





***NOS ACTIONS
PERMANENTES
= prôner
l'informatisation
mais...***

Aujourd' hui nous débattons
d'un sujet délicat et
probablement bien présent



30 Mars

**« L'informatique
hospitalière... soudain
tout se plante
quel est votre plan B? »**

Des questions importantes,
des réponses

- J.Bellon -



**1= sûreté
du fonctionnement ?**

*= le niveau de confiance
d'un système informatique
pour les utilisateurs*

*Soit un service approprié
correspondant
aux attentes*



➡ **2 = Quid du
dysfonctionnement local ?**

*Prévention , tolérance
élimination et prévision
des fautes par anticipation*



➡ **3 = La disponibilité ?**

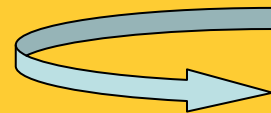
Différents niveaux

Haute disponibilité (24/24)

Disponibilité

Fiabilité

Continuité du service

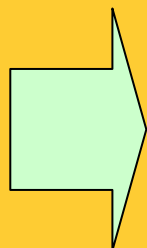




La disponibilité en %

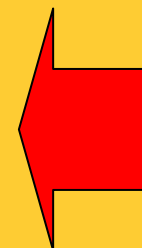
Taux de disponibilité

Durée d'indisponibilité



97%
98%
99%
99,9%
99,99%
99,999%
99,9999%

11 jours
7 jours
3 jours et 15 heures
8 heures et 48 minutes
53 minutes
5 minutes
32 secondes





4 =

Evaluer les risques ?

Un constat important :

La panne d'un système informatique peut causer une perte de productivité et d'argent, voire des pertes matérielles ou humaines dans certains cas critiques.

Actions à mener

- ***évaluer les risques liés à un dysfonctionnement (faute) d'une des composantes du système d'information***
- ***prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident.***



Equation des risques ?

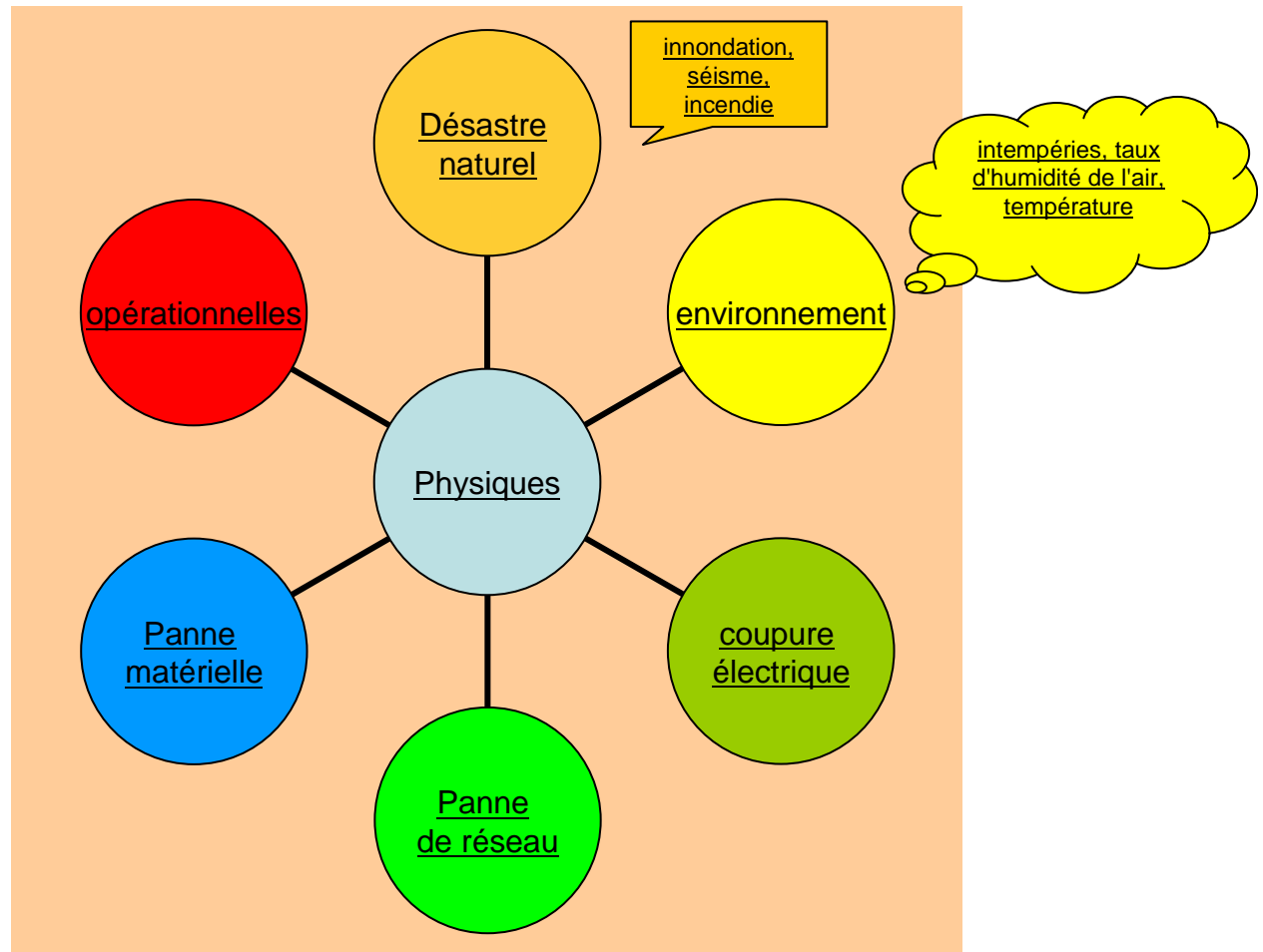
$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$

