SÉCURISATION DES SYSTÈMES D'INFORMATION

TOME I:

SÉCURISATION DES MATÉRIELS.

VERSION	OBJET	DATE
1	Création	26/05/2024

INDEX

Table des matières

I.INTRODUCTION:

I.1.OBJET DE L'ÉTUDE:

Le présent ouvrage a pour objets:

- D'étudier la démarche de sécurisation des SYSTÈMES D'INFORMATION (S.D.I) vis à vis de TOUTES LES CAUSES qui sont susceptibles d'interrompre les services offerts aux usagers externes ou internes ou d'en dégrader la DISPONIBILITÉ, la QUALITÉ des services rendus ou la SÛRETÉ;
- De déduire de cette étude les différentes actions susceptibles de maintenir ou d'améliorer ces trois critères.

I.2.PUBLIC CONCERNÉ:

La démarche définie ci-dessus est beaucoup plus générale que la sécurisation contre les actions malveillantes. Nous verrons que si elle concerne en premier lieu tous les responsables de l'administration et de l'exploitation des S.D.I, elle concerne également la plupart des acteurs du développement des logiciels ainsi que les utilisateurs internes et externes des systèmes.

I.3.PRÉREQUIS:

La compréhension du présent ouvrage nécessite une bonne connaissance des concepts informatiques de base et de l'utilisation des outils informatiques usuels dans un environnement professionnel. Les différents rappels effectués dans les ANNEXES ont pour but de bien préciser certaines notions mentionnées dans l'ouvrage qui ne font pas forcément partie de ce socle de connaissances.

II.POSITION DU PROBLÈME ET PLAN DE L'ÉTUDE :

II.1.IMPORTANCE CROISSANTE DE L'UTILISATION DES OUTILS INFORMATIQUES:

De nos jours, nous utilisons les outils offerts par l'informatique dans l'exercice de la plupart de nos activités. Ceci est évidemment plus ou moins vrai suivant les régions du monde, mais même dans des endroits très reculés de notre planète, il est possible de rencontrer des personnes utilisant (par exemple) un téléphone mobile dit "intelligent" (smartphone) pour accomplir diverses tâches, allant de la simple communication à distance (mails, SMS, appels audios ou vidéos) à des tâches plus complexes comme la réservation de billets de transport.

Or, un ensemble composé de quelques personnes organisées pour effectuer certaines tâches et s'appuyant entièrement ou partiellement sur des moyens informatiques pour les réaliser peut être considéré comme constituant un SYSTÈME D'INFORMATION (S.D.I).

EXEMPLE: dans les pays dits "développés", la plupart des familles, pour réaliser un grand nombre de processus relatifs à la vie interne de ces foyers familiaux, s'aident d'un SYSTÈME INFORMATIQUE composé de plusieurs postes de travail ou terminaux audio-visuels reliés par un réseau interne construit autour d'un routeur permettant d'accéder à internet ((une "BOX"). Nous pouvons considérer cette organisation comme un SYSTÈME D'INFORMATIONS FAMILIAL, qui, comme tout S.D.I. qui se respecte, peut être décomposée en deux sous-systèmes:

- Un SOUS-SYSTÈME SOCIAL composé des différents membres de la famille, structuré par les relations familiales "traditionnelles", et dont les activités sont liées à la gestion du foyer familial: loisirs, communication, achats en ligne, démarches administratives, etc;
- Un SOUS-SYSTÈME INFORMATIQUE (S.I) constitué par les différents postes de travail et terminaux utilisés par la famille (PC, Tablettes, téléphones mobiles, décodeurs TV, etc), mais aussi par des équipements de stockage de données (disques externes), de bureautique (imprimantes, scanners, etc.), reliés entre eux et au réseau internet global par un ROUTEUR (la BOX).

Un tel SYSTÈME D'INFORMATION permet de gérer des activités qui dans un S.D.I professionnel seraient appelés des PROCESSUS D'AFFAIRE comme la gestion de l'inscription des enfants à l'université, l'organisation d'un voyage ou la souscription en ligne d'un crédit à la consommation. La complexité de ces procédure est donc souvent comparable à ce qui se fait dans un milieu professionnel.

II.2.IMPORTANCE DE LA SÉCURISATION DE CES OUTILS:

Cette importance croissante de l'utilisation des moyens informatiques à tous les niveaux de l'activité humaine (professionnel, familial, éducatif, ludique, etc.), et surtout, la généralisation de l'utilisation de ces outils dans des environnements où ceux-ci se retrouvent connectés entre eux au sein de systèmes Informatiques locaux et avec les différentes "communautés en ligne" par l'intermédiaire d'internet accroît simultanément la gravité des risques liés aux dysfonctionnements de ces systèmes. Par exemple:

- La perte de données suite à une panne matérielle ou une erreur d'utilisation peut avoir des conséquences dramatiques sur les plans financiers et sociaux pour une entreprise mais aussi pour une famille ou un particulier;
- Le cryptage de ces données par un hacker avec demande de rançon peut entraîne également des conséquences très importantes pour les mêmes victimes.

Ceci est d'autant plus grave que les différents outils utilisés sont de plus en plus interconnectés, "synchronisés", etc, ce qui favorise la propagation de ces dysfonctionnements ou actions malveillantes.

II.3.LA NOTION DE SÉCURITÉ POUR LES DIFFÉRENTS USAGERS D'UN S.D.I:

Chacun des usagers d'un S.D.I, qu'il appartienne au sous-système social ou qu'il en soit uniquement un clients externe, perçoit le NIVEAU DE SÉCURITÉ de celui-ci en fonction de plusieurs critères qualifiant la qualité du service rendu:

- La DISPONIBILITÉ des services offerts. Celle-ci renvoie à la notion de TAUX DE DISPONIBILITÉ (durée de disponibilité sur un intervalle de temps donnée).
- La QUALITÉ des services rendus. Ce critère peut être défini comme l'écart entre le service rendu par le S.D.I et le service attendu par l'utilisateur;
- La SÛRETÉ des opérations effectuées à l'aide du S.D.I (en particulier, la garantie de l'INTÉGRITÉ et de la CONFIDENTIALITÉ des données échangées ou stockées).

L'appréciation de la sécurité d'un S.D.I par un usager ne dépend donc pas uniquement de la protection contre les actions malveillantes: que la perte de données qu'il subit provienne d'une défaillance matérielle, d'une attaque informatique ou d'une erreur de manipulation, le résultat est le même pour lui.

De ce fait, il nous a semblé intéressant d'aborder la sécurisation des S.D.I dans un ouvrage qui traite de toutes les causes de dégradation de celle-ci et non uniquement de la protection contre le piratage informatique.

II.4.PERSONNEL CONCERNÉS PAR LA SÉCURITÉ DES S.I:

La plupart des personnes qui, comme l'auteur de ces lignes, ont été amenées à exercer dans les domaines de la création, de l'administration ou de l'utilisation d'outils informatiques (matériels et logiciel) et à leur intégration dans l'activité d'une entreprise ont probablement pu constater que la prise en compte des exigences en matière de SÉCURITÉ sont difficiles à faire accepter par les différentes catégories de personnels concernées (maîtres d'ouvrages, développeurs, testeur, utilisateurs, administrateurs, etc.).

En effet, assurer la sécurité est souvent perçue par eux comme une activité chronophage, onéreuse et génératrice de contraintes. De plus, comme les bénéfices engendrés pas les actions de sécurité sont difficilement quantifiables dans l'immédiat, il est souvent malaisé de faire ressortir la plus-value qu'elles apportent.

Pourtant, tous les intervenants sur un système d'information sont concernés par la sécurité à un moment où à un autre de leur activité. Par exemple:

- Un développeur qui ne sécurise pas suffisamment un menu de paramétrage favorise un piratage par injection de contenu;
- Un testeur de logiciels qui ne vérifie pas suffisamment les effets des paramétrages aberrants peut rendre possibles des comportements erratiques du logiciel testés allant du dysfonctionnement temporaire ou définitif à l'ouverture de failles de sécurité;
- Un administrateur (ou même un simple utilisateur) qui ne se déconnecte pas après sa session d'utilisation peut compromettre plus ou moins gravement la sécurité des accès;
- Et d'une manière générale, nous pouvons affirmer que tout employé d'une entreprise est susceptible de révéler, par l'emploi de la force, de la ruse, de la persuasion , ou simplement par négligence, des informations permettant d'ouvrir des failles dans la sécurité d'un S.D.I ou même du S.I correspondant.

II.5.CAUSES DE LA DÉGRADATION DE LA SÉCURITÉ D'UN S.D.I:

En première analyse, nous pouvons considérer qu'un Système d'Information repose sur l'interaction de 3 sortes d'entités: les composants MATÉRIELS, les composants LOGICIELS et les UTILISATEURS. Un UTILISATEUR peut être interne au système (employé de l'organisation à laquelle le S.D.I appartient) ou externe à celui-ci (client utilisateur des services externes, mais aussi, personne malveillante cherchant à porter atteinte au fonctionnement où à l'intégrité du système).

Nous traiterons les composants matériels séparément des composants logiciels car il existe d'importantes différences dans leurs mécanismes de défaillance.

Parmi les dysfonctionnements matériels, nous distinguerons ceux qui aboutissent à une indisponibilité PERMANENTE d'un service que l'on ne peut corriger que par une intervention de maintenance matérielle corrective, de ceux qui n'aboutissent qu'à une dégradation TEMPORAIRE du service qui disparaît sans intervention de maintenance, sinon un redémarrage du système matériel (reboot, réinitialisation).

De ce fait, nous classerons les dysfonctionnements en cinq catégories:

- Les DYSFONCTIONNEMENTS PERMANENTS de composants MATÉRIELS;
- Les DYSFONCTIONNEMENTS TEMPORAIRES de composants MATÉRIELS;
- Les DYSFONCTIONNEMENTS de composants LOGICIELS;
- Les ERREURS et NÉGLIGENCES des usagers (actions INVOLONTAIRES);
- Les ACTIONS MALVEILLANTES (actions VOLONTAIRES).

Le TOME I de l'ouvrage comprend l'introduction générale, l'étude des deux premières catégories de dysfonctionnements et une annexe technique.

Le TOME II de l'ouvrage comprend l'étude des trois autres catégories de dysfonctionnements et une annexe technique.

III.SÉCURISATION CONTRE LES DYSFONCTIONNEMENTS MATÉRIELS PERMANENTS:

III.1.DÉFINITION D'UN DYSFONCTIONNEMENT PERMANENT:

Nous qualifierons de DYSFONCTIONNEMENT PERMANENT d'un équipement un dysfonctionnement qui ne peut disparaître sans qu'une action de maintenance corrective (autre que le réamorçage de l'équipement) soit effectuée.

EXEMPLE: *Le DYSFONCTIONNEMENT PERMANENT d'un réseau local peut être provoqué par une panne du routeur local. Les actions de correction qui en découleront seront probablement:*

- *La substitution d'un SPARE (composant de rechange configuré et paramétré) au routeur en panne;*
- *L'envoi en réparation du routeur en panne;*
- *Éventuellement, une étude complémentaire sur les besoins en fiabilité du réseau.*

III.2.CAUSES DIRECTES: AGRESSIONS DE L'ENVIRONNEMENT:

Le fonctionnement des composants électroniques est sensible aux agressions en provenance de leur environnement d'utilisation. Nous pouvons citer ici:

1. Une ALIMENTATION ÉLECTRIQUE défaillante (micro-coupures, variation de la fréquence, ou de la tension, défauts de mise à la terre, etc.);
2. Une AMBIANCE RADIOÉLECTRIQUE perturbée (exposition à des perturbations électromagnétiques ou électrostatiques);
3. Une TEMPÉRATURE DE FONCTIONNEMENT ANORMALE par rapport aux spécifications d'utilisation (température excessive ou trop basse);
4. Une HUMIDITÉ EXCESSIVE (génératrice d'oxydation et de courts-circuits) ou TROP FAIBLE (favorisant les décharges électrostatiques);
5. La PRÉSENCE DE POUSSIÈRES (s'opposant à une bonne ventilation, affaiblissant la qualité des contacts et pouvant créer des problèmes électrostatique);
6. Les AGRESSIONS MÉCANIQUES (chocs, vibrations);
7. etc.

REMARQUE: *à l'item n°1, l'alimentation électrique évoquée est celle qui est fournie au système informatique par un réseau électrique externe au système. En général, il s'agit du réseau électrique public de la zone géographique concernée (en France, c'est le réseau d'Enedis). Il peut s'agir également d'un système de fourniture privé (groupes électrogènes ou autres), intervenant comme fournisseur principal ou en secours du réseau public. Il ne s'agit donc pas des boîtiers d'alimentation internes aux différents composants du S.I qui fournissent les différentes tensions internes de ceux-ci à partir du réseau externe.*

III.3.CAUSES INDIRECTES: VIEILLISSEMENT DES COMPOSANTS:

Le Système Informatique d'une entreprise ou d'une administration importantes fonctionne la plupart du temps dans un environnement sécurisé (atmosphère climatisée, hors poussière, alimentation électrique sécurisée, accès limités, etc.). En revanche, lorsqu'il s'agit de petites entreprises ou de particuliers, les composants du S.I fonctionnent très souvent dans des locaux dont les accès et l'ambiance sont très peu contrôlés. Certes, en fonction de leur nature, les boîtiers des composants de premier niveau sont

dotés de dispositifs de protection (ventilation des boîtiers régulant plus ou moins la température interne et minimisant le dépôt des poussières, alimentations sécurisées, prises de terre conformes, etc.), mais globalement, il est rare que les exigences des constructeurs soient entièrement respectées.

De plus, il est bien évident qu'aucune mesure de protection ne peut garantir totalement les matériels d'un S.I. contre les agressions citées ci-dessus quand elles revêtent une intensité exceptionnelle (en cas d'événements catastrophiques, par exemple). De ce fait, même dans une enceinte sécurisée, il existe une probabilité non nulle, pour que certains équipements d'un S.I. subissent tout de même des agressions pouvant entraîner leur dysfonctionnement, soit immédiatement, en provoquant une détérioration fatale de leur structure interne, soit à terme en accélérant leur VIEILLISSEMENT PRÉMATURÉ.

Cette notion de VIEILLISSEMENT est plutôt intuitive. Elle peut être rattachée à la notion de FIABILITÉ dont nous donnons une explication rigoureuse dans les annexes.du présent document: le VIEILLISSEMENT d'un matériel peut être rapproché de la DIMINUTION de la FIABILITÉ de ce matériel, c'est à dire de la probabilité de celui-ci d'être encore en fonction après un temps d'utilisation donné:

L'annexe du présent ouvrage consacrée à la fiabilité expose les faits suivants:

- Même si le TAUX DE PANNES d'un composant électronique digital peut être considéré comme constant, sa FIABILITÉ décline dans le temps après sa première mise en fonction ou après un redémarrage suivant sa remise en état après panne;
- Dans le cas d'un composant comprenant une partie mécanique ou analogique (un disque dur classique, par exemple), le taux de panne a tendance à augmenter légèrement avec le temps et l'usure des différents constituants. L'évolution de sa fiabilité est donc une fonction plus complexe que dans le cas d'un composant digital, mais également décroissante. En première approximation, on peut considérer que le modèle à taux de panne constant peut être appliqué à l'électronique non digitale comme à l'électronique digitale;
- Comme le montre l'annexe consacrée à la fiabilité, un composant en partie mécanique ou en partie analogique ne peut être totalement remis en état, ce qui fait que le M.T.B.F (temps moyen entre deux pannes) a tendance à se raccourcir après chaque réparation.

Quelle que soit la nature du composant, la décroissance de la fiabilité est accentuée par un environnement agressif. L'agressivité de l'environnement d'utilisation est donc un facteur d'accélération du vieillissement, qui lui-même augmente la probabilité d'un dysfonctionnement permanent.

III.4.MÉCANISMES DES DYSFONCTIONNEMENTS MATÉRIELS PERMANENTS:

III.4.1.INTRODUCTION:

Nous allons maintenant étudier, pour chaque type d'agression, les mécanismes qui interviennent pour provoquer soit un dysfonctionnement permanent immédiat, soit un vieillissement prématuré des composants affectés par ces agressions.

