# Introduction à la sûreté de fonctionnement des ordinateurs

S. Natkin

Octobre 2002

# DOIT ON AVOIR PEUR DES ORDINATEURS?
# LE COMPLEXE DE FRANKENSTEIN

Importance croissante du rôle de la diffusion de l'information via des systèmes techniques de plus en plus complexes, dans des domaines de plus en plus variés.

Par exemple:

- Le contrôle de processus critiques (transport, énergie…)
- Les relations commerciales (commerce et les électronique et monétique)
- La gestion de données confidentielles (secrets militaires ou industriels, données personnelles…)

La peur d 'une technologie nouvelle, incomplètement maîtrisée, l'immaturité sociale dans la pratique de ces nouveaux outils induit une peur => Complexe de Frankenstein

# DOIT ON AVOIR PEUR DES ORDINATEURS?
# LES RISQUES LIES A LA COMPLEXITE

L ’informatique induit la possibilité de construire rapidement et à faible coût des systèmes de traitement de l ’information d ’une incroyable complexité:

Peu de limites aux demandes des utilisateurs qui ne maîtrisent pas la viabilité et la fragilité intrinsèque de cette expression de besoins.

Les limites des possibilités de validation de ces systèmes par rapport à ce qu’ils doivent faire et surtout ce qu ’ils ne doivent pas faire.

L ’incapacité d ’évaluer correctement les conséquences des éventuelles défaillances et donc, a fortiori, des agressions.

L ’incapacité de vérifier à posteriori ce que fait un système automatisé de traitement de l ’information.

# L ’ORIGINE DES RISQUES EST SOUVENT HUMAINE

- Défaillances des systèmes techniques (usure des équipements, panne catalectique, catastrophes naturelles)
- Erreur de conception
- Erreur de réalisation
- Erreur d ’exploitation
  - La négligence , l ’inattention…
  - Les fautes réelles (violation d ’une procédure formalisée)
- Malveillance à caractère ludique
- Fraude, Vol
- Sabotage

# QUELQUES STATISTIQUES :
# COUT DES SINISTRES EN MFF EN 1996
# (Clusif)

| | | |
|---|---|---|
| **Accidents** | | |
| Physiques (incendie, explosion, dégât des eaux…) | 1630 | 12,81 |
| Pannes | 1110 | 8,73 |
| Force majeure | 35 | 0,28 |
| Perte services essentiels (Télécoms, électricité…) | 280 | 2,20 |
| **Total** | **3055** | **24,02** |
| | | |
| **Erreurs humaines** | | |
| Utilisation | 800 | 6,29 |
| Conception, Réalisation | 1020 | 8,02 |
| **Total** | **1820** | **14,31** |
| | | |
| **Malveillances** | | |
| Vol, vandalisme physique | 240 | 1,89 |
| Fraude non physique | 2300 | 18,08 |
| Sabotage | 5 | 0,04 |
| Attaque logique | 1090 | 8,57 |
| Divulgation | 1100 | 8,65 |
| Autres (copies de logiciels) | 3110 | 24,45 |
| **Total** | **7845** | **61,67** |
| | | |
| **TOTAL** | **12720** | **100** |

# DÉFINITIONS ET TERMINOLOGIE

- [Laprie89] : “la sûreté de fonctionnement d’un système informatique est la propriété qui permet de placer une confiance justifiée dans le service qu’il délivre.
- Service rendu par le système : comportement perçu par l’utilisateur
  - environnement fonctionnel (procédé,autre produit, opérateur)
  - environnement non fonctionnel (température, environnement electromagnétique,....)
  - mission et durée de mission
- Défaillance : service délivré non acceptable (par rapport à la fonction attendue du système)

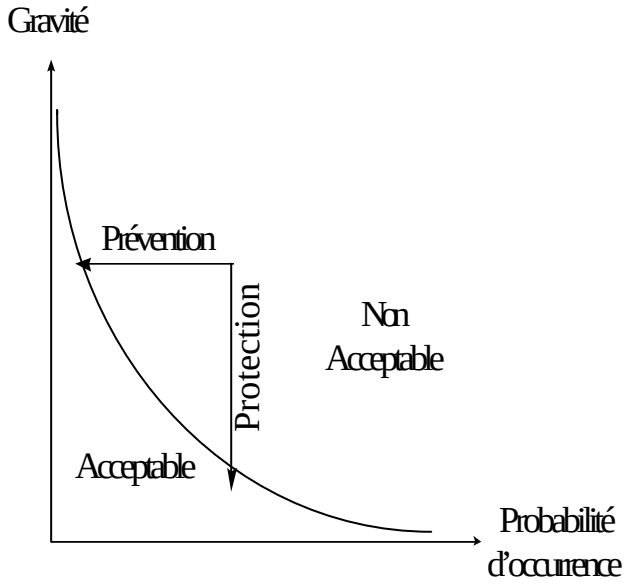
# TYPES DE DÉFAILLANCES (1)

