibilité

$$D_{totale} = D_1 * D_2 * \ldots * D_n$$

L'**I**ndisponibilité est alors $I_{totale} = 1 - D_{totale}$
Et si $D \approx 1$ (I très petit) alors $I_{totale} = \sum_1^n I_n$

On peut aussi montrer : $MTBF_{serie} = \frac{1}{\sum_{i=1}^{i=n}(\frac{1}{MTBF_i})}$

La structure parallèle : la **I**ndisponibilité totale est plus petite que celle du composant qui a la plus faible indisponibilité

$$I_{totale} = I_1 * I_2 * \ldots * I_n$$

La **D**isponibilité est alors $D_{totale} = 1 - I_{totale}$

De même on peut aussi montrer : $MTTR_{parallele} = \frac{1}{\sum_{i=1}^{i=n}(\frac{1}{MTTR_i})}$

Quizz de synthèse sur la sureté de fonctionnement

- Quelle est la solution clé aux problèmes de sûreté de fonctionnement (crash disque, serveur surchargée, etc.) ?
- Que signifie les acronymes MTTR et MTBF ? Et comment se définissent-ils l'un par rapport à l'autre ?