III.4.2.DÉFAUTS DE L'ALIMENTATION ÉLECTRIQUE:

III.4.2.1.Généralités:

Les composants internes des différents équipements d'un S.I. ne sont, en général, pas exposés directement au courant du "secteur". En effet, les courants électriques qu'ils utilisent en interne sont la plupart du temps des courants continus de tensions relativement faibles par rapport à celle du courant alternatif fourni par le "secteur" (+12 v, -12 v, +5 v, -5 v, etc). Les boîtiers d'alimentation des différents équipements les élaborent à partir du courant alternatif du secteur, via des "transformateurs de tension" et des "redresseurs de phase". Cependant, certaines perturbations de l'alimentation externe peuvent, à partir d'un certain niveau de puissance, se répercuter sur les tensions fournies par les boîtiers d'alimentation internes. Certaines d'entre elles sont donc susceptibles d'endommager les différents circuits électroniques de l'équipement.

Ces perturbations peuvent être de plusieurs ordres:

- La DÉFAILLANCE COMPLÈTE de l'alimentation électrique. Nous distingueront deux cas:
  - L'interruption brutale et franche de l'alimentation électrique;
  - L'interruption de l'alimentation électrique à l'issue d'une phase de variation "chaotique".
- Des MICRO-COUPURES de secteur;
- Des perturbations de la FRÉQUENCE ou de la TENSION électrique;

III.4.2.2.Effets d'une défaillance brutale et franche de l'alimentation électrique:

Une variation rapide de l'alimentation électrique d'un équipement a pour effet d'induire dans les parties conductrices de cet équipement des courants appelés "extra-courants de rupture". Comme tous les courants induits, ceux-ci sont d'autant plus importants que cette variation est rapide et de grande amplitude.

De ce fait, la défaillance brutale de l'alimentation externe d'un équipement provoque des extra-courants de rupture importants qui peuvent détériorer ses composant électriques et électroniques (par effet de "claquage", par exemple).

REMARQUE: *à l'intérieur d'un composant, la brusque apparition d'une surtension importante peut entraîner l'amorçage d'un arc électrique à travers la paroi isolante d'un condensateur ou la "jonction" d'un composant semi-conducteur (diode, transistor, etc.). C'est ce type de détérioration que l'on appelle souvent "claquage".*

Lorsqu'une telle défaillance brutale interrompt une séquence de calcul dans un processeur, elle peut provoquer une perte des données en cours d'élaboration. Cependant, les équipements incluent des mécanismes qui permettent de détecter ces phénomènes brusques et d'en minimiser les effets sur les composants. Par exemple:

- *En cours de fonctionnement, les têtes de lecture d'un disque dur mécanique sont maintenues à très faible distance des surfaces magnétiques par le déplacement d'air causé par la rotation.*

Un arrêt ou un ralentissement de cette rotation peut amener ces têtes à entrer en contact avec les surfaces et à arracher des copeaux de métal. De ce fait, les têtes de lecture des disques durs mécaniques sont équipées de mécanisme qui produisent leur relevage automatique en cas de détection d'une anomalie d'alimentation;

- *Les systèmes d'exploitation des ordinateurs utilisent les alarmes d'alimentation qu'elles détectent et la réserve d'énergie contenue dans les capacités des boîtiers d'alimentation pour dérouler des actions automatiques de sauvegarde qui permettent le plus souvent de récupérer l'état des traitements en cours.*

III.4.2.3.Effets d'une défaillance chaotique de l'alimentation électrique:

Cependant, certaines défaillances de l'alimentation électrique peuvent se produire d'une manière beaucoup moins nette, avec une chute chaotique de la tension pouvant présenter des "rebonds" d'amplitude. Même s'il provoque rarement une panne immédiate, ce type de défaillance est extrêmement préjudiciable car il provoque un vieillissement rapide des composants tout en étant beaucoup plus difficile à détecter qu'une défaillance "franche".

EXEMPLES:

- *Si ce type de défaillance chaotique se produit fréquemment, les composants de l'équipement, soumis à des chocs électriques répétés, vont connaître un vieillissement accéléré, raccourcissant leurs durées de vie;*
- *Nous avons vu au paragraphe précédent les effets d'une coupure franche inopinée de l'alimentation électrique. Une défaillance "chaotique" peut produire de la même manière une succession de petites détériorations qui peuvent souvent passer inaperçues jusqu'au moment où il ne sera plus possible de fonctionner.*

III.4.2.4.Effets des micro-coupures de secteur:

On appelle "micro coupures" des interruptions de l'alimentation électrique dont la durée est suffisamment faible pour qu'elles ne perturbent pas le fonctionnement apparent des équipements. Les principales causes de ces dysfonctionnements sont:

- Les vents violents, qui provoquent des contacts entre les lignes à haute tension ou avec d'autres objets, comme des branches d'arbre, par exemple;
- La commutation entre les différents sources alimentant le réseau général (centrales électriques de différents types), pilotée par le gestionnaire de réseau.

Nous avons vu plus haut que les alimentations internes des équipements sont capables, en cas de défaut d'alimentation du secteur, de maintenir pendant quelques millisecondes (moins de 60 ms en général), la fourniture des tensions aux composants internes. De ce fait, des interruptions de durée inférieure ne provoquent en apparence aucun dysfonctionnement. Cependant, ces perturbations peuvent provoquer sur les équipements sensibles aux irrégularités de l'alimentation des dégâts analogues à de petites défaillances chaotiques:

- Dans tous les cas, on observe un vieillissement prématuré des composants;
- Dans le cas d'un équipement muni de processeurs et d'un système d'exploitation (ordinateurs, terminaux "intelligents", etc.), une micro coupure suffisamment longue peut enclencher le réamorçage automatique du système, provoquant ainsi une interruption temporaire du service: une telle interruption se produisant dans le cadre d'un processus industriel peut avoir sur des équipements supportant des fonctionnalités CRITIQUES des conséquences aussi graves

qu'une défaillance totale de l'alimentation électrique (la notion de "criticité" est exposée en annexe).

III.4.2.5.Effets des perturbations de la fréquence ou de la tension:

Des variations importantes de la fréquence ou de la tension du réseau d'alimentation électrique peuvent également contribuer à la détérioration des composants électroniques d'un S.I:

- Une tension de secteur trop élevée entraînera automatiquement une intensité trop élevée dans les conducteurs. Celle-ci produira une chaleur excessive, susceptible de détériorer les circuits électriques ou électroniques qui la subissent si la ventilation ne permet pas de la dissiper rapidement;
- Les tensions de secteur trop faibles ou trop élevées auront des répercussions à la baisse ou à la hausse sur les tensions continues produites par les boîtiers d'alimentation internes. Si ces valeurs ne se situent plus dans les créneaux de tolérance des composants utilisateurs, ceux-ci ne fonctionneront plus correctement;
- Les variations de fréquence du courant alternatif fourni se répercutent sur les courants continus produits par les boîtiers d'alimentation interne. Par exemple, une baisse de fréquence provoque une baisse des tensions "redressées".

REMARQUE: en France, la tension alternative et la fréquence du courant de secteur fourni par ENEDIS sont données comme étant comprise entre 220 et 230 volts et entre 49,9 Hz et 50,1 Hz.

III.4.3.AMBIANCES RADIOÉLECTRIQUES PERTURBÉE:

III.4.3.1.Introduction:

Pour étudier les perturbations de nature radioélectrique susceptibles d'avoir un impact sur le fonctionnement d'un Système Informatique, nous allons les classer, en fonction de leur origine, en trois catégories:

- Les perturbations d'origine interne au système;
- Les perturbations induites par les équipements externes au S.I. situés dans son environnement immédiat;
- Les perturbations liées aux phénomènes radioélectriques globaux, et en particulier à la foudre.

III.4.3.2.Causes et effets des perturbations électromagnétiques d'origine interne:

III.4.3.2.1.Causes:

Ces perturbations ont pour origine les rayonnements électromagnétiques émis par les équipements internes au S.I. En effet, les différents circuits et câbles de transmission de données qui composent ces équipements sont parcourus par divers signaux électriques codés en digital dont les états binaires peuvent varier très rapidement (temps de commutation d'état de l'ordre de quelques nanosecondes).

Selon les lois de l'induction magnétique, la circulation de ces signaux variables crée dans l'environnement des champs magnétiques susceptibles d'induire des courants perturbateurs dans les circuits et équipements voisins.

Les courants alternatifs des alimentations peuvent également induire des courants parasites (à basse fréquence, cette fois).

III.4.3.2.2.Effets:

En se superposant algébriquement aux signaux électriques digitaux circulant dans les circuits, ces différents courants induits parasites peuvent les altérer suffisamment (les brouiller) pour que le fonctionnement des équipements se retrouve dégradé ou même impossible.

En théorie, les équipements composant un S.I. doivent satisfaire aux critères de COMPATIBILITÉ ÉLECTRO MAGNÉTIQUE (C.E.M) que l'on peut résumer comme suit:

- L'appareil doit réduire ses ÉMISSIONS électromagnétiques à un niveau acceptable pour l'environnement au sein duquel il est intégré;
- L'appareil doit être suffisamment protégé contre les perturbations électromagnétiques pour pouvoir fonctionner normalement dans son environnement d'intégration. Pour un type et une intensité de perturbation donnés, un appareil dont le fonctionnement n'est pas affecté est dit IMMUNISÉ. Dans le cas contraire, le comportement de l'équipement face à ces perturbation (ses dysfonctionnements éventuels) définit son niveau de SUSCEPTIBILITÉ électromagnétique.

De ce fait, pour un S.I. dont les différents équipements satisfont aux critères de compatibilité électromagnétique exigés par le milieu, il ne peut se produire de dysfonctionnement dû à des perturbations magnétiques d'origine interne, à moins qu'un composant ne présente un défaut qui dégrade sa compatibilité (le plus fréquemment, il s'agit d'un défaut de mise à la masse ou à la terre).

NOTA: Mesures favorisant la compatibilité électromagnétique:

La suppression (ou l'atténuation) du rayonnement issu des circuit internes peut être obtenue par diverses dispositions, dont, en particulier:

- **Le BLINDAGE des parties émettrices** (enveloppement des éléments émetteurs par des gaines ou des enceintes conductrices). Ces dispositifs constituent des barrières à la propagation des ondes électromagnétiques. Assortis de la mise à la terre et de l'utilisation de filtres en fréquence, ils permettent de dériver les courants induits parasites vers la TERRE;
- **Le fait de TORSADER des "paires" de conducteurs transmettant les données (paires torsadées):** Le fait de torsader les deux conducteurs d'une paire fait que les champs magnétiques émis par les deux conducteurs se retrouvent en opposition en tout point de l'environnement. Comme ils transportent les mêmes signaux au même moment, les deux champs magnétiques qu'ils créent dans l''espace ont en tout point la même intensité mais des directions opposée. De ce fait, leur somme vectorielle a tendance à s'annuler. Très souvent, les paires torsadées sont également blindées.

Ces mêmes dispositions permettent de diminuer la SUSCEPTIBILITÉ de ces circuits.

REMARQUE: *la directive CEM de l'Union Européenne définit les différents niveaux acceptables. Pour un équipement donné, l'obtention du marquage CE implique que la SUSCEPTIBILITÉ de cet équipement face à ses contraintes d'utilisation ait été évaluée et publiée par le constructeur.*

III.4.3.3.Causes et effets des perturbations électromagnétiques induites par l'environnement immédiat:

III.4.3.3.1.Causes:

L'environnement immédiat des Systèmes Informatiques héberge le plus souvent un certain nombre d'équipements susceptibles de créer des perturbations électromagnétiques fortes:

1. Il s'agit essentiellement des équipements qui participent au soutien du S.I: Groupes électrogènes (alimentation électrique principale ou moyens de secours), équipements de contrôle des accès (caméras, lecteurs de cartes d'accès, portails électriques télécommandé), équipements de climatisation, équipements d'éclairage extérieur, et d'une façon générale, tous les équipements dont le fonctionnement implique l'utilisation de "charges selfiques" importantes (comme les moteurs électriques, les serrures ou vannes électromagnétiques, etc.);
2. D'autre part, des équipements n'ayant aucun rapport avec le S.I mais qui se situent dans son environnement immédiat peuvent également constituer de puissantes sources de perturbations électromagnétiques. C'est le cas, en particulier, des différents systèmes RADARS (radars de circulation urbaine, radars d'aéroports, etc.), des "spots wifi" et même des feux de circulation dont la commutation peut induite des perturbations sur les équipements environnants.

III.4.3.3.2.Effets:

La plupart des S.I. dont la continuité du fonctionnement revêt un caractère critique, comme les "data centers" ou les systèmes de conduite de processus industriels (contrôle de centrales nucléaires, contrôle aéroportuaire, systèmes militaires, etc.), sont confinés dans des enceintes conçues pour les protéger contre les perturbations électromagnétiques se propageant dans l'espace environnant. Cependant, beaucoup de S.I dont la continuité du fonctionnement semble moins essentielle, ne sont pas (ou sont peu) protégés des perturbations extérieures. Il s'agit souvent des S.I. d'entreprises à vocation administrative ou commerciale qui, de ce fait, sont exposés à des ambiances plus ou moins perturbées.

En l'absence de mesures de protection, les effets des perturbations provoquées par ces équipements externes au S.I. sont sensiblement les mêmes que ceux qui ont été mentionnés pour les équipements internes.

A priori, nous pourrions penser que les S.I. qui bénéficient de la protection d'enceintes adéquates sont immunisés contre les perturbations externes. Malheureusement, les équipements de la première catégorie citée plus haut ont la particularité de présenter des connections avec le S.I, soit par leur alimentation électrique, qui peut être commune, soit par l'intermédiaire des liaisons de données qui leur permettent d'échanger avec ce S.I. des états ou des commandes. Ces connections posent nécessairement le problème des différences de potentiel qui peuvent exister entre la masse des équipements du S.I. et celle des équipements externes. D'autre part, elles peuvent constituer des points d'entrée pour les perturbations électriques ou magnétiques d'origine externes (comme celles qui sont produites par la foudre).

III.4.3.4.Causes et effets des perturbations liés aux phénomènes radioélectriques globaux:

III.4.3.4.1.Causes:

Les plus connues de ces perturbations sont:

Les DÉCHARGES ÉLECTROSTATIQUES ET LES RAYONNEMENTS causés par la foudre:

Le phénomène de la FOUDRE se traduit par des décharges électrostatiques entre deux nuages ou entre un nuage et le sol. Ces décharges, qui sont causées par les différences de potentiels électriques énormes qui peuvent exister entre deux nuages d'orages ou entre les nuages d'orage et la TERRE, se traduisent par de gigantesques ARCS ÉLECTRIQUES (les éclairs) dont la TENSION peut atteindre des millions de volts et l'INTENSITÉ des dizaines de milliers d'ampères.

Lorsque la foudre touche des objets situés au sol, l'électricité transportée par l'éclair s'évacue dans la masse de la terre par des courants électriques dont l'intensité est beaucoup plus faible que celle de l'éclair mais dont la tension reste très élevée. De ce fait, la PUISSANCE dégagée par ces courants peut tout de même être considérable.

D'autre part, les éclairs peuvent engendrer des RAYONNEMENTS ÉLECTROMAGNÉTIQUES à très haute énergie, comme les rayons X ou les rayons GAMMA.

Les RAYONNEMENTS ÉLECTROMAGNÉTIQUES de forte puissance:

Ceux-ci peuvent être produits par diverses sources, comme les éruptions solaires, les explosions d'armes nucléaires ou thermonucléaires ou d'armes non nucléaires à effets électromagnétiques, etc.

III.4.3.4.2.Effets:

Du fait des puissances électriques transportées, les courants induits par la foudre dans les équipements qu'ils sont amenés à traverser pour rejoindre la terre peuvent provoquer des échauffements très importants dans les conducteurs et les circuits et même leur fonte totale ou partielle.

D'autre part, les arcs électriques produits à ces occasions à travers les jonctions des composants électroniques (diodes, transistors, condensateurs, etc.) peuvent également détériorer celles-ci.

Les perturbations dues à la foudre peuvent affecter même les systèmes situés dans des enceintes protégées, par l'intermédiaire des différentes voies de conduction qui existent nécessairement entre l'extérieur et l'intérieur (masses métalliques communes, alimentation électrique, liaisons de données, etc.).

Les rayonnements à haute énergie produits par les éruptions solaires, les arcs de foudre ou les armes à effet électromagnétique ont, comme toutes les perturbations électromagnétiques, des effets thermiques sur les circuits électroniques.