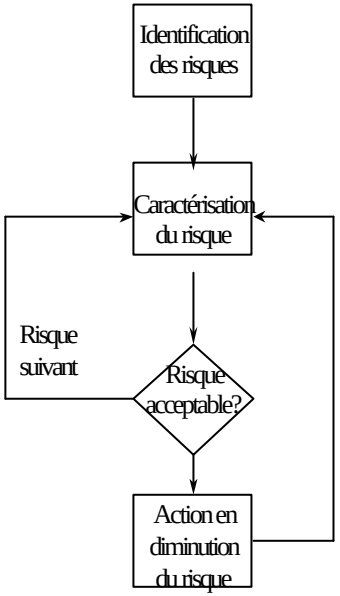
- Caractéristiques externes des défaillances
  - défaillance statique : le système produit un  résultat non correct de manière permanente (aspects fonctionnels)
  - défaillance dynamique : le système a un régime transitoire pendant lequel le système produit un résultat faux puis atteint un régime permanent durant lequel les sorties sont correctes (aspects temporels)
  - défaillance durable : le système produit des résultats erronés de manière persistente
  - défaillance transitoire
  - défaillance cohérente ou incohérente suivant que la perception de la défaillance est identique pour les utilisateurs ou non.

# TYPES DES DÉFAILLANCES (2)

- Classification des défaillances pour les systèmes répartis (Dolev, Cristian)
  - panne franche
  - panne d'omission
  - panne temporelle
  - panne byzantine
  - panne franche < panne d'omission < panne temporelle < panne byzantine
- Gravité ou mesure des effets sur la mission

# CLASSEMENT DES CONSÉQUENCES DES DÉFAILLANCES



# NIVEAUX DE GRAVITÉ

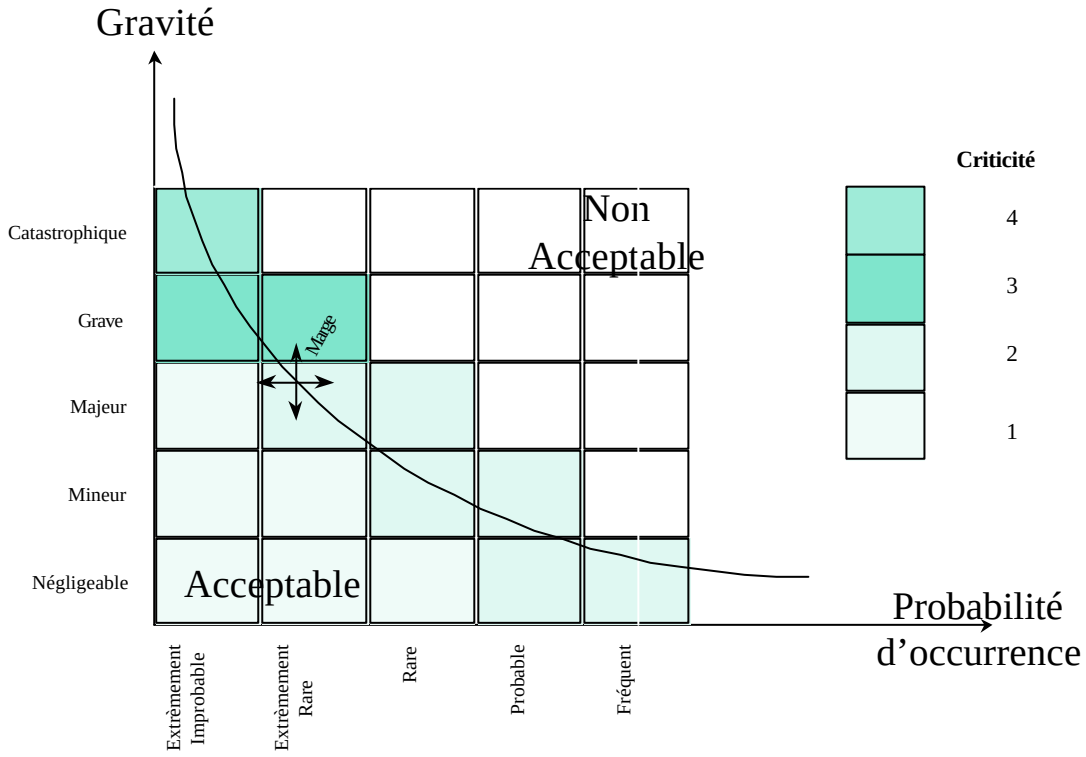
Classification des risques selon une échelle, qui peut dépendredu domaine applicatif