- la **menace** = le type d'action susceptible de nuire dans l'absolu,
- la **vulnérabilité** = représente le niveau d'exposition
dans un contexte particulier.
- la **contre-mesure** = l'ensemble des actions
en prévention de la menace.
- **Les contre-mesures à mettre en oeuvre**
 - = des solutions techniques
 - = des mesures de formation et de sensibilisation
 - = ainsi qu'un ensemble de règles clairement définies



5 =

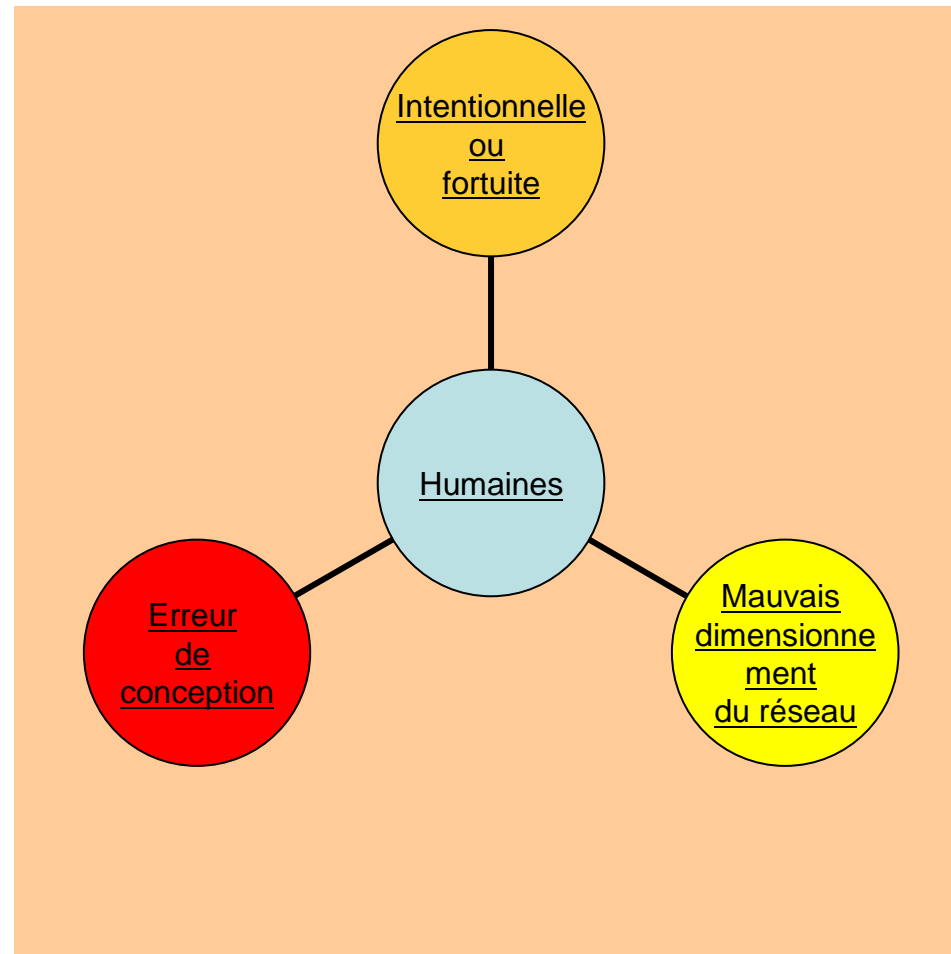
L'origine des pannes ?