D'autre part, ils ont sur les matériaux un effet IONISANT (modification de la structure électronique des atomes), susceptible d'en altérer les propriétés physico-chimiques. Ils peuvent donc altérer le fonctionnement des composants électroniques, entraînant des dysfonctionnements irréversibles.

Ainsi, les éruptions solaires produisent des "orages magnétiques" capable de perturber fortement ou même d'endommager les équipements électroniques des véhicules circulant dans les hautes altitudes (avions, missiles, satellites artificiels, etc) ou de perturber les transmissions hertziennes. En revanche, du fait de l'effet protecteur des basses couches atmosphériques, leurs effets sur les équipements situés près du sol est en général peu considérable.

Il n'en va pas de même pour les armes à effet électromagnétique, qui peuvent déclencher leurs émissions dans l'atmosphère relativement près de leurs cibles: leur pouvoir destructeur peut s'exercer même sur les équipements au niveau du sol.

*III.4.4.*DÉFAUTS LIES À LA MISE À LA MASSE DES CIRCUITS*:*

REMARQUE PRÉLIMINAIRE: *l'annexe du présent document consacrée aux notions de masse et de terre rappelle succinctement les notions abordées dans ce paragraphe.Le lecteur est prié de s'y référer en cas de difficulté.*

III.4.4.1.Utilité de la connexion à la masse:

Dans les équipements d'un SYSTÈME INFORMATIQUE qui **fonctionnent selon les principes de l'électronique digitale**, la MASSE (le châssis) est reliée à une des bornes des alimentations en courant continu fournies par le BOÎTIER D'ALIMENTATION INTERNE (en général, c'est le pôle de potentiel le moins élevé). Le "retour" du courant continu alimentant les différents circuits internes à l'équipement s'effectue à travers la masse. Ce dispositif permet de fixer pour ces circuits un même POTENTIEL ÉLECTRIQUE. Ceci, outre l'avantage de simplifier les câblages, permet d'éviter que des courants parasites circulent entre les différents circuits et perturbent leur fonctionnement.

III.4.4.2.Effets d'une mise à la masse défaillante dés circuits:

De ce fait:

- Une absence complète de connexion avec la masse d'un des circuits de l'équipement entraîne le dysfonctionnement complet du circuit concerné (qui n'est plus alimenté) et induit un dysfonctionnement au moins partiel de l'équipement;
- Une mauvaise connexion d'un circuit avec la masse amène une dégradation de la qualité des signaux délivrés par celui-ci (souvent par effet capacitif), entraînant forcément une dégradation du fonctionnement de l'équipement.

La dégradation ou l'interruption totale de la connexion d'un circuit avec la masse peut provenir de nombreuses causes:

- Choc mécanique entraînant la rupture d'une soudure ou le dessertissage d'un élément;
- Vieillissement d'une soudure;
- Etc.

REMARQUE: dans les équipements (ou parties d'équipements) qui fonctionnent en courant alternatif, les circuits sont isolés de la masse.

III.4.4.3.Défauts d'interconnexion des masses d'une installation:

Dans les installations complexes, comme les DATA CENTERS, où les différents équipements sont montés dans des "RACKS" (rayonnages, étagères) métalliques, les MASSES de ces équipement sont souvent interconnectées (en général avec de la TRESSE DE MASSE), de façon à assurer leur ÉQUIPOTENTIALITÉ. Ceci permet d'éviter que des courants parasites s'établissent entre les différents équipements, à travers les liaisons filaires qui les relient. Ces courants parasites peuvent perturber leur fonctionnement, mais aussi provoquer des chocs électriques pour les personnes entrant en contact simultanément avec deux équipements voisins.

L'absence de connexion (ou une connexion déficiente) de la masse d'un équipement avec les autres masses de l'installation peut donc entraîner deux types de dysfonctionnements:

- Des chocs électriques pour les usagers du système qui entrent simultanément en contact avec l'équipement concerné et un autre équipement du site. Ces chocs peuvent être assez puissants pour provoquer une électrocution;
- La perturbation du fonctionnement de l'équipement concerné, perturbation qui peut s'étendre aux équipement du site qui lui sont connectés.

III.4.4.4.Défauts de mise a la masse des blindages:

Enfin, lorsque des circuits ou des conducteurs sont équipés de BLINDAGES, ceux-ci doivent être reliés à la MASSE. En effet, les blindages ont pour fonction de "piéger" les courants induits parasites issus du

circuit lui-même ou de l'environnement du circuit. La mise à la masse d'un blindage permet d'évacuer ces courants parasites vers la masse, puis vers la terre comme nous le verrons plus loin.

En l'absence de mise à la masse, un blindage n'a pratiquement aucune utilité.

III.4.5.DÉFAUTS DE MISE À LA TERRE:

REMARQUE: *l'annexe du présent document consacrée aux notions de masse et de terre rappelle succinctement les notions abordées dans ce paragraphe.Le lecteur est prié de s'y référer en cas de difficulté.*

III.4.5.1.Utilité de la mise à la terre des installations:

Les équipements électriques qui ont besoin d'être reliés au secteur par une prise 3 points en courant alternatif monophasé utilisent la fiche TERRE pour se relier à la PRISE DE TERRE de l'installation. Cette liaison est utilisée par les alimentations internes pour fournir le potentiel 0 v aux équipements (sortie GRD pour ground).

La MISE A LA TERRE des MASSES MÉTALLIQUES des équipements présente les avantages suivants:

- Éviter les courts circuits entre la MASSE et la TERRE par l'intermédiaire du sol de l'installation, ou du moins en atténuer les effets;
- Atténuer les perturbations électriques induites dans les circuits par l'environnement électromagnétique en les redirigeant vers la TERRE (à l'aide d'un filtre séparateur).
- Permettre aux courants parasites circulant dans les MASSES (ceux qui sont induits dans les circuits ou piégés par les BLINDAGES entourant les circuits ou conducteur) de s'écouler vers la TERRE;

III.4.5.2.Dysfonctionnements liés à une mise à la terre défaillante:

L'absence de MISE A LA TERRE des MASSES de l'installation peut donc entraîner plusieurs sortes de dysfonctionnement:

- Si l'installation est protégée par un DISJONCTEUR DIFFÉRENTIEL, un court-circuit entre la masse et la terre peut provoquer la disjonction de son alimentation électrique. Cette disjonction peut constituer une panne majeure dans certaines circonstances, car elle entraîne une indisponibilité complète. Cependant, elle a l'avantage de protéger les circuits contre la surintensité que le court-circuit peut engendrer: le fonctionnement peut être rétabli dès que le court-circuit est éliminé;
- Si l'installation n'est pas protégée par un DISJONCTEUR DIFFÉRENTIEL, un court-circuit entre la masse et la terre peut provoquer des surtensions importantes dans les circuits, entraînant un échauffement susceptible d'entraîner leur destruction: les conséquences sont alors beaucoup plus préjudiciables pour la disponibilité de l'installation car il va falloir également remplacer les éléments détériorés avant de rétablir le fonctionnement;
- Un utilisateur non isolé du sol qui touche une masse de l'installation risque l'électrocution, avec des conséquences potentiellement mortelles;
- Du fait de l'absence de mise à la terre des masses:
    - Les champs magnétiques rayonnés par le circuit et piégés par les blindages ne sont pas amenés à la terre mais rediffusés dans l'environnement;

- Les perturbations magnétiques issues de l'environnement et piégées dans les blindages ne sont pas évacuées vers la terre, mais se retrouvent superposées aux signaux internes des circuits.

III.4.6.ANOMALIES DE LA TEMPÉRATURE DE FONCTIONNEMENT:

III.4.6.1.Effets de la température sur les matériaux conducteurs:

Dans la plupart des cas, la RÉSISTANCE d'un matériau conducteur ou semi-conducteur varie en fonction de sa TEMPÉRATURE. L'intensité et le sens de ces variations dépendent fortement de la nature de ces matériaux. Par exemple:

- Pour la plupart des métaux (fer, cuivre, aluminium, etc.), la résistance augmente quand la température de fonctionnement augmente;
- En revanche, pour la plupart des semi-conducteurs (carbone, silicium, germanium, etc.), la résistance DIMINUE quand la température de fonctionnement augmente.

Ces variations de résistance peuvent être très importante pour certains matériaux. Ceci explique que les caractéristiques d'un circuit électronique complexe, composé à la fois de conducteurs métalliques et de semi-conducteurs, dépendent assez fortement de sa température de fonctionnement. En général, le fonctionnement d'un composant électronique n'est garanti nominal par le constructeur que dans des conditions de température bien précises.

EXEMPLE: *le fonctionnement d'un processeur INTEL CORE courant n'est garanti qu'entre 25 et 85 degrés Celsius.*

III.4.6.2.Effets des dysfonctionnements dus aux anomalies de la température de fonctionnement:

Nous avons vu plus haut que les plages de températures de fonctionnement des différents circuits électroniques peuvent varier en fonction de leur structure. En règle générale, les températures trop peu élevées (inférieures à une quinzaine de degrés C) perturbent le fonctionnement mais ne provoquent pas l'altération des circuits (à moins qu'elles soient accompagnées d'une humidité trop importante, génératrice d'oxydation ou de cours-circuits). En revanche, des températures trop élevées peuvent provoquer un vieillissement rapide des matériels et même leur destruction.

Parmi les composants informatiques que l'on peut trouver dans les équipements des Systèmes Informatiques, les PROCESSEURS sont ceux qui sont les plus sensibles aux températures anormales. En effet, il s'agit de composants très complexes, constitués de millions de circuits intégrés dans une même "puce électronique" de faible dimension, fonctionnant avec des fréquences de commutation de l'ordre de la nanoseconde et dissipant de ce fait une grande quantité d'énergie. Ceci explique pourquoi les "puces" des processeurs sont équipées de leur propre système de ventilation (plaque de refroidissement pour capter la chaleur produite et ventilateur pour dissiper celle-ci).

Les plages de fonctionnement des équipements sont donc largement déterminées par celles des processeurs qu'ils intègrent (processeurs principaux des ordinateurs, processeurs des cartes graphiques, etc.). De ce fait, nous pouvons, en première approximation, prendre ces dernières plage comme références pour le fonctionnement de tout l'équipement.

Les informations suivantes donnent des valeurs approximatives pour les températures des processeurs dans diverses situations

- ***PROCESSEUR INOCCUPÉ***: Un processeur intégré dans un équipement n'est jamais complètement au repos.En effet, lorsqu'il n'est pas affecté à l'exécution d'un code quelconque, il exécute une boucle d'attente, que l'on appelle quelquefois "Idle" (boucle "inactive"). Ce

faisant, il met tout de même en jeu une grande partie des mécanismes liés à l'exécution des programmes, ce qui provoque une certaine dissipation de chaleur. Dans cette situation, la température du processeur se situe en général autour de 35° C. Une température supérieure à 45° C doit être considérée comme anormale;

- ***PROCESSEUR EN COURS D'EXÉCUTION***: l'exécution de la plupart des applications informatiques élève la température des processeurs entre 45° C et 60° C. Dans le cas d'applications très exigeantes en puissance CPU, la température peut couramment atteindre les 80° C. Au delà, il ne peut s'agir que de périodes de très courte durée, et en tout état de cause, au-delà de 100° C, le risque de panne du processeur devient très important.

Le dépassement de ces valeurs de température doit, en fonction du contexte, amener à suspecter un défaut de ventilation du composant. Les conséquences à long terme sont un vieillissement accéléré, de celui-ci, voire même une détérioration irréversible si le défaut persiste trop longtemps.

Certains composants possèdent des mécanismes protecteurs capables de les mettre automatiquement hors circuits en cas de surchauffe. Cependant, une telle mise hors circuit, si elle a l'avantage d'éviter la détérioration du composant, a en fait les mêmes conséquences opérationnelles qu'une panne franche, puisqu'elle peut remettre en cause le fonctionnement du S.I. pour une période plus ou moins longue.

III.4.7.ANOMALIES DE L'HYGROMÉTRIE:

III.4.7.1.Causes des dysfonctionnements liés à une anomalie hygrométrique:

Les dysfonctionnements dus aux anomalies de l'hygrométrie à l'intérieur du châssis d'un équipement peuvent être de deux sortes:

- Une hygrométrie trop élevée par rapport à la température va causer la CONDENSATION de l'eau sous forme de gouttelettes susceptibles d'entraîner l'oxydation des composants, ou même des court-circuits;
- Une hygrométrie trop faible (air trop sec) peut, elle, favoriser les décharges électrostatiques entre composants ou entre les composants et la terre.

III.4.7.2.Effets des dysfonctionnements liés à une anomalie hygrométrique:

- L'oxydation peut entraîner la détérioration des CONTACTS entre composants, ce qui peut provoquer la dégradation des SIGNAUX échangés entre eux. A terme, une panne franche peut survenir si les signaux deviennent trop dégradés pour être exploités par les composants récepteurs;
- Si la condensation est suffisante pour provoquer un court-circuit, les conséquences peuvent être fatales pour l'équipement: le court-circuit peut provoquer des détérioration irréversibles à l'intérieur des composants, comme la fusion de ceux-ci;
- Les décharges électrostatiques provoquent des courants de faible intensité, mais de tension élevée qui peuvent détériorer les jonctions à l'intérieur des circuits intégrés en traversant ceux-ci pour rejoindre la terre.

Les TAUX D'HUMIDITÉ acceptables pour les composants électroniques se situent entre 35% et 60%. Il est donc impératif que les équipements d'un S.I. soient situés dans des locaux suffisamment aérés, isolés et dont la température puisse être maintenue entre des fourchettes raisonnables. La présence d'une climatisation efficace est donc très souhaitable.

III.4.8.PRÉSENCE DE POUSSIÈRES:

III.4.8.1.Causes des dysfonctionnements liés à l'accumulation de poussières:

L'atmosphère de la plupart des lieux de vie ou de travail (même des mieux entretenus) est plus ou moins chargée de différentes poussières: poussières minérales issues du délitement des constructions (particules de plâtre ou de ciment), particules végétales (pollens), micro-particules issues des activités domestiques ou industrielles (chauffage domestique, gaz d'échappement, etc.), fibres textiles détachées des vêtements, des tapis et moquettes, etc. Ces particules sont présentes même dans les lieux clos et non fréquentés car sous l'action des vibrations et du vieillissement des matériaux, elles se détachent des surfaces intérieures.

Dans les locaux fréquentés, et en particulier les locaux professionnels, les différents occupants et visiteurs apportent avec eux des particules collées à leurs chaussures ou à leurs vêtements. Ils y apportent également les cheveux et autres poils qu'ils ont tendance à perdre.

La fumée des cigarettes est également une importante source de pollution aux particules, d'autant plus que celle-ci, en plus des particules engendrées par la combustion du tabac, contient des produits de combustion qui les agglomèrent et les collent sur les surfaces.

D'autre part, chacun peut également constater, simplement en renversant un clavier d'ordinateur, que la consommation de nourriture produit également beaucoup de débris.

En l'absence de mesures protectrices, ces différentes particules ont tendance à être entraînées dans les boîtiers des équipements par les systèmes de ventilation de ces derniers. Elles s'y déposent sur les différents organes intérieurs, plus ou moins agglomérées par l'humidité et les substances grasses, avec une prédilection pour les organes d'aération (grilles et pales des ventilateurs) et les surfaces chargées en électricité statique.

III.4.8.2.Effets des dysfonctionnements liés à l'accumulation de poussières:

Cette pollution peut, à la longue, gêner considérablement la circulation de l'air dans les boîtiers. En effet, en se déposant sur les grilles d'aération et les pales et roulements des ventilateurs, elle peut diminuer l'efficacité de ceux-ci. Or, cette circulation d'air est la plupart du temps le principal moyen d'évacuation de la chaleur: l'accumulation de poussières peut donc engendrer des problèmes de surchauffe très préjudiciables à la durée de vie des équipements.

D'autre part, les agglomérats de particules sèches peuvent nuire à la qualité des contacts dans les jonctions entre composants et, de ce fait, dégrader les signaux circulant entre ces composants.

A l'inverse, ils peuvent être conducteurs s'ils sont humides: leur présence en certains endroits peut provoquer des court-circuits capables de détruire certains composants, ce qui conduit généralement à un dysfonctionnement permanent.