| Niveau de gravité | Code de gravité | Description |
|---|---|---|
| Catastrophique | 0A | Risque de perte de vie humaine ou agression sur le personnel d'exploitation..<br>Effets sur l'environnement à long terme. |
| Grave | 0B | Destruction importante de biens qui interrompent les activités sur une longue période.<br>Effets sur l'environnement à court terme. |
| Majeur | 1 | Perte de mission.<br>Endommagement d'un bien. |
| Mineur | 2 | Mission dégradée. |
| Négligeable | 3 | Sans effet sensible sur le déroulement de la mission. |

# NIVEAUX DE PROBABILITÉ

| Niveaux de probabilité | Code de Probabilité |
|---|---|
| Extrêmement improbable | PA |
| Extrêmement Rare | PB |
| Rare | PC |
| Probable | PD |
| Fréquent | PE |

# NIVEAUX DE GRAVITÉ ET NIVEAUX DE PROBABILITÉ



# DÉFAILLANCES, ERREURS, FAUTES

- Erreur : état (partiel) susceptible d'entraîner une défaillance
  - latente/détectée
  - propagation d'erreur, produit d'autres erreurs
- Faute : cause adjugée ou supposée d'une erreur
- Défaillance
  - manifestation d'une erreur qui par propagation traverse la frontière du système avec son environnement.
- ...defaillance -> faute -> erreur -> défaillance -> faute ->....

# LES FAUTES : CARACTÉRISTIQUES

- Fautes [Laprie]
  - Cause phénoménologiques
    - fautes physiques
    - fautes dûes à l'homme
  - Nature
    - accidentelle
    - intentionnelle
  - Phase d'occurrence
    - conception
    - exploitation
  - Frontière du système
    - faute interne
    - faute externe
  - Persistence
    - temporaire
    - permanente

# PRÉVISION DES FAUTES

- Evaluer prévisionnellement le comportement du système par rapport à l'occurrence des fautes
  - Examiner les défaillances des composants d'un système et leurs conséquences sur la sûreté de fonctionnement
- Etats observables du système
  - Service correct : accomplit la (les) fonctions du système
  - Service incorrect : non (accomplit la (les) fonctions du système)
- Attributs principaux
  - Fiabilité
  - Disponibilité
  - Sécurité-innocuité

# Attributs de la sûreté de fonctionnement

Disponibilité: capacité instantanée a rendre le service

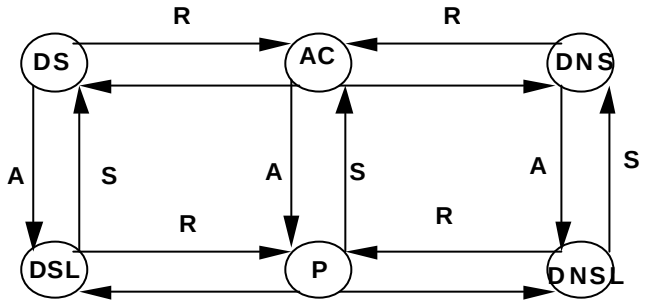
Fiabilité: continuité du service

Securité-innocuité (safety): non occurrence de défaillances a caractère catastrophique

Maintenabilité: facilite de retour a un état sans erreur après défaillance

Securité-confidentialité (security): non occurrence de défaillances causées par des fautes intentionnelles

# graphes de sûreté de fonctionnement



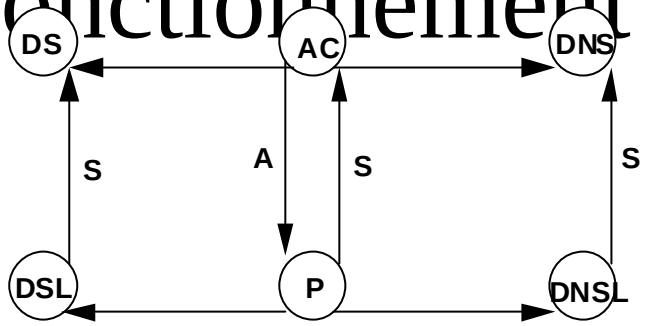

**GRAPHE DE DISPONIBILITÉ**

**AC: Actif**
**P:Passif**
**DS:Défaillance Sécuritaire**
**DSL:Défaillance Sécuritaire Latente**
**DNS:Défaillance Non Sécuritaire**
**DNSL:Défaillance Non Sécuritaire Latente**

