

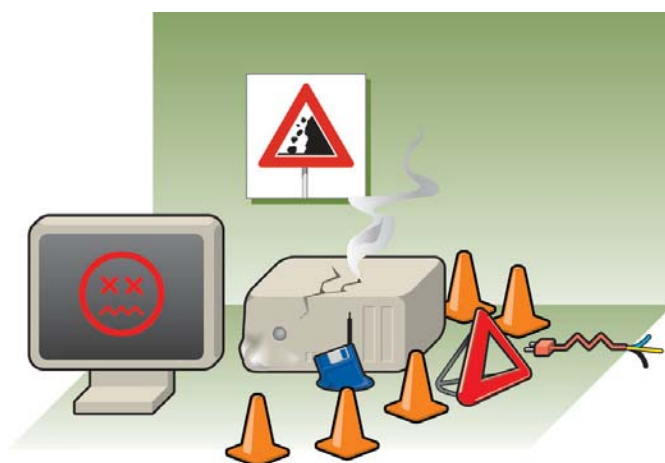
Résumé

Cette fiche dresse une liste plus ou moins exhaustive des pannes physiques qui peuvent mettre en péril tout ou partie d'un système informatique.

Certaines pannes décrites dans ce document ne sont pas directement applicables à un ordinateur personnel mais bien à un système incluant une salle informatique, des éléments réseaux et de télécommunication.

Table des matières

- 1 Qu'entend-on par panne physique ? →
- 2 Quelles peuvent être les causes des pannes ? →
- 3 Une catégorisation selon les systèmes concernés →
- 4 Les bases d'estimation des préjudices →
- 5 Statistiques →
- 6 Les vulnérabilités exploitées →
- 7 Les contre-mesures →



1 Qu'entend-on par panne physique ?

On entend par panne physique la rupture de service ou le mauvais fonctionnement d'un ou plusieurs éléments physiques constitutifs d'un système informatique.

2 Quelles peuvent être les causes des pannes ?

Il y a autant de causes de pannes possibles que d'éléments ou de couches constitutives d'un système informatique. Toutefois, il est nécessaire de faire la différence entre les catégories suivantes :

2.1 Les pannes logicielles et les pannes de matériel

Il faut faire la différence entre les pannes touchant directement un élément physique d'un système et les pannes touchant la couche logicielle des éléments physiques. En effet, la plupart des équipements électroniques exercent leur fonction grâce à des logiciels. Le mauvais fonctionnement de ces couches logicielles peuvent également rendre l'équipement inopérant, voire le détruire.

2.2 Le rôle de l'environnement

Un grand nombre d'indisponibilités de solutions informatiques ne sont pas directement liées à un équipement informatique, mais simplement au fait que les conditions générales de bon fonctionnement ne sont plus données :

- ➔ Pannes d'alimentation en courant (220-230 V).
- ➔ Pannes de climatisation, provoquant une surchauffe.

La survenance de tels événements extérieurs peut entraîner une indisponibilité du système, mais peut également provoquer des pannes physiques diverses au niveau des éléments.

[→ suite](#)

3

Une catégorisation selon les systèmes concernés

La catégorisation des pannes physiques se base sur la partie du système directement concerné, et fait une différence entre :

3.1 Les pannes touchant les fonctions de calcul

On inclut dans cette catégorie toutes les pannes qui empêchent le bon fonctionnement du traitement des données par un serveur ou un ordinateur personnel. Les pannes à ce niveau vont concerner des éléments physiques tels que :

- La mémoire.
- Le processeur.
- La carte mère.

3.2 Les pannes touchant les systèmes de stockage

Cette catégorie regroupe toutes les pannes ayant des conséquences sur l'accès aux données, que ce soit en écriture ou en lecture.

Les pannes pouvant concerner différentes parties d'un système informatique sont :

- Le stockage interne d'un serveur.
- Le stockage interne d'un ordinateur personnel.
- La solution de réseau de stockage SAN (Storage Area Network).
- Les systèmes de sauvegarde de données (bande magnétique, cassettes...).

Les pannes pouvant être causées par des défaillances à différents niveaux, tels que :

- les supports de stockage (disque dur, bande, cassette, etc...),
- le mécanisme de lecture/écriture (contrôleur, lecteurs de bandes/disquettes, etc...),
- la couche logicielle embarquée sur certains de ces composants.

3.3 Les pannes touchant la connectique

On peut regrouper sous ce titre toutes les pannes causant une incapacité d'accès à l'une ou l'autre ressource du système.

Ces pannes peuvent donc concerner différentes parties de l'architecture, telles que :

- Le réseau d'entreprise comme LAN (Local Area Network) et WAN (Wide Area Network).
- Les accès télécommunications.
- Les réseaux de fibre optique (SAN).