III.4.9.AGRESSIONS MÉCANIQUES:

III.4.9.1.Causes des dysfonctionnements liés aux agressions mécaniques:

Les agressions mécaniques sont dues soit à des CHOCS subis par les équipements (soit du fait d'une chute, soit durant leur transport, soit encore en cours d'utilisation), soit à des VIBRATIONS (essentiellement pendant leur utilisation au cours d'un déplacements). Ces différentes causes produisent des accélération brèves mais intenses susceptibles d'endommager les composants, en particulier si certaines pièces de ceux-ci sont mobiles.

III.4.9.2.Effets des dysfonctionnements liés aux agressions mécaniques:

Les CHOCS subis par un équipement peuvent provoquer la rupture des liaisons mécaniques ou électriques des composants avec le châssis (rupture de fixations ou de soudures, sortie des composants enfichables de leurs "sockets", détérioration des éléments mobiles, etc.).

Les VIBRATIONS sont la plupart du temps subie par les équipements individuels mobiles utilisés en cours de transport ou par les équipements des systèmes embarqués. A moyen terme, elles ont des conséquences similaires aux chocs.

Les équipements FIXES d'un système informatique logé dans une structure d'accueil industrielle (hébergés dans des racks et fixés à ceux-ci) sont, en général, peu sensibles aux agressions mécaniques (en dehors de catastrophes naturelles ou de guerres). Il n'en est évidemment pas de même lorsque ces équipements sont distribués dans des locaux non protégés ou lorsqu'il s'agit d'équipements mobiles comme les ordinateurs portables ou les tablettes.

Si les équipements ne sont pas en fonction au moment du choc ou pendant les vibrations, les dégâts peuvent être circonscrits à ce qui est décrit plus haut. Sinon, ces dégâts peuvent eux-mêmes entraîner des conséquences, d'ordre électrique, cette-fois (courts-circuits ou arcs électriques entraînant la destruction de composants).

Notons que les DISQUES DURS mécaniques, très vulnérables aux chocs et vibrations du fait de la présence de parties tournantes et du mécanisme des têtes de lecture, possèdent des systèmes de verrouillage permettant de bloquer le mécanisme pendant une manutention ou un transport. Cependant, lorsqu'on utilise un ordinateur portable dans un moyen de transport (train, autobus, etc.), le disque dur ne peut évidemment être bloqué: il faut donc faire très attention aux mouvements du support sur lequel on les pose et intercaler si nécessaire une couche amortissante entre l'équipement et le support.

III.5.MESURES DE PROTECTION CONTRE LES DYSFONCTIONNEMENTS MATÉRIELS PERMANENTS:

III.5.1.INTRODUCTION:

Dans les pages précédentes, nous avons exposé les différentes causes de dysfonctionnement des COMPOSANTS MATÉRIELS d'un S.I. Nous trouvons essentiellement parmi elles:

- Celles qui sont produites par le VIEILLISSEMENT NORMAL des composants;
- Celles qui sont produites directement (par un DYSFONCTIONNEMENT IMMÉDIAT) ou indirectement (par l'ACCÉLÉRATION DU VIEILLISSEMENT), du fait des agressions issues de l'environnement d'utilisation.

REMARQUE: *pour obtenir des renseignements sur ces notions, consulter l'annexe du présent ouvrage.*

Il est évident qu'en regard de ces deux types de causes, les dispositions susceptible d'améliorer la fiabilité globale d'un S.I entraînent des surcoûts plus ou moins élevés en FONCTION DES NIVEAUX DE SÉCURITÉ VISÉS. Ces surcoûts vont concerner les domaines de la conception, de l'exploitation et du maintien en condition opérationnelle. Il est donc primordial, lors de la création d'un S.I, comme à l'occasion des évolutions futures du système, de bien définir et caractériser les exigences des différents utilisateurs en matière de sécurité d'utilisation et de continuité des services offerts.

III.5.2.ACTIONS DE PROTECTION CONTRE LES DYSFONCTIONNEMENT:

III.5.2.1.INTRODUCTION:

Ce sous-chapitre présente et commente succinctement différentes actions susceptibles de limiter la survenue de dysfonctionnements matériels (actions PRÉVENTIVES) ou d'en limiter les effets (actions CORRECTIVES). Les actions préventives tendent essentiellement à infléchir la conception et la réalisation des système de façon à prendre en compte les besoins en matière de FIABILITÉ et de CONTINUITÉ DES SERVICES tandis que les actions CORRECTIVES tendent à facilité le retour au fonctionnement nominal après une panne.

III.5.2.2.SÉCURISER L'ENREGISTREMENT DES DONNÉES PERSISTANTES DU S.I:

III.5.2.2.1.NOTION DE DONNÉES PERSISTANTES:

A chaque instant, un S.I. supporte l'exécution de nombreux logiciels. Durant leur exécution, ces logiciels sont amenés à utiliser et à produire de nombreuses données.

Certaines des données produites n'ont d'utilité que pendant l'exécution en cours du logiciel. Elles sont, en général, détruites en fin d'exécution et l'espace qu'elles occupaient sur les différents supports d'enregistrement est récupéré (il s'agit, par exemple, des "fichiers temporaires" créés durant l'exécution dans le cadre d'un traitement donné). Ces données sont, dans ce cas, dites NON PERSISTANTES.

D'autre données produites, en revanche, doivent être conservées car elles pourront être réutilisées pour une session d'exécution ultérieure du même logiciel ou par un autre logiciel. Ces données sont dites PERSISTANTES car elles "survivent" à l'exécution des logiciels qui les produisent ou utilisent.

Les données PERSISTANTES d'un S.I. sont enregistrées sous diverses formes (fichiers à plat, bases de données, etc) dans des unités de stockage permanent (disques durs, S.S.D, clefs USB, Cloud, etc.). Ce sont ces enregistrements qui assurent la persistance de ces données d'une session d'exécution à une autre.

RAPPEL: Dans le domaine de l'informatique, on nomme SESSION une période bien délimitée pendant laquelle un système de traitement informatique effectue des traitements pour le service d'un utilisateur donné. Cet utilisateur peut être:

- Un **utilisateur "humain"**. Par exemple: un secrétaire utilisant un logiciel de bureautique);
- Un **logiciel** s'exécutant sur la même machine. Par exemple: un navigateur web utilisant les services réseau du système d'exploitation);
- Un **système distant**. Par exemple: un système de traitement déléguant l'exécution d'une requête à un système de traitement distant en utilisant le protocole C.O.R.B.A.

En général, une session débute par la CONNEXION de l'utilisateur à la ressource et se termine par sa DÉCONNEXION. Les données persistantes sont alors celles qui survivent à la déconnexion.

III.5.2.2.2.IMPORTANCE DE LA SÉCURISATION DE CES DONNÉES:

A tout instant, l'ensemble des données PERSISTANTES enregistrées par un S.I constitue une "photographie" de l'ÉTAT D'AVANCEMENT des différentes tâches supportées par ce système. De ce fait, un dysfonctionnement matériel grave provoquant une altération irréversible de tout ou partie de ces données sur un support quelconque peut entraîner l'impossibilité de continuer certains des travaux en cours (les travaux qui UTILISENT ces données mais aussi ceux qui les PRODUISENT).

Ce type d'incident peut donc avoir de très graves conséquences sur l'activité d'une entreprise. Dans certains cas (la perte d'une base de donnée "clients", par exemple), sa survie peut être menacée. Il est donc de la plus grande importance de sécuriser les données persistantes d'une organisation contre les dysfonctionnements matériels.

III.5.2.2.3.TECHNIQUES DE SÉCURISATION DES DONNÉES:

III.5.2.2.3.1.Principe de base:

Le principe consiste toujours à dupliquer les données persistantes à sécuriser sur un ou plusieurs supports permanents afin de pouvoir les récupérer dans le S.I. dans le cas où un dysfonctionnement les a endommagées sur leur support de travail.

NOTA: *un support permanent doit être capable de conserver les informations enregistrées sans qu'il soit nécessaire de les régénérer périodiquement par un processus automatique (exemples: disque dur, clef U.S.B).*

Pour assurer la sécurité des données, le fonctionnement de l'équipement de sauvegarde doit être le plus indépendant possible de celui des équipements qui utilisent ou produisent les données sauvegardées. Cette précaution permet d'éviter que le fonctionnement du support de sauvegarde soit altéré par les mêmes causes que celui des équipements dont il assure la sauvegarde.

D'un point de vue technique, cette recommandation se traduit par:

- Veiller à ce que l'équipement de sauvegarde ne soit pas directement relié aux équipements à sauvegarder par des liaisons filaires "point à point" à média métallique. Cette précaution permet de limiter le risque de remontée de perturbations électriques ou électrostatiques. La solution la plus sûre est une liaison par réseau à base de fibre optique;
- Veiller à ce que l'alimentation électrique de l'équipement de sauvegarde soit le plus possible séparée de celle de l'équipement à sauvegarder (par exemple, en utilisant un système d'Alimentation Sans Interruption (communément appelé onduleur);
- Veiller à ce que l'équipement de sauvegarde ne soit pas dans le même local que les équipements dont il sauvegarde les données. Ceci permet d'éviter que les équipements à sauvegarder et les équipements de sauvegarde ne soient touchés simultanément par la même catastrophe (incendie, fuite d'eau, vandalisme, etc.).

La suite du sous-chapitre examine quelques exemples de dispositifs de sauvegarde.

III.5.2.2.3.2.Utilisation d'un espace de sauvegarde en NUAGE (stockage dans le CLOUD):

PRÉSENTATION:

La SAUVEGARDE DANS LE CLOUD consiste à déléguer la sauvegarde des données persistantes d'un client (entreprise ou particulier) à un opérateur accessible par internet. Cet opérateur se charge de gérer les données sauvegardées (les enregistrer, les sécuriser, les protéger contre les actions malveillantes, les restituer) dans son espace de stockage. Les données du client sont accessibles par celui-ci en ligne, via le réseau internet.

Le service peut être gratuit en deçà d'une certaine capacité de stockage (Par exemple, cette limite est de 5 go pour Onde drive de microsoft et de 15 go pour Google drive. Au delà de ces limites, il devient payant (de l'ordre de 2 euros/mois pour 100 go).

REMARQUE: Ce service cloud correspond au niveau d'abstraction PAAS (Platform As A Service): le client utilise une PLATEFORME externe pour stocker ses données).

AVANTAGES:

L'utilisation d'un CLOUD pour la sauvegarde des données:

- Permet d'éloigner géographiquement les données sauvegardées des supports de données à sauvegarder, limitant ainsi drastiquement la probabilité de destruction simultanée par la même cause;
- Permet de bénéficier d'une sécurisation des données de niveau professionnel pour un coût nettement plus faible que ne le serait l'acquisition et le maintien en condition d'une infrastructure de sauvegarde (matériel et personnels) d'un même niveau. Ceci est particulièrement vrai pour un particulier ou une petite entreprise pour lesquelles, du fait de la

faible taille des données à sauvegarder, l'accès peut être gratuit (les 15 go de données gratuites offert par Google Drive peuvent souvent largement leur suffire);

- Ne nécessite ni investissement de départ ni formation particulière;
- Les donnée sont accessibles depuis n'importe quel poste connecté à Internet.

INCONVÉNIENTS ET RISQUES:

- Le risque le plus grave est la défaillance temporaire ou définitive de l'entreprise fournisseuse du CLOUD. Il s'agit la plupart du temps d'entreprises solides pour lesquelles ce risque semble minime, mais il ne faut pas oublier qu'au cas où cette défaillance se produirait, le client aurait très peu de moyens matériels et juridiques pour récupérer ses données. Ceci est moins le cas pour une sauvegarde locale pour laquelle on a un accès physique aux différents supports;
- L'utilisation des fichiers sauvegardés dépend du bon fonctionnement d'internet au niveau local, mais aussi au niveau mondial. De ce fait, en cas de dysfonctionnement local du réseau, ou de crise politique majeure, l'accès aux données peut devenir problématique pendant une durée qui peut être très importante;
- A priori, la sécurité et la confidentialité des données se doivent d'être d'un excellent niveau. Cependant, d'une part, les Clouds constituent des cibles intéressantes pour les hackers et sont souvent attaqués et d'autre part, suivant la localisation des données (qui dépend uniquement des fournisseurs), des autorités locales malveillantes peuvent être tentées d'utiliser les moyens de stockage à des fins politiques ou délictueuses (chantage, espionnage, etc.).

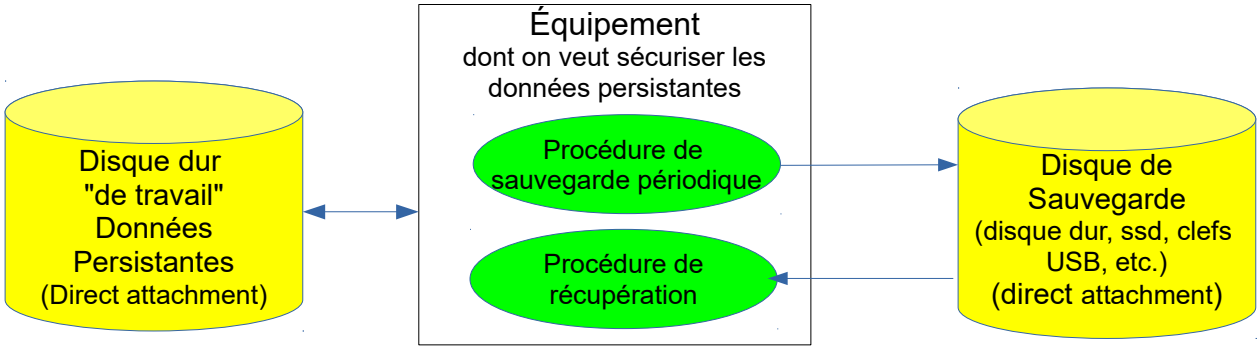
III.5.2.2.3.3.Utilisation d'un support de sauvegarde directement attaché à l'équipement sans utilisation de R.A.I.D:

PRÉSENTATION:

Ce type de sauvegarde consiste à effectuer la copie des données à sauvegarder sur un support de sauvegarde directement attaché a l'équipement dont on veut sauvegarder des données. Après la sauvegarde sur le CLOUD, c'est le dispositif le plus simple à mettre en place. En effet, le support de sauvegarde peut être:

- Soit un disque dur supplémentaire dédié à cette fonction et connecté à l'équipement par Direct Attached Storage (D.A.S) et utilisant l'un des protocoles dédiés à ce type de liaison (PATA, SATA, eSATA, SCSI, SAS, etc.);
- Soit un support amovible se branchant sur l'un des ports U.S.B de l'équipement.

EXEMPLE: Le schéma ci-dessous décrit un tel dispositif:



Sauvegarde sur disque directement attaché à l'équipement à sauvegarder

DÉCLENCHEMENT DES SAUVEGARDES:

Le déclenchement manuel des actions de sauvegarde peut suffire lorsque le S.I. n'est jamais utilisé simultanément par plusieurs personnes (ordinateur personnel ou familial, système monoposte d'une microentreprise, etc.).

En revanche, si plusieurs sessions d'utilisateurs peuvent être actives simultanément, il est difficile de déterminer un instant pertinent pour déclencher la sauvegarde de données partagées entre plusieurs utilisateurs. De ce fait, la PLANIFICATION des opérations de sauvegarde est recommandée, afin de les déclencher durant les périodes de non utilisation du S.I. (si de telles périodes existent et sont prévisibles).

Les systèmes d'exploitation offrent tous aux utilisateurs la possibilité de planifier l'exécution de logiciels à une date donnée ou avec une fréquence donnée:

- Dans les environnements WINDOWS, on utilise la fonctionnalité "tâches planifiées";
- Dans les environnements LINUX, c'est le logiciel CRON qui peut être utilisé.

REMARQUE: La période d'enregistrement doit être fixée en fonction de l'activité de l'équipement à sécuriser. Par exemple, pour sécuriser des équipements supportant des tâches administratives courantes, une sauvegarde systématique programmée pendant une période de non-activité (tous les jours à minuit, par exemple) peut être suffisante. En revanche, il est évident que cette périodicité ne convient absolument pas pour sécuriser la base de donnée des commandes d'un grand système de vente en ligne qui est utilisé 24 heures sur 24;

AVANTAGES:

- La solution est très peu onéreuse (il suffit de disposer d'un disque de sauvegarde suffisamment dimensionné);

INCONVÉNIENTS:

- Le support de sauvegarde est directement attaché à l'équipement qui supporte le disque des données à sauvegarder. Les deux supports sont donc probablement très proches, situés dans le même local ou dans des locaux mitoyens. De ce fait, un incident grave affectant ces locaux (incendie, inondation, agressions physiques, etc.) risque de détruire à la fois les données et leur sauvegarde;
- L'attachement direct des deux supports permet à des perturbations électriques, électrostatiques ou électromagnétiques d'affecter à la fois les deux supports et l'équipement auquel ils sont attachés;
- Enfin, l'attachement direct implique d'installer au moins un disque de sauvegarde par équipement, ce qui peut entraîner des surcoûts importants et compliquer la récupération des données.