**R: Réparation**
**A: Activation**
**S: Sollicitation**
**- > Défaillance**

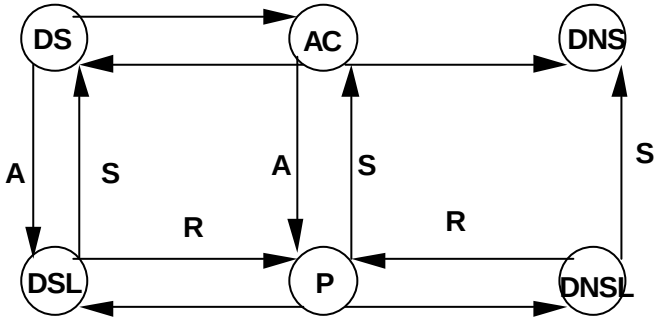
$$A(t) = P_{AC}(t) + P_{P}(t) + P_{DSL}(t) + P_{DNSL}(t)$$

# graphes de sûreté de fonctionnement




**GRAPHE ASSOCIE A LA FIABILIITE**

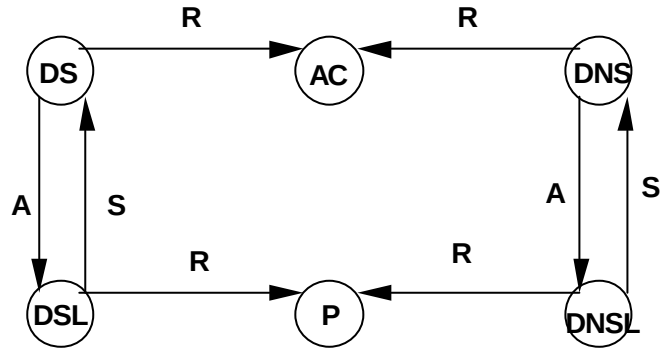
$$R(t) = P_{AC}(t) + P_{P}(t) + P_{DSL}(t) + P_{DNSL}(t)$$