5 =

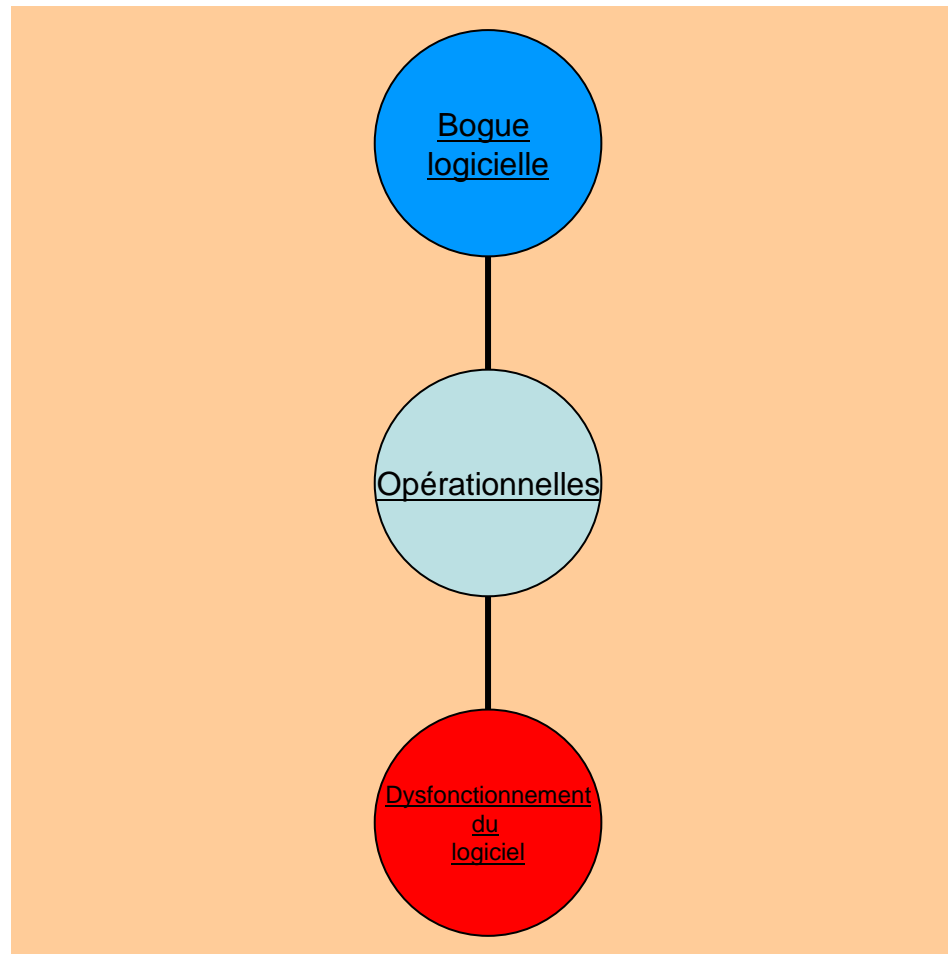
L'origine des pannes ?





5 =

L'origine des pannes ?





5 =

Et les solutions ?

- mettre en place des mécanismes de **redondance**, en dupliquant les ressources critiques.
- fonctionner malgré une défaillance = ***fault tolerance***.
- « **Fail-Over Service** »
- remplacement à chaud des éléments matériels fautifs (en anglais « *hot swappable* »)
- installer des mécanismes de sauvegardes, idéalement sur des sites distants pour garantir la pérennité des données
= **les données correspondant à une date donnée.**



6 =

Sécurité informatique ?

- L'**intégrité** = garantir que les données sont bien celles que l'on croit être
- La **confidentialité** = consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction
- La **disponibilité** = maintenir le bon fonctionnement du système d'information
- La **non répudiation** = garantir qu'une transaction ne peut être niée
- L'**authentification** = assurer que seules les personnes autorisées aient accès aux ressources.



7 =

Approche globale ?

- La **sensibilisation** des utilisateurs aux problèmes de sécurité
- La sécurité **logique** = la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- La sécurité des **télécommunications** = technologies réseau, serveurs de l'entreprise réseaux d'accès,
- La sécurité **physique** =
la sécurité au niveau des infrastructures matérielles
salles sécurisées,
lieux ouverts au public,
espaces communs de l'entreprise,
postes de travail des personnels,



8 =

Politique de sécurité en quatre étapes :

- **Identifier les besoins en terme de sécurité**,
les risques informatiques pesant sur l'entreprise
et leurs éventuelles conséquences
- **Elaborer des règles et des procédures** à mettre en oeuvre
dans les différents services de l'organisation
pour les risques identifiés
- **Surveiller et détecter les vulnérabilités** du système
d'information et se tenir informé des failles sur les applications
et matériels utilisés
- **Définir les actions à entreprendre** et les personnes à
contacter en cas de détection d'une menace.