La sécurisation est donc assez faible.

III.5.2.2.3.4.Utilisation d'un support de sauvegarde directement attaché à l'équipement et géré par un R.A.I.D Logiciel:

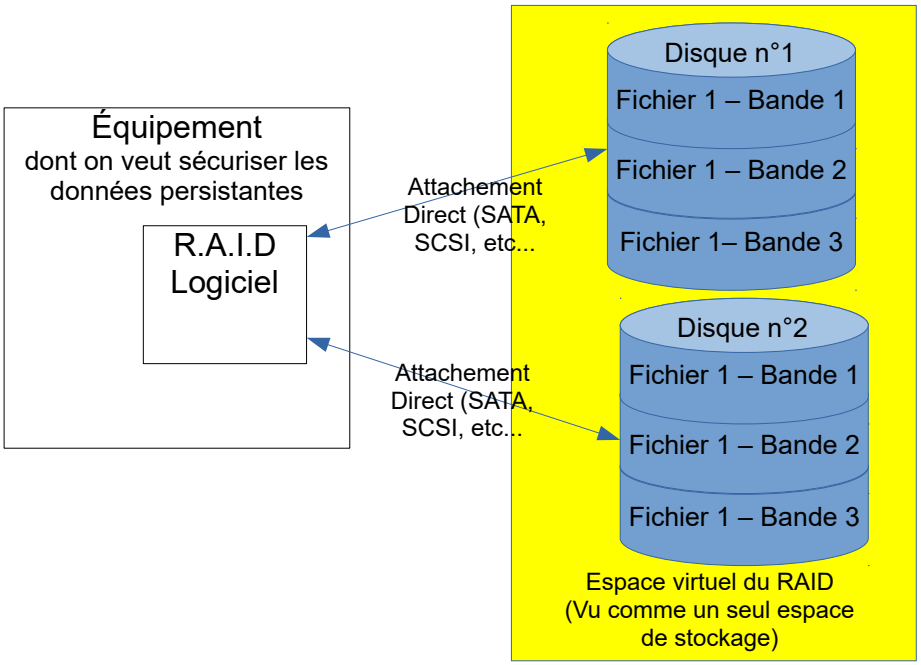
RAPPEL: *L*a technologie R.A.I.D (Redundant Array of Independent Disk) fait l'objet d'un rappel en annexe du présent ouvrage. Elle permet:

- De VIRTUALISER les espaces de stockage de plusieurs supports de données en les présentant aux utilisateurs comme un seul espace;
- De REPARTIR physiquement les données des fichiers sur plusieurs supports de façon à optimiser les temps d'accès ou à sécuriser les enregistrements (par utilisation de redondances ou de codes auto correcteurs).

Un R.A.I.D logiciel est un R.A.I.D entièrement supporté par le système d'exploitation alors qu'un R.A.I.D matériel est installé sur un CONTRÔLEUR R.A.I.D enfiché dans le bus d'entrée-sortie.

PRÉSENTATION:

La solution présentée ici correspond au schéma ci-dessous:



R.A.I.D 1

*Les disques 1 et 2 sont vus par l'utilisateur comme un seul espace;
*Les deux fichiers 1 physiques sont vus comme un seul fichier ;
*Toute modification apportée à ce fichier sont reportées reportées sur les copies du disque 1 et du disque 2.

Elle consiste à installer sur l'équipement à sauvegarder un RAID logiciel (RAID 1) mettant en commun deux disques en attachement direct. Supposons qu'au moment de la création du R.A.I.D, le disque 1 soit le disque à sauvegarder et que le disque 2 soit vide. La fonction MIRRORING du RAID 1 va dupliquer les informations du disque 1 dans le disque 2. A partir de cet état, l'utilisateur voit les deux disques comme un seul espace de stockage contenant un seul Fichier 1. Toute modification apportée à ce fichier "virtuel" se traduira par la modification des deux disques "physiques" du R.A.I.D 1. Il n'existe donc plus, à proprement parler de disque de sauvegarde car la sauvegarde est réalisée par le maintien à l'identique des deux copies physiques.

AVANTAGES:

- Les modifications apportées aux données sont sauvegardées automatiquement sur les deux disques physiques après chaque modification. Il n'est donc plus nécessaire de planifier les actions de sauvegarde;

- Après dysfonctionnement puis réparation ou remplacement d'un des disques physiques, la fonction MIRRORING duplique automatiquement dans ce disque les données de l'autre disque physique. La récupération des données est donc automatique;
- La solution est très peu onéreuse car la configuration en R.A.I.D 1 logiciel est disponible sur la plupart des systèmes d'exploitation.

INCONVÉNIENTS:

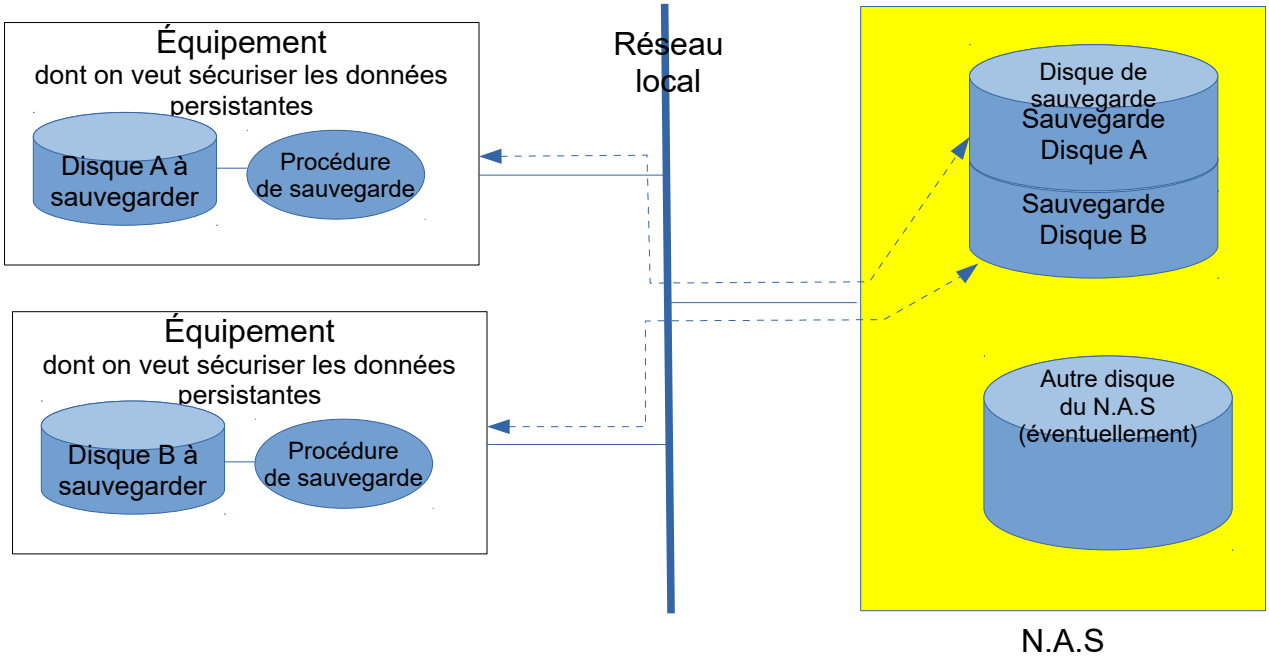
- L'attachement direct des deux disques ne permet pas de les éloigner suffisamment l'un de l'autre et de l'équipement pour éviter une destruction simultanée;
- L'attachement direct ne permet pas le remplacement "à chaud" d'un disque défaillant;
- La vitesse d'écriture des données à sauvegarder est ralentie par le fait qu'elle doit s'effectuer sur les deux disques physiques du R.A.I.D 1;
- Les données ne sont directement accessibles qu'à l'équipement local.

III.5.2.2.3.5.Utilisation d'un support de sauvegarde en réseau sans utilisation d'un R.A.ID:

RAPPEL: Un N.A.S (Network Attached Storage) est un équipement MATÉRIEL qui héberge une GRAPPE d'unités de stockage (disques durs ou S.S.D) et permet de les connecter à un réseau. Vis à vis des hôtes de ce réseau, un N.A.S se comporte comme un SERVEUR DE FICHIER qui leur permet d'accéder (en écriture et en lecture) à tous les supports d'enregistrement de la grappe. La technologie N.A.S fait l'objet d'un rappel en annexe du présent ouvrage.

PRÉSENTATION:

La solution présentée ici consiste à héberger le support de sauvegarde dans un N.A.S, le ou les supports des données à sauvegarder restant en attachement direct ou étant hébergés par un N.A.S. distinct.



COMMENTAIRES:

- ***NOTA:*** Le fait d'héberger le support de sauvegarde et le support à sauvegarder dans le même N.A.S n'est pas optimale du point de vue de la sécurité car les deux supports étant attachés directement au même équipement (le N.A.S) sont forcément très voisins géographiquement: ils risquent donc d'être atteints en même temps par les mêmes causes de dysfonctionnement (pannes d'alimentation, incendies, inondations, etc);
- ***REMARQUE:*** Dans la configuration représentée par le schéma, le disque de sauvegarde est hébergé par le N.A.S. Il est possible d'utiliser les autres emplacements pour d'autres utilisations. Tous les hôtes du réseau peuvent accéder aux données du N.A.S. Dans cet exemple, seuls deux équipements accèdent au N.A.S pour sauvegarder leurs données sur le disque A.

AVANTAGES:

- Le support à sauvegarder n'est lié au support de sauvegarde que par une liaison en réseau: ceci permet d'éviter que les deux équipements ne soient perturbés par les mêmes anomalies électriques ou électrostatiques (surtout s'il s'agit d'un réseau fibre). D'autre part, cette solution permet d'éloigner géographiquement les deux supports;
- La technologie N.A.S permet de sécuriser le fonctionnement du support de sauvegarde, en particulier dans le domaine de l'alimentation électrique;
- Un même support de sauvegarde peut être utilisé par plusieurs hôtes du réseau;
- Pour certains N.A.S, un disque du cluster peut être remplacé "à chaud".

INCONVÉNIENTS:

- Les N.A.S sont des équipements relativement onéreux;
- Les sauvegardes doivent être planifiées comme dans le premier cas étudié;
- Dans cette configuration, si le disque de sauvegarde peut être remplacé à chaud, la récupération de son contenu doit être effectuée par recopie du (ou des disques) à sauvegarder.

III.5.2.2.3.6.Utilisation d'un R.A.I.D sur un N.A.S:

PRÉSENTATION:

La plupart des N.A.S hébergent un logiciel permettant d'organiser en R.A.I.D tout ou partie des disques de la grappe. Ce R.A.I.D peut être organisé et paramétré par l'intermédiaire du serveur H.T.T.P interne de paramétrage du N.A.S. Le paramétrage peut donc être effectué depuis n'importe quel hôte du réseau, en utilisant un navigateur. La solution consiste à définir un R.A.I.D 1 (ou tout autre R.A.I.D intégrant la fonction MIRRORING) comprenant au moins deux disques durs.

Les fichiers à sauvegarder sont alors hébergés dans l'espace virtuel constitué par ces deux disques durs. Si l'on néglige la durée de propagation des modifications d'un disque sur l'autre disque, la fonction MIRRORING du R.A.I.D 1 permet de disposer en permanence de deux copies des données à sauvegarder.

AVANTAGES:

- A tout moment, la solution permet de disposer automatiquement de deux copies des données à sauvegarder (sauf pendant la durée de propagation des modifications d'un disque vers l'autre disque), sans qu'aucune planification des duplications soit nécessaire;
- L'utilisation d'un N.A.S permet de sécuriser le fonctionnement des deux disques physiques;
- Dans le cas où le N.A.S permet le remplacement à chaud des disques en cas de dysfonctionnement, la fonction MIRRORING permet la reconstitution automatique du contenu du disque remplaçant;

INCONVÉNIENTS:

- Si l'on s'équipe d'un N.A.S performant, la solution peut être onéreuse;
- Les données et leur sauvegarde se retrouvant dans le même équipement, la destruction du N.A.S risque d'entraîner leur perte simultanée. Il est donc prudent d'effectuer à intervalles plus ou moins réguliers d'autres sauvegardes (par exemple, sur des supports amovibles ou dans le CLOUD).
- La vitesse d'écriture des données à sauvegarder est ralentie par le fait qu'elle doit s'effectuer sur les deux disques physiques du R.A.I.D 1;

III.5.2.2.3.7.Résumé et conclusion sur les solutions de sécurisation des données persistantes présentées:

SAUVEGARDE SUR LE CLOUD:

La sauvegarde sur le CLOUD est une solution peu onéreuse qui ne demande aucun investissement initial en matériel et en logiciel. En ce qui concerne les frais de location, ceux-ci sont très peu coûteux, voire nuls. L'accès aux données sauvegardées (manuellement ou par une procédure système) est très simple et rapide. Il peut être réalisé à partir de n'importe quel poste accédant à internet.

Cependant, cette solution exige de disposer d'une connexion internet fiable. De plus, si la perte des données est très peu probable, elle peut survenir en cas de dysfonctionnement majeur du fournisseur de cloud (piratage, panne générale, faillite): dans ce cas, la récupération des données est souvent problématique. Il est donc conseillé de doubler les sauvegardes CLOUD par des sauvegardes simples sur support amovibles (disques ou clefs U.S.B) à des intervalles réguliers.

Cette solution convient particulièrement à des particuliers désireux de sauvegarder à peu de frais leurs documents écrits, leurs photographie ou leurs vidéos et de pouvoir y accéder depuis n'importe quel poste connecté à internet (y compris depuis leur téléphone portable).

SUPPORT DE SAUVEGARDE DIRECTEMENT ATTACHE A L'ÉQUIPEMENT ET NON GÉRÉ PAR UN RAID LOGICIEL:

La solution est peu onéreuse (il suffit de disposer d'un disque de sauvegarde suffisamment dimensionné). Elle a l'avantage de pouvoir fonctionner "en local", sans avoir besoin d'une connexion réseau.

Cependant, la sécurisation des données est assez faible car le support de sauvegarde est directement attaché à l'équipement qui supporte le disque des données à sauvegarder: cette configuration expose le dispositif à un dysfonctionnement simultané des deux supports.

De plus, le fait de sauvegarder à intervalles réguliers pose le problème de la détermination de la fréquence minimale admissible: ce paramètre doit s'apprécier en fonction de l'activité du S.I.

Cette solution convient à des entreprises individuelles ou de petites entreprises dont le type et l'intensité de l'activité permettent, en cas de "crash" du S.I. de se contenter de récupérer les données d'un état antérieur de quelques heures à la survenue du "crash".

SUPPORT DE SAUVEGARDE DIRECTEMENT ATTACHE A L'ÉQUIPEMENT ET GÉRÉ PAR UN RAID 1 LOGICIEL:

Il s'agit également d'une solution peu onéreuse et relativement facile à mettre en place moyennant un minimum de connaissances en administration de systèmes. En fonctionnement normal, elle exige très peu d'interventions humaines car les réplications ou régénérations de données sont effectuées automatiquement.

Cette solution, pour être mise en place, exige quelques connaissances en administration système. Si l'on dispose de ces compétences en interne, son coût n'est pas plus élevé que celui de la solution précédente. Elle a l'avantage de fournir en permanence (a la durée du MIRRORING près), des informations de sauvegarde redondantes sur les deux disques du R.A.I.D 1.

Cependant, cette solution ne permet pas le remplacement "à chaud" d'un disque défaillant et reste peu sécurisée en cas de sinistre (incendies, dégâts des eaux, etc.).

Cette solution peut donc convenir pour tous les S.I dont la continuité de service n'est pas trop critique.