Les pannes pouvant survenir à plusieurs niveaux :

- Les équipements (routeur, commutateurs).
- La couche câblage (câble, panneaux de connexions).
- La couche logicielle embarquée sur certains de ces composants.

4

Les bases d'estimation des préjudices

L'estimation des préjudices subis va évidemment dépendre des domaines touchés par la ou les pannes physiques, ainsi que par la faculté de faire face aux éventuelles altérations des données et systèmes.

4.1 La perte d'équipements

La panne peut parfois nécessiter le remplacement de l'équipement concerné. Le coût direct équivaut donc à la valeur d'achat et de mise en fonction de cet équipement.

Il est vivement conseillé d'éviter l'utilisation de technologies hybrides ou hautement propriétaires, dont la nécessité de remplacement risque d'engendrer une surcharge financière ou une obligation de revoir complètement le système.

4.2 La perte de données

Si aucune mesure préventive n'a été implémentée pour réduire les impacts causés par la perte de données, des préjudices importants peuvent être causés. Notamment la perte de savoir-faire, la perte de données financières, la perte de clés logiques d'accès peuvent avoir des conséquences néfastes.

Cependant si la solution informatique a été conçue avec les précautions d'usage, la rupture de service d'un des éléments de la chaîne de stockage ne peut avoir qu'un impact réduit, voire aucun impact. En effet, le rôle de la solution de sauvegarde est justement de limiter les impacts en ce domaine.

[→ suite](#)

4.3 La perte d'accès et perte de productivité

La rupture d'accès à des ressources informatiques internes ou externes, qu'elle soit provoquée par des pannes réseau ou serveur, peut causer d'énormes préjudices.

En effet, dans des domaines tels que l'informatique des salles de marchés bancaires, ou de sites de commerce électronique, l'indisponibilité des ressources risque d'engendrer d'énormes pertes ou manques à gagner.

L'estimation du préjudice est donc directement dépendante de l'usage fait de la communication.

6 Les vulnérabilités exploitées

Dans ce domaine, on ne peut pas nécessairement parler d'exploitation de vulnérabilités, mais plutôt de survenance d'événements souvent inévitables, liés au caractère faillible des composantes d'un système informatique. Il n'y a donc que peu de moyens d'en limiter la survenance (entretien...). Toutefois, comme expliqué ci-dessous, il y a moyen d'en restreindre l'impact.

7 Les contre-mesures

Les principales mesures préventives visant à limiter l'impact des pannes physiques sont :

7.1 La mise en place d'une salle informatique organisée

Il est indispensable d'offrir des conditions de fonctionnement optimales à tous les éléments critiques du système informatique. Cela passe par la mise en place d'une salle informatique, ainsi que de salles « connectique » offrant des services tels que « no break » (pas d'interruption du courant), onduleurs, climatisation, détection d'incendie, et un contrôle des accès.

7.2 La conception d'une architecture redondante dite « à tolérance de panne »

Lors de la conception d'une architecture informatique, il y a moyen de se prémunir contre les pannes physiques ou assimilées, de manière à rendre « transparente » toute rupture de service de l'une ou l'autre des composantes.

Cette redondance peut être mise en place au niveau des couches suivantes :

5 Statistiques

Ce tableau exprime l'estimation, en unités de temps, des pourcentages de disponibilité.

Selon IDC (International Data Corporation), 60% des défaillances des disques durs sont attribuées à un arrêt incontrôlé ou trop rapide du système.

Disponibilité	« Downtime » par an
99.999%	30 secondes
99.99%	5.26 minutes
99.9%	52.56 minutes
99%	3.65 jours
98%	7.3 jours
97%	10.95 jours
95%	18.25 jours
90%	36.5 jours
71%	104 jours
24%	277 jours

Selon IDC (International Data Corporation), 60% des défaillances des disques durs sont attribuées à un arrêt incontrôlé ou trop rapide du système.

- Câblage.
- Réseau (HSRP - Hot Standby Router Protocol).
- Télécommunication.
- Serveur (Clustering).
- Stockage (RAID - Redundant Array of Inexpensive/Independent Disks).

7.3 Une politique d'archivage fonctionnel

Afin de limiter autant que possible le risque de perte de données, la mise en place et le respect de procédures d'archivage des données, tant au niveau des serveurs que des ordinateurs personnels, sont vivement conseillés.

7.4 Le choix de standards

Le choix de solutions propriétaires qui peut paraître alléchant au départ, peut devenir un vrai « cauchemar » en cas d'obligation de remplacement de l'un ou l'autre élément. Le risque peut aller jusqu'à la nécessité de revoir et remplacer complètement la chaîne de traitement en cas de rupture physique d'un élément.

CASES,

pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois



OFFICE LUXEMBOURGEOIS
D'ACCREDITATION ET DE
SURVEILLANCE



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie
et du Commerce extérieur