**GRAPHE ASSOCIE A LA SECURITE**

$$S(t) = P_{AC}(t) + P_{P}(t) + P_{DSL}(t) + P_{DNSL}(t) + P_{DS}(t)$$

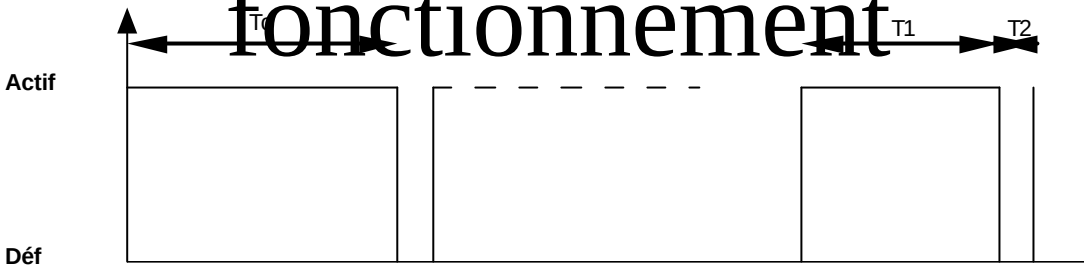
# graphes de sûreté de fonctionnement




GRAPHE ASSOCIE A LA MAINTENABLIITE

$$M(t) = P_{AC}(t) + P_{P}(t)$$

# Paramètres de la sûreté de fonctionnement




**Mean Time to First Failure**

**MTFF = E( To )**

**Mean Up Time**

**MUT= E( T1 )**

**Mean Down Time**

**MDT= E( T2 )**

**Mean Time Between Failures**

**MTBF = E( T1 + T2 ) = MUT+MDT**

**Disponililé asymptotique**

**A* = lim A( t ) = MUT/ MTBF**

# Hiérarchisation des classes

panne franche < panne d’omission
< panne temporelle < panne byzantine

**En effet :**

**défaillance franche => pas de réponse à une entrée**

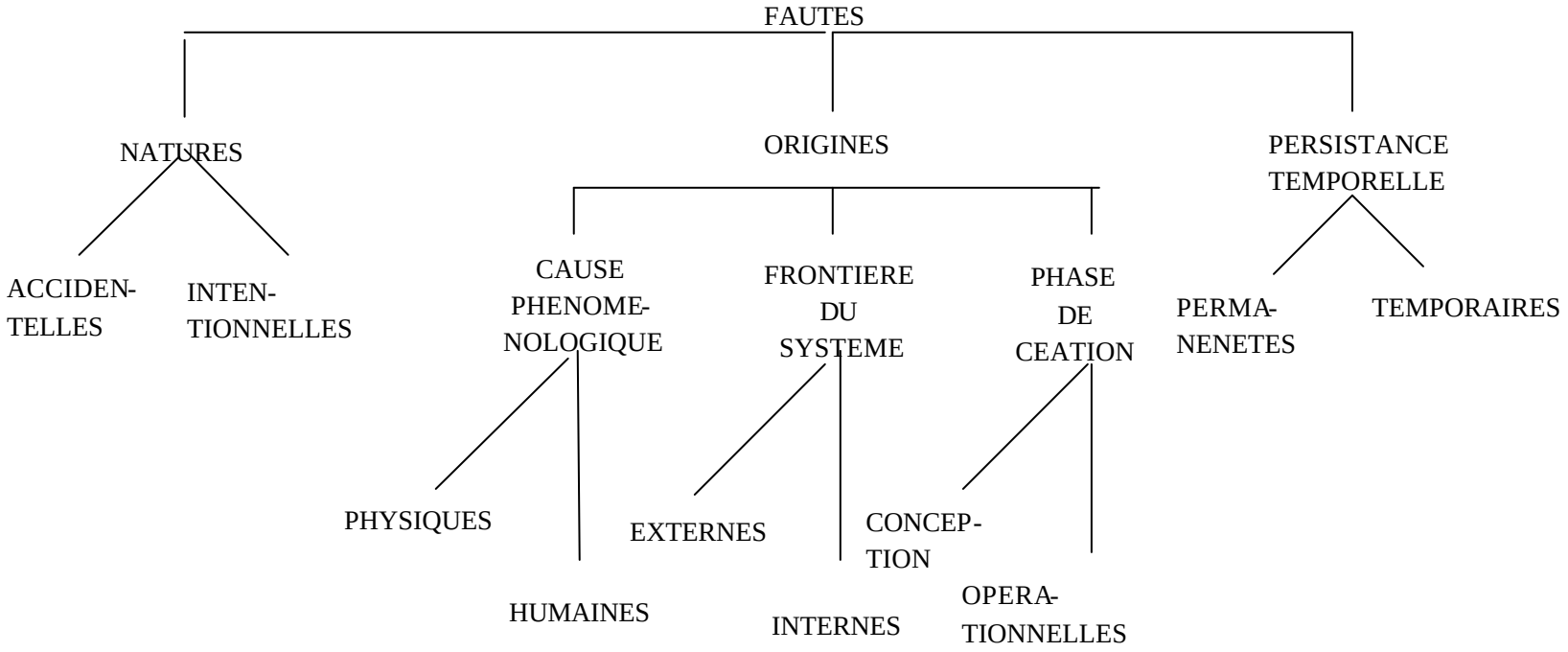
**défaillance transitoire => délai de réponse à un événement infini.**

**défaillance quelconque => défaillance temporelle**

**On réalise des composants sous des hypothèses de défaillance appartenant à l'une des classes précédentes pour tolérer cette classe.**

**L'une des hypothèses les plus fréquentes est la tolérance aux défaillances intermittentes (d'omission).**

# Les Fautes : caractéristiques (Laprie)



# phase d’occurrence des fautes (1)

- fautes de spécification
  - erreur de frontière
  - incomplétude
  - incohérence
- fautes de conception
  - erreur de raffinement
    - faute au niveau d’un module (production de sorties non conformes à la spécification du module)
    - fautes dans les interfaces entre modules
  - non respect de contraintes technologiques (utilisation de ressources, partage de ressources,...)

# phase d’occurrence des fautes (2)

- fautes de production
  - matériel
  - logiciel
    - génération de code à partir d’un modèle de conception (manuel ou générateur)
    - passer du programme source à l’exécutable : l’exécutable doit produire un comportement équivalent à l’interprétation du du source (avec la sémantique du langage) => deux sources d’erreur la défaillance du compilateur et les ambiguités sémantiques du langage de programmation

# Bibliographie

- LIS : Guide de la Sûreté de Fonctionnement, CEPADUES Editions
    - Qui renvoie à une bibliographie très importante
- Sûreté de fonctionnement…

G. Mottet