SUPPORT DE SAUVEGARDE HÉBERGE SUR UN N.A.S (SANS UTILISATION D'UN RAID):

Cette solution est plutôt onéreuse, bien que les slots libres du N.A.S puissent être utilisés pour d'autres fonctions. En revanche, elle est relativement bien sécurisée. De plus, l'ajout d'un N.A.S en réseau n'exige pas de compétences particulière (un N.A.S peut se brancher sur une BOX INTERNET dans une prise RJ45 disponible). Elle convient donc pour tous les S.I. dont les données rémanentes ne sont pas trop volumineuses.

SUPPORTS HÉBERGES SUR UN N.A.S AVEC UTILISATION D'UN RAID 1:

Le principal avantage de cette solution est qu'elle permet à tout moment de disposer automatiquement de deux copies des données à sauvegarder sans qu'aucune planification des duplications soit nécessaire (sauf pendant la durée de propagation des modifications d'un disque vers l'autre disque). De plus, dans le cas où le N.A.S permet le remplacement à chaud des disques en cas de dysfonctionnement, la fonction MIRRORING permet la reconstitution automatique du contenu du disque remplaçant.

Cependant, si l'on s'équipe d'un N.A.S performant, la solution peut être onéreuse. D'autre part, la sécurité pâtit du fait que les données et leur sauvegarde se trouvent dans le même équipement. Il est donc prudent d'effectuer à intervalles plus ou moins réguliers d'autres sauvegardes (par exemple, sur des supports amovibles ou sur le cloud).

Enfin, la vitesse d'écriture des données à sauvegarder est ralentie par le fait qu'elle doit s'effectuer sur les deux disques physiques du R.A.I.D 1.

Cette solution combine les avantages du N.A.S (gestion sécurisée de disques de grande capacité) et ceux du R.A.I.D 1 (virtualisation de l'espace disque total et sécurisation par Mirroring). Elle convient donc pour tous les S.I. dont les données rémanentes ne sont pas trop volumineuses. Cependant, le

paramétrage d'un R.A.I.D 1 sur un N.A.S exige quelques connaissances en administration systèmes et réseaux.

REMARQUES:

- d'autres types de R.A.I.D, combinés à l'utilisation d'un cluster de plusieurs disques sur le N.A.S permettent des sauvegardes plus volumineuses tout en étant sécurisées (par exemple, un R.A.I.D 5 avec 4 disques);
- La sauvegarde sur le CLOUD peut être utilisée "en doublon" pour sécuriser les sauvegardes obtenues par d'autres dispositifs.

III.5.2.3.BIEN CHOISIR LES ÉQUIPEMENTS OU COMPOSANTS DU S.I:

Pour obtenir une fiabilité globale d'un S.I. conforme aux exigences des utilisateurs et conserver ces capacités lors des évolutions de ce système, une des solutions consiste a agir au niveau du choix des composants (donc, au niveau des phases de CONCEPTION) en s'assurant que leur fiabilité est suffisante pour que ces exigences puissent être atteintes.

Les exigences de fiabilité concernant les différents équipements ou composants d'un S.I. varient beaucoup suivant les fonctionnalités auxquelles ceux-ci participent dans le cadre de ce système. De plus, comme il n'est pas rare qu'un équipement participe à plusieurs des fonctionnalités du S.I, un tel équipement doit être dimensionné pour pouvoir répondre à l'exigence la plus forte en matière de fiabilité.

Il est donc important, pour éviter les "sur spécifications" (génératrices d'inflation des coûts), d'évaluer correctement les besoins en fiabilité concernant chaque équipement, en tenant compte de ses différentes utilisations.

III.5.2.4.RESPECTER LES CONDITIONS D'UTILISATION:

III.5.2.4.1.INTRODUCTION:

Les estimations de fiabilité données par les constructeurs ne sont garanties que pour des composants fonctionnant dans des conditions d'exploitation conformes à celles qui sont préconisées par ces constructeurs. Si ces conditions ne sont pas respectées, les probabilités de dysfonctionnement (voir en annexe les considérations sur la fiabilité) peuvent se trouver notablement augmentées.

De ce fait, les conditions RÉELLES d'utilisation des composants influent très notablement sur la courbe de fiabilité de ceux-ci en fonction de la durée d'utilisation. Nous avons étudié dans les chapitre précédents les différentes causes liées à l'environnement susceptibles soit d'entraîner immédiatement le dysfonctionnement d'un composant électronique, soit d'entraîner à terme un dysfonctionnement en provoquant son vieillissement accéléré. Nous avons vu que ces différentes causes peuvent être résumées par la liste suivante:

1. Une alimentation électrique défaillante ou non conforme aux exigences des constructeurs.
2. Des défauts dans les liaisons entre équipements ou composants internes (mauvais contacts, problèmes de masses et de terre).
3. Des perturbations électromagnétiques d'origine internes (rayonnements émis par certains composants internes à l'enceinte du S.I.)
4. Des perturbations électromagnétiques d'origine externes (dues à des équipements perturbateurs externes à l'enceinte du S.I).
5. Des perturbations électrostatiques d'origine interne (dues à des ambiances trop sèches ou la présence de poussières agglomérées dans les châssis);
6. Des perturbations électrostatiques d'origine externe (phénomènes climatiques tels que la foudre ou perturbations dues à des équipements externes);
7. Une ambiance climatique anormale:
   - Température de fonctionnement anormale;
   - Humidité excessive ou trop faible;
   - Présence de poussières;
8. Des agressions mécaniques (vibrations et chocs causés par l'environnement d'utilisation).

Les paragraphes suivants détaillent les mesures de protection les plus importantes:

III.5.2.4.2. ACTIONS POUR CONTRER LES DYSFONCTIONNEMENTS DE L'ALIMENTATION ÉLECTRIQUE:

III.5.2.4.2.1.Utilisation de dispositifs d'Alimentation Sans Coupure:

PRINCIPES ET DESCRIPTIONPHYSIQUE:

Ces dispositifs, que l'on appelle communément "onduleurs", sont en fait composés de trois éléments "fonctionnels" distincts:

- Un dispositif "redresseur" permettant de transformer un courant alternatif en courant continu;
- Un autre dispositif capable de stocker l'énergie du courant continu obtenu sous forme chimique (batterie électrique) ou parfois mécanique (air comprimé, volant inertiel, etc.);
- Un autre dispositif capable de recréer un courant alternatif de tension et de fréquence données à partir de l'énergie stockée. Ce dernier dispositif peut être un système mécanique (alternateur) ou un dispositif électronique (c'est en fait ce dernier dispositif que l'on nomme ONDULEUR).

Dans la plupart des cas, le stockage de l'énergie se fait dans des batteries électriques. L'onduleur transforme le courant continu stocké par ces batteries en un courant alternatif dont la tension et la fréquence ne peuvent, du fait de la séparation des circuits opérée par le dispositif de stockage, être altérées par les perturbations de la source externe de courant alternatif (coupures de secteur, micro-coupures, variations de fréquence et de tension, etc.),

Système d'Alimentation Sans Coupure

AVANTAGES:

- Les systèmes d'A.S.C. fournissent un courant alternatif non perturbé et de caractéristiques constantes à partir d'une source perturbée. Ils permettent donc de protéger les équipements des défauts passagers de l'alimentation électrique externe (micro-coupures, coupures "erratiques", variations de la tension et de la fréquence);
- Ils offrent d'autre part l'avantage de permettre à l'équipement qu'ils alimentent de fonctionner pendant quelques temps "en autonomie" après la survenue d'une coupure de l'alimentation électrique externe. Ils permettent donc de pallier pour une durée déterminée l'interruption de l'alimentation électrique externe;
- Ils intègrent souvent des dispositifs "para-foudres".

INCONVÉNIENT:

Le coût de ces dispositifs dépend essentiellement de la puissance électrique qui peut être délivrée en sortie et de la durée maximale de fonctionnement en autonomie exigée. Leur prix peut représenter une fraction importante du prix de l'équipement à protéger;

EXEMPLES:

- Un équipement permettant d'alimenter un ordinateur de "gamer" équipé d'une carte graphique haut de gamme doit pouvoir délivrer une puissance d'environ 1500 watts. Si l'on désire avoir une autonomie d'une dizaine de minutes, son prix de revient va être de l'ordre de quelques centaines d'euro. Ce prix est à comparer avec le prix de l'ordinateur protégé (entre 1500 et 2000 euros, à peu près);
- Le coût d'un équipement capable de protéger l'ensemble des équipements sensibles d'un data center avec une autonomie de 1 heure peut avoisiner quelques dizaine de milliers d'euros.

Il s'agit donc d'équipements très coûteux à l'acquisition, mais aussi à l'entretient, car les batteries, qui constituent une fraction importante du prix d'acquisition, doivent être remplacées au bout d'environ deux années.

CONCLUSION:

Les dispositifs d'A.S.C. garantissent une très bonne protection contre les dysfonctionnements de l'alimentation électrique externe et, dans une certaine mesure, contre la foudre.

Ils permettent également, en cas de défaut total de l'alimentation interne, de fonctionner en mode autonome pendant une durée qui permet soit de pallier une interruption de quelques minutes à quelques dizaines de minutes, soit de prendre des mesures de sauvegarde avant l'épuisement des batteries internes.

Du fait de leur prix élevé, il convient de les réserver aux équipements dont le fonctionnement est "critique" pour le S.I: serveurs, systèmes N.A.S, routeurs, etc.

REMARQUE: *dans le cas des systèmes informatiques de très petites tailles, constitués de très peu de postes informatiques (installations familiales, micro-entrepreneurs, très petites entreprises, particuliers ayant besoin de travailler en ligne, etc.), l'utilisation de PC portables permet de disposer d'une autonomie de plusieurs heures en cas de panne électrique externe, à condition que ces PC soient branchés en permanence au secteur quand celui-ci est disponible. Dans ce cas, pour travailler en ligne pendant une panne de secteur, il suffit d'utiliser un téléphone mobile configuré en point d'accès wifi internet: ce dispositif constitue un "mode dégradé" peu coûteux et dont la mise en place ne demande qu'une minute ou deux.*

III.5.2.4.2.2.Utilisation de dispositifs d'alimentation de secours:

Ces dispositifs sont constitués principalement de GROUPES ÉLECTROGÈNES fonctionnant avec du carburant classique. Ils peuvent également comprendre une électronique interne capable de démarrer automatiquement le groupe lorsque l'alimentation externe du S.I. fait défaut.

AVANTAGES:

- Nous avons vu qu'à moins d'investissement importants dans les moyens de stockages d'électricité, les systèmes d'A.S.C. ne peuvent garantir un fonctionnement autonome sur une longue durée. En revanche, les GROUPES ÉLECTROGÈNES fonctionnant avec du carburant classique permettent un fonctionnement quasi illimité;
- Il s'agit en général de moyens robustes et fiables, nécessitant peu d'entretien;
- Comparé avec le prix des équipements qu'ils protègent, leur coût (qui varie avec la puissance et la qualité du courant fourni) n'est pas très élevé.

INCONVÉNIENTS:

- A moins de faire fonctionner en permanence le groupe électrogène (ce qui est un non sens économique et écologique), le temps de passage de l'alimentation externe à l'alimentation de secours, même s'il s'effectue automatiquement, entraîne une interruption de l'alimentation d'une durée non négligeable pour les systèmes informatiques, capable d'occasionner leur réinitialisation ou de les endommager s'ils n'ont pas été arrêtés au préalable. En effet, entre le démarrage d'un groupe et la stabilisation des paramètres du courant produit, plusieurs secondes peuvent s'écouler pendant lesquelles le courant fourni par le groupe est inexploitable;
- A moins d'investir dans des équipements de très haute qualité, la qualité du courant fourni (continuité, fréquence, tension) est en général inférieure à celle du réseau externe (réseau public).

CONCLUSION:

L'emploi de groupes de secours peut être justifié pour l'alimentation de S.I. dont la continuité du service est très importante. Cependant, du fait de la qualité du courant fourni, ils s'emploient alors EN AMONT de systèmes d'A.S.C. Les deux dispositifs, disposés en cascade, garantissent alors en cas de défaillance du système d'alimentation externe, une alimentation électrique de qualité en même temps qu'une autonomie quasi-illimitée.

III.5.2.4.3.ACTIONS CONTRE LES PROBLÈMES DE CONTACTS, MISE À LA MASSE ET À LA TERRE:

III.5.2.4.3.1.Veiller à la qualité de réalisation et à la conformité des installations:

- Lors de l'installation des équipements (installation initiale ou évolutions), surveiller la qualité de réalisation et la conformité de la distribution électrique (courant alternatif monophasé) dans les différents locaux: conformité des tableaux électriques, et des dispositifs de sécurité (disjoncteurs de divisions, disjoncteur différentiel), diamètres des conducteurs, qualité des prises électriques, solidité et bonne fixation de celles-ci, etc;
- Veiller à la qualité des connexions à la terre fournies par les prises 3 points: vérifier les tensions entre phase et terre et neutre et terre de chaque prise (en 220 volts alternatif monophasé, la tension entre terre et neutre doit être quasi nulle tandis que la tension entre phase et neutre doit être très proche de 220 volts);
- Les multiprises ne doivent être utilisées qu'en dépannage ou pour des montages d'essai et pour des durées très courtes. Elles doivent être proscrites en fonctionnement nominal. Il est donc très important pour faciliter les évolutions de prévoir dans chaque local un nombre de prises supérieur (d'environ 20%) aux besoins du moment.

NOTA: Pour effectuer rapidement les dépannages et réaliser facilement des évolutions, une installation posée "en apparent" est plus pratique à gérer qu'une installation encastrée;

III.5.2.4.3.2.Veiller à la bonne qualité des prises de terres de l'implantation:

Les fiches de terre de chacune des prises "3 points" en 220 volts alternatif monophasé sont reliées au tableau électrique de l'installation par les "fils de terre" (fils vert et jaunes en général). Le tableau électrique se charge de relier ces fils à l'installation de terre à travers un disjoncteur différentiel capable de détecter les "fuites vers la terre" et de mettre en sécurité l'installation dans le cas où un défaut est détecté.

REMARQUE: *pour éviter qu'un défaut sur une des prises entraîne la disjonction de toute l'installation, les prises peuvent être regroupées en DIVISIONS munies chacune d'un disjoncteur placé en amont du disjoncteur différentiel.*

La détection d'un courant électrique non négligeable entre le neutre d'une prise et la fiche terre ou entre les fiches terres de deux prises différentes peut indiquer:

- Soit une mauvaise connexion entre une des fiches de terre et le disjoncteur différentiel (via le tableau électrique);
- Soit la mauvaise qualité de l'installation de terre elle-même (piquet de terre ou «fond de fouille»).

REMARQUE: Pour que le disjoncteur différentiel puisse fonctionner d'une manière nominale (avec 50 Volts pour le seuil de tension et 500 mA pour le seuil de déclenchement), la résistance du "circuit de terre" doit être inférieure à 100 ohms. Cette valeur peut être vérifiée à l'aide d'un TESTEUR DE TERRE. Comme le test doit être réalisé sous-tension, en prenant des points de test dans le tableau électrique, il s'agit d'une manipulation plutôt dangereuse pour les personnels et pour les matériels qu'il vaut mieux confier à un professionnel.

III.5.2.4.3.3.Pour les équipements sensibles et critiques, favoriser les montages en "racks industriels":

- Le montage des équipements dans des armoires ("racks" industriels) permet de réaliser des installations beaucoup plus robustes qu'une simple répartition sur des plans de travail: les

liaisons entre équipements sont plus courtes et beaucoup plus protégées, les mises à la masse et à la terre bien mieux réalisées (par des dispositifs solides comme les tresses de masse).

- Les équipements montés en racks sont également bien mieux protégés des chocs et vibrations que des équipements simplement disposés sur des plans de travail;
- En revanche, pour des raisons ergonomiques évidentes, il est impossible de placer dans ces racks des terminaux de travail informatiques. En effet, les exploitants doivent pouvoir accéder à ces terminaux dans de bonnes conditions ergonomiques, si possible depuis leur poste de travail habituel.

L'installation en racks doit donc être réservée aux équipements critiques qui ne supportent pas en local des terminaux informatiques (serveurs, routeurs, unités de disques, etc.). L'accès à ces équipement (pour surveillance, dépannage ou autres raisons techniques) doit alors être assuré à distance par des terminaux X, des logiciels ouvrant des shells à distance, des navigateurs (si l'équipement intégré un serveur HTTP) ou des logiciels de prise en main à distance.

III.5.2.4.4.ACTIONS POUR MAINTENIR L'AMBIANCE CLIMATIQUE ET LA QUALITÉ DE L'AIR:

III.5.2.4.4.1.Maintenir les équipements informatiques dans une plage de température acceptable pour leur maintien en condition opérationnelle:

Lorsque les composants informatiques sont en fonction, ils dégagent par effet joule de la chaleur.

REMARQUE: *La quantité de chaleur dégagée dépend du composant lui-même mais aussi de l'activité supportée par l'équipement qui l'utilise: ainsi, le processeur d'un ordinateur accomplissant des tâches de type administratif dégage aux alentours de 150 watts tandis que le processeur d'un ordinateur exécutant un jeu vidéo moderne peut dégager plus de 1000 watts!*

Si cette chaleur n'est pas suffisamment dissipée par les équipements de ventilation des différents boîtiers d'équipements (radiateurs, ventilateurs, etc.), la température interne de ces composants tend à augmenter. Or, pour la plupart des composants, l'augmentation de la température au delà de certaines limites altère leur fonctionnement jusqu'à les rendre inopérants et même à les détériorer.

A l'inverse, lorsque les équipements informatiques ne sont pas en fonction ou sont en attente de tâche, leurs composants ne dégagent pas (ou très peu) de chaleur. De ce fait, en l'absence de dispositif de maintien de leur température, celle-ci tend à s'aligner sur la température ambiante. Si cette température descend au delà d'une certaine limite et si l'air ambiant est suffisamment humide (taux d'humidité >60%), cette humidité peut se condenser et se déposer sur les composants, entraînant une augmentation de l'oxydation et un risque de court-circuit (la ventilation des boîtiers diminue ce risque de condensation mais ne l'annule pas).

Il est donc absolument nécessaire pour le bon fonctionnement des systèmes informatiques que la température ambiante des locaux les accueillant soit comprise entre certaines limites (que l'on peut estimer à peu près entre 15 et 30 degrés Celsius).

Les grands systèmes informatiques professionnels (industriels, commerciaux, administratifs, militaires, etc) sont toujours hébergés (au moins partiellement) dans des locaux climatisés qui garantissent une température d'ambiance conforme: les équipements "critiques" (serveurs, unités de stockage de données, routeurs, etc.) sont toujours placées dans ces locaux tandis que les postes de travail des exploitants peuvent être placés dans des locaux non climatisés (mais ventilés et chauffés). L'accès physique aux équipements placés en salle climatisées est souvent réservé aux personnels amenés à intervenir physiquement sur ces équipements (essentiellement les personnels de maintenance). Les autres personnels autorisés peuvent accéder à ces équipements par le réseau interne à l'aide de

logiciels hébergés par les postes de travail (shells à distance, navigateurs, logiciels de prise en main à distance, etc.).

A défaut, de climatisation des locaux, il est possible de placer les équipements dans des locaux bien aérés et chauffés si nécessaire. La température (ainsi que l'hygrométrie) de ces locaux doit pouvoir être vérifiée facilement (il existe des équipements peu onéreux qui peuvent mesurer ces paramètres: il est bon d'en équiper chaque local). Il est également très important de protéger les équipements d'un ensoleillement direct. Il suffit pour cela d'équiper les fenêtres de stores efficaces (en effet, un objet métallique éclairé directement par le soleil peut, même dans un climat tempéré et en hiver, atteindre des températures de l'ordre de 60 degrés Celsius). Dans ce cas, il est conseillé comme précédemment de placer les équipements "critiques" dans une ou des salles dédiées dont l'accès physique est réservé à la maintenance (comme précédemment, l'accès des autres personnels autorisés doit se faire en ligne, par le réseau interne).

III.5.2.4.4.2.Protéger les équipements informatiques contre les atmosphères trop sèches ou trop humides:

Nous avons vu au paragraphe précédent que les atmosphères trop humides (à partie de 60% d'humidité) présentent un risque de condensation sur les composants, pouvant potentiellement entraîner des courts-circuits et l'oxydation des circuits. Une atmosphère trop sèche (<35% d'humidité) présente elle aussi des risques, car elle favorise les décharges électrostatiques.

La plage de fonctionnement idéale est souvent définie entre 40% et 60% d'humidité.

La climatisation est évidemment le dispositif de protection idéal contre les anomalies de l'hygrométrie, à condition d'être correctement réglée (55% d'humidité constitue un bon compromis entre le bien être des personnels et les exigences des matériels).

Dans les locaux non climatisés, les exigences exposées au paragraphe précédent restent globalement de mise (bonne ventilation, chauffage si nécessaire). Cependant, il ne faut pas oublier que le phénomène de condensation est lié à la fois à la température de l'air et au degrés d'hygrométrie: la "tension de vapeur" de l'air augmente avec sa température. Un air chaud peut donc se charger de plus d'humidité qu'un air froid, évitant ainsi que cette humidité se condense. Il est donc prudent, pour éviter la condensation, de maintenir la température des locaux non climatises autour de 22 degrés Celsius.

III.5.2.4.4.3.Protéger les équipements informatiques contre les poussières atmosphériques et autre impuretés amenées par les personnels et les visiteurs:

Ce type d'impuretés, en s'agglomérant avec l'humidité de l'air et le goudron de cigarette s'accumule dans les boîtiers et finit par encrasser les dispositifs de ventilation, les rendant moins efficaces. Elle peut également provoquer des courts-circuits par formation de "ponts" entre deux conducteurs. Le seul moyen de lutter contre ces impuretés est de les supprimer de l'air ambiant.

Les poussières et les particules sont essentiellement apportées par les personnels et visiteurs: débris de nourriture, cheveux et poils, fibres textiles, particules de combustion et goudrons issues du tabagisme. Elles sont également issues du délitement des revêtements internes des locaux (débris de plâtre, particules de peinture, etc).

Le confinement des matériels sensibles dans des locaux dont l'accès est limité à des personnel habilités et conscients de ces risque constitue une première mesure de protection. En ce qui concerne les locaux accessibles aux exploitants et aux visiteurs, il convient, autant que faire se peut, de:

- D'éviter d'y pénétrer avec des tenues trop poussiéreuses;
- De proscrire le tabagisme;

- D'interdire d'y consommer de la nourriture;
- De nettoyer régulièrement les sols et les parois.

III.5.2.4.4.4.Remarque sur les paragraphes précédents:

Qu'il s'agisse de la régulation de la température, de l'humidité ou de la protection contre les différentes impuretés atmosphériques, il ne faut pas oublier qu'elles dépendent en dernier ressort du bon fonctionnement de la ventilation interne des boîtiers d'équipements.

La circulation de l'air y est assurée par des ventilateur placés dans des points stratégiques de la structure. Ceux-ci aspirent l'air extérieur au boîtier et le repoussent vers l'extérieur après lui avoir fait décrire un parcours pendant lequel cet air baigne tous les composants (sauf dans des cas très improbables, les ventilateurs aspirent de l'air frais et repoussent l'air réchauffé en dehors du boîtier).

Certains composants très énergivores sont équipée de ventilateurs dédiés dont le rôle est d'accélérer la dissipation de leur chaleur interne dans l'air intérieur au boîtier (la circulation intérieure se chargeant d'évacuer cette chaleur à l'extérieur). Il s'agit essentiellement des processeurs (processeurs principaux, processeurs des cartes graphiques, etc).

Pour garantir une bonne ventilation d'un boîtier, il faudrait donc s'assurer à intervalles réguliers:

- Que les ouvertures de ventilation ne sont pas obstruées ou placées trop près d'une paroi;
- Que tous les ventilateurs intérieurs sont bien en état de marche et que leur rendement n'est pas trop affecté par la crasse déposées sur leurs pales ou sur leurs grilles. Si nécessaire, procéder au remplacement des ventilateurs en panne ou au nettoyage des ventilateurs encrassés.

Il est évident que si un particulier (très motivé!) peut assurer cette surveillance périodiquement sur son (ou ses) ordinateurs personnels, il n'en est pas question lorsqu'il s'agit d'un Système Informatique un tant soit peu important.

Dans ce dernier cas, on pourra surveiller la température interne des équipements par l'intermédiaire de moyens logiciels de visualisation (logiciels CPU Id, Core Temp, etc). Le dépannage pourra alors être déclenché sur constatation d'une anomalie de température.

REMARQUES:

- *Lorsque l'équipement en question ne peut pas supporter de tels moyens, il ne faut pas négliger l'investigation "sensorielle": impression de chaleur anormale au toucher du boîtier, détection d'une odeur de surchauffe, etc. Avec un peu d'expérience, elle suffit souvent à détecter une anomalie.*
- *La plupart des cas de surchauffe sont provoqués par une mauvaise disposition de l'équipement par rapport à ses ouvertures de ventilation.*

III.5.2.4.5.ACTIONS CONTRE LES PERTURBATIONS ÉLECTROSTATIQUES:

III.5.2.4.5.1.Rappels sur les causes de ces perturbations:

Les causes peuvent être EXTERNES au S.I ou INTERNES à celui-ci:

Les perturbations électrostatiques d'origine externe sont essentiellement provoquées par les décharges électriques atmosphériques qui se produisent à l'occasion des orages. Lorsque ces décharges se produisent entre les nuages et des bâtiments, et en l'absence de protection adéquate, les très fortes charges électriques s'évacuent vers la terre à travers les divers éléments conducteurs de ces bâtiments (conducteurs électriques, tuyaux métalliques, ferraillages, etc.), formant des courants dont l'intensité et la tension peuvent être très considérables. Ces courants peuvent donc provoquer divers dégâts, tels que des incendies, l'électrocution des personnes présentes dans ces locaux ou la destruction des équipements électriques et électroniques.

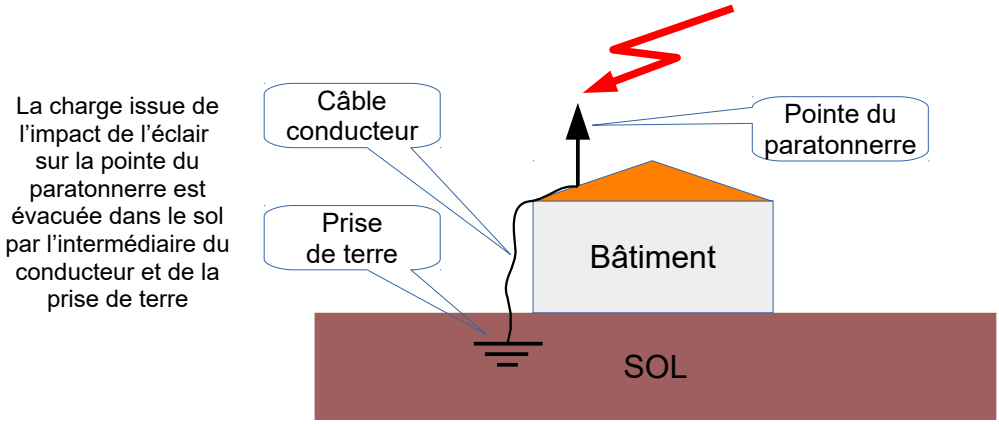
Les perturbations d'origine interne sont provoquées par des décharges électriques entre deux composants d'un même équipement. Pour se produire, ces phénomènes ont besoin de trois conditions:

- Une atmosphère très sèche;
- L'existence d'une différence de potentiel importante entre les deux composants;
- Une distance entre ces composants assez réduite pour permettre l'amorçage d'un arc électrique (La distance maximale d'amorçage croît avec la différence de potentiel).

III.5.2.4.5.2.Actions contre les perturbations électrostatiques externes:

INSTALLATION DE PARATONNERRES:

Le plus ancien système de protection contre les décharges électriques atmosphérique est celui que l'on appelle communément "paratonnerre". Ce procédé, dont l'invention remonte au XVIII° siècle, consiste à installer en dessus des immeubles à protéger des "pointes" métalliques dressées ver le ciel et reliées à une "Prise de Terre". Ce dispositif est sensé capturer les charges électriques issues des éclairs d'orages, puis évacuer ces charges dans le sol. Ce dispositif protège les bâtiments des alentours des effets d'un impact direct sur leurs structures, mais n'empêche pas les effets indirects de la foudre (champs magnétiques créés par les décharges) sur les équipements électroniques.



Dispositif paratonnerre

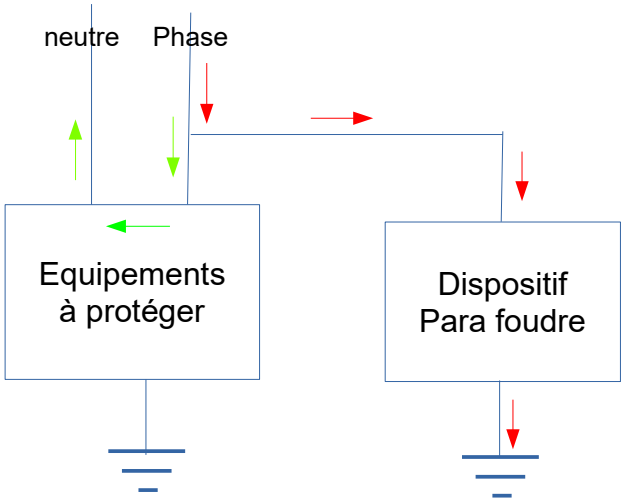
UTILISATION DE DISPOSITIFS PARAFOUDRES:

Ces dispositifs protègent les installations électriques (circuits de puissances, circuits basse tension, circuits de télécommunication) des surtensions provoquées par la foudre. Le principe général des parafoudres est de dévier les surtensions surgissant dans les circuits à protéger vers la terre.

Pour ce faire, on utilise des dispositifs qui ont la propriété de présenter une très forte impédance pour les courants dont la tension est faible et une très faible impédance pour les tensions très fortes, telles que celles engendrées par la foudre ou l'utilisation d'équipements électriques de forte puissance. Les composants utilisés peuvent être des ÉCLATEURS, des VARISTANCES, des DIODES TRANSIL, etc.

Lorsqu'un tel dispositif est branché en dérivation entre un circuit supportant les équipements à protéger et la terre, son comportement peut se décrire comme suit:

- Si la tension dans le circuit à protéger est faible (c'est à dire si elle correspond à un fonctionnement normal de l'équipement), il va opposer une très forte impédance. De ce fait, la partie du courant qu'il va dériver vers la terre sera très faible par rapport au courant circulant dans le circuit à protéger (flèches verte du schéma);
- En revanche, si la tension dans le circuit à protéger devient très forte, son impédance va devenir très faible. De ce fait, il va dériver la quasi-totalité du courant vers la terre, protégeant ainsi les équipements placés dans le circuit à protéger (flèches rouges du schéma).

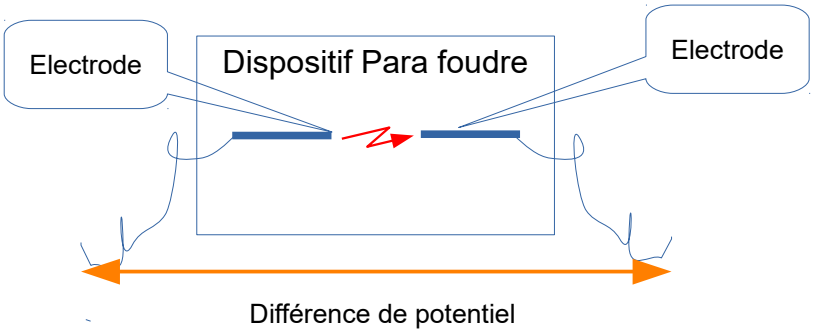


- **Flèches vertes** : trajet des courants de tension normale : le courant ne peut emprunter la dérivation du dispositif para foudre car l'impédance de celui-ci est très grande pour ces tensions ;
- **Flèches rouge:** trajet des courants de tension excessives : le courant emprunte la dérivation du dispositif para foudre car l'impédance de celui-ci est très faible pour ces tensions ;

Schéma de principe d'un dispositif para foudre

Exemple de composant utilisés par les parafoudres: les ÉCLATEURS sont constitués de deux électrodes placées face à face, sans se toucher. Lorsqu'une tension faible est appliquée à ce dispositif, le courant électrique ne peut le traverser. En revanche, si sa tension est suffisamment forte, un arc électrique se forme entre les deux électrodes et le dispositif devient conducteur. En effet, l'arc électrique ionise l'air situé entre les électrodes. Ce volume d'air passe donc d'un état isolant à un état très conducteur. Cet état se maintient tant que la surtension se maintien. Lorsque la surtension disparaît, l'air revient à son état initial (isolant).

- Si la DDP entre les électrodes n'est pas suffisante, le courant électrique ne peut pas traverser l'espace entre les électrodes : l'impédence du dispositif est pratiquement infinie.
- Si la DDP entre les électrodes est suffisante pour qu'un arc électrique se produise entre les électrodes, le dispositif "amorce" et son impédance devient quasi nulle : le courant peut traverser le dispositif.



Principe d'un dispositif "éclateur"

Utilisation de cages de Faraday:

DESCRIPTION SOMMAIRE: Les CAGES DE FARADAY sont des enceintes dont les parois sont conductrices du courant électrique. Leur propriété caractéristique est de protéger les équipements qu'elles contiennent contre les perturbations électromagnétiques et électrostatiques extérieures à l'enceinte.

Ce type d'enceinte peut être un simple boîtier contenant les équipements à protéger ou un local entier. Les parois peuvent être constituées de plaques de métal (cuivre), de treillis métalliques, de tissus métallisés collés sur les parois intérieures ou même des peintures conductrices que l'on appose à l'intérieur des boîtiers. Pour permettre la protection contre les perturbations ÉLECTROSTATIQUES, les parois doivent être reliées à la terre.

Le caractère protecteur des cages de faraday vis à vis des perturbations ÉLECTROSTATIQUES est dû au fait que leurs parois soit conductrices du courant électrique. De ce fait, les charges déposées sur ces parois par les champs électrostatiques ont tendance à être captées par elles et à se répartir uniformément sur toute leur surface, annulant ainsi les effets du champ électrique à l'intérieur de l'enceinte. La liaison à la terre a pour fonction d'évacuer le trop plein de charge, évitant ainsi l'accumulation d'un trop fort potentiel électrique.

UTILISATION: Placer dans les cages de Faraday les équipements sensibles permet de protéger ceux-ci des perturbations électrostatiques d'origine externe, à condition de s'assurer:

- Que les différentes ouvertures qui existent obligatoirement dans l'enceinte ne constituent pas des brèches. Différents équipements permettent de réduire la perméabilité des portes, fenêtres et bouches de ventilation (nids d'abeilles, coupe ondes, etc.). Cependant, ces dispositifs ont une efficacité limitée. C'est pour cela que certaines enceintes sont dépourvues d'ouvertures et

sont surveillées par des caméras intérieures. Les conducteurs entrant et sortants de la cage doivent être munis de filtres radioélectriques.

- Que la liaison à la terre est de bonne qualité (pour cela, il faudra recourir aux vérifications décrites plus haut, au paragraphe IV.5.23.6.ACTIONS CONTRE LES PROBLÈMES DE CONTACTS, MISE À LA MASSE ET À LA TERRE).

III.5.2.4.5.3.Actions contre les perturbations électrostatiques internes:

Les perturbations électrostatiques internes sont favorisées par la conjonction des causes suivantes:

- Une atmosphère très sèche;
- L'existence d'une différence de potentiel importante entre deux équipements;
- Une distance entre des composants internes assez réduite pour permettre l'amorçage d'un arc électrique dans ces conditions (La distance maximale d'amorçage croît avec la différence de potentiel).

La protection contre ces perturbations passe donc par les actions suivantes:

- Vérifier le degrés hygrométrique des locaux et, en cas de défaillance constatée (hygrométrie inférieure à 35%), agir sur la climatisation (si elle existe) ou sur la ventilation des locaux pour le faire revenir dans une plage normale (idéalement, entre 40% et 60%);
- L'existence d'une D.D.P importante entre deux équipement peut révéler un défaut dans la mise à la masse de composants ou de l'équipotentialité entre équipements (l'équipotentialité entre les équipements d'un S.I. est réalisée en connectant entre elles les masses de ces équipements). Il est donc important de s'assurer que ces connexions ont bien été réalisées **lors de l'installation** ou **des évolutions** d'un S.I. et qu'elles continuent d'être efficientes;
- Normalement, les études de conception des équipements prennent en compte le risque d'amorçage entre composants dans des conditions normales d'utilisation. Cependant, ce risque peut être augmenté par l'encrassement des composants (formation de ponts conducteurs). La mesure de prévention est de s'assurer de la pureté de l'air (absence de poussières, de goudrons de combustion, etc.).

III.5.2.4.6.ACTIONS CONTRE LES PERTURBATIONS ÉLECTROMAGNÉTIQUES:

III.5.2.4.6.1.Rappels sur les causes de ces perturbations:

Comme dans le cas des perturbations électrostatiques, les causes peuvent être EXTERNES au S.I ou INTERNES à celui-ci:

Les perturbations électromagnétiques d'origine externe peuvent être provoquées par les décharges électriques atmosphériques qui se produisent à l'occasion des orages. Ces décharges, produisent le déplacement de charges électriques importante qui, à leur tour, engendrent des CHAMPS MAGNÉTIQUES VARIABLES puissants, eux mêmes créant dans les conducteurs des alentours des courants induits brefs mais intenses. Certains équipements externes peuvent également produire de telles perturbations à condition d'être dans l'environnement immédiat du S.I (par exemple: les feux tricolores, les portails automatiques, les moteurs électriques de forte puissance, etc.).

Les perturbations d'origine interne sont provoquées par les rayonnement électromagnétiques engendrés par certains composants ou certains conducteurs internes à certains équipements du S.I, ou par les liaisons entre ces équipements (lignes de transmission de données, réseaux internes, etc.).

III.5.2.4.6.2.Actions contre les perturbations magnétiques d'origine externes:

Utilisation de cages de faraday:

Les cages de Faraday, abordées dans le cadre de la protection contre les perturbations électrostatiques, sont également efficaces contre les perturbations électromagnétiques externes. Cependant, la protection qu'elles offrent dépend en partie de leur conception et de la fréquence des perturbations en question.

Si les enceintes métalliques entièrement fermées (en aluminium ou en feuilles de cuivre) sont efficaces quelle que soit la fréquence, les treillis métalliques ne protègent que contre les fréquences dont la longueur d'onde est supérieure à la taille des mailles.

il est également très difficile de protéger entièrement les ouverture pratiquées dans les enceintes (portes, fenêtres, bouches de climatisation), bien qu'il existe des dispositifs qui diminuent sensiblement les perturbations dues à ces ouvertures (parfois, jusqu'à 80%). Il est aussi primordial de protéger les orifices des conducteurs traversant l'enceinte par des dispositifs adéquats.

Blindage des équipements et des composants:

- Les boîtiers métalliques des équipements électroniques tels que les unités centrales de PC, les routeurs, les unités de disques, etc.) constituent des enceintes de Faraday qui les protègent des perturbations extérieures et qui bloquent les rayonnements de leurs composants.
- En ce qui concerne les équipements dotés de boîtiers non métalliques, la surface intérieure de ces boîtiers est très souvent revêtue d'une peinture conductrice qui atténue les rayonnements d'origine externe.
- Enfin, il est recommandé pour les liaisons internes au S.I. (réseaux internes, câbles de transports de données, etc.), d'utiliser des conducteurs électriques blindés à paires torsadées, reliés à la terre, ou de la fibre optiques), et de veiller à la bonne qualité des terres et de la mise à la terre des blindages.

III.5.2.4.6.3.Actions contre les perturbations magnétiques d'origine interne:

- A l'intérieur des équipements, les composants susceptibles de rayonner des ondes électromagnétique sont enfermés dans des boîtiers métalliques mis à la terre. Ces dispositifs les empêchent de perturber les autres composants.
- Le blindage des câbles de transport de données (ou l'utilisation de fibre optique) empêche les liaisons de données de perturber les autres composants des équipements.
- Cependant, ces protections ne sont efficaces que si ces boîtiers ou blindages sont correctement reliés à une prise de terre et si celle-ci est de bonne qualité. Il est donc, là aussi, très important de s'assurer de la qualité des dispositifs de mise à la terre.

III.5.2.4.7.ACTIONS CONTRE LES AGRESSIONS MÉCANIQUES:

III.5.2.4.7.1.Rappels sur les causes de ces agressions:

Celles-ci sont causées par les chocs et les vibrations qui sont transmis aux équipements par leurs structures d'accueil (plan de travail, rack). L'origine de ces chocs et vibrations peut être externes aux locaux (circulation de véhicules, activités industrielles dans l'environnement) ou interne (activités humaines se déroulant dans les locaux).

III.5.2.4.7.2.Actions contre les agressions mécaniques:

En ce qui concerne les vibrations, il convient d'éviter de placer les locaux en bordure de routes fréquentées ou de voies ferrées. Sinon, monter les appareil sensibles aux chocs et vibrations sur des

supports amortisseurs. L'idéal, pour les équipements les plus sensibles est de les monter dans des racks industriel en utilisant des joints amortisseurs.

En ce qui concerne les chocs, l'idéal est de placer les équipements sensibles dans des locaux dédiés dont les accès sont restreints et réglementés. A défaut, éviter de poser les équipements sur des supports situés trop bas.

III.5.2.5.PRÉVOIR DES MÉCANISMES DE REDONDANCE OU DES MODES DÉGRADÉS:

Il est possible également d'améliorer la fiabilité globale de ce S.I en utilisant diverses stratégies de conception parmi lesquelles nous pouvons citer:

- L'intégration au système de capacités de traitement REDONDANTES susceptible de pallier le dysfonctionnement d'une partie des composants;
- L'utilisation de dispositifs qui permettent de prolonger le fonctionnement en MODE DÉGRADÉ.

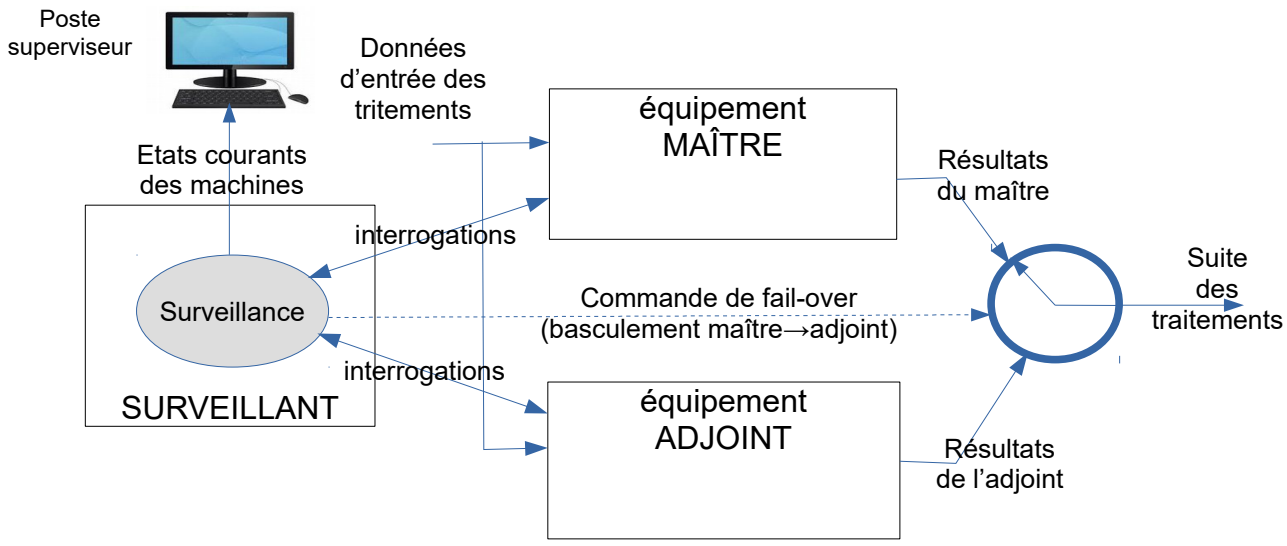
III.5.2.5.1.MÉCANISMES DE REDONDANCE:

La première stratégie consiste à intégrer dans le S.I. deux (ou plusieurs) équipements matériels identiques supportant les mêmes fonctionnalités externes. Ces équipements redondants reçoivent les mêmes données et commandes en entrée et effectuent les mêmes traitements sur ces données, mais un seul (le MAÎTRE) transmet les données et commandes qu'il a élaborées au reste du S.I. Les autres équipements redondants (appelés ADJOINTS), se tiennent prêts à suppléer le MAÎTRE en cas de défaillance de celui-ci. Le basculement du MAÎTRE vers un ADJOINT peut s'effectuer:

- Soit sur détection automatique de la défaillance par un système de surveillance dédié (on parle alors de REDONDANCE A CHAUD);
- Soit par une commande d'un opérateur (REDONDANCE A FROID).

Le choix entre ces deux modes dépend évidemment de la criticité de la fonctionnalité supportée.

Schéma d'une redondance à chaud



La redondance permet de maintenir la continuité du service avec des performances identiques à celles qui étaient fournies en mode nominal. Il est donc possible d'entreprendre les travaux de dépannage des composants en cause et de revenir en mode nominal sans aucune perturbation pour les utilisateurs si la redondance est assurée "à chaud" ou avec une perturbation minime si la redondance est assurée "à froid" (temps de réaction du superviseur).

REMARQUES:

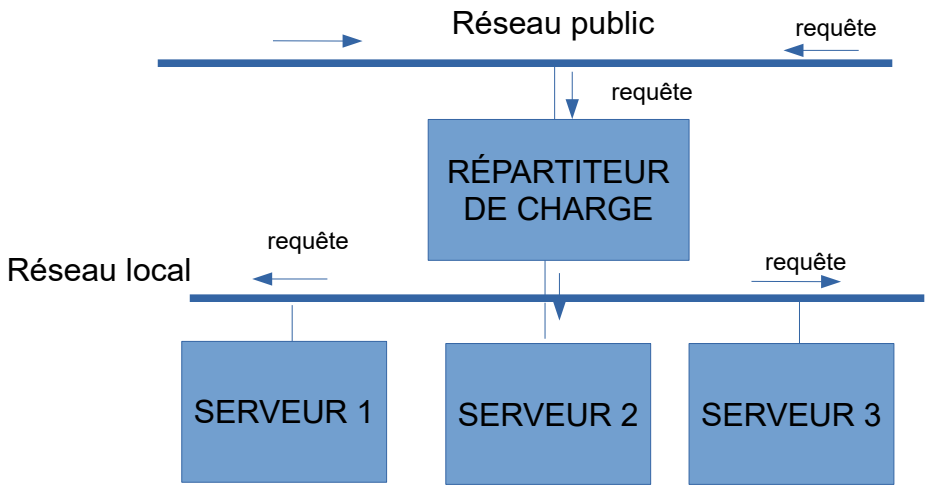
- *Pour une redondance à froid, la commande de fail-over est émise par un opérateur humain à partir du poste de supervision.*

- *Ces notions sont traitées dans l'ouvrage: Conception des logiciels. Tome II – Démarches de conception (site atlantic-83.fr, rubrique documentation).*

III.5.2.5.2.MODES DÉGRADÉS:

Un MODE DÉGRADÉ est un mode de fonctionnement qui permet, en cas de dysfonctionnement d'un des composants d'un ensemble matériel, de continuer à fournir le SERVICE produit par cet ensemble, moyennant une détérioration des PERFORMANCES associées à ce service (augmentation du temps de réponse, diminution de la précision des calculs, etc.).

EXEMPLE: supposons que pour traiter sa fonctionnalité "banque en ligne", un établissement bancaire dispose d'un CLUSTER de 3 serveurs et que les requêtes des clients en ligne soient réparties également sur ces 3 serveurs par un RÉPARTITEUR DE CHARGE placé en frontal:



En mode NOMINAL, les requêtes des utilisateurs vont être réparties sur les trois serveurs de façon à optimiser leurs charges respectives. Lorsque l'un des serveurs tombe en panne, le service n'est pas interrompu car le répartiteur de charges va détecter la panne et continuer de répartir les requêtes entrantes sur les deux autres serveurs. En revanche, ces deux serveurs ayant à traiter plus de requêtes, leur temps de réponse s'allongera: ce mode de fonctionnement est donc DÉGRADÉ par rapport au mode nominal.

III.5.2.5.3.REMARQUE SUR LES REDONDANCES ET MODES DÉGRADES:

Le fait de prévoir des dispositifs de redondance ou de modes dégradés ne doit pas être considérée comme réservée aux S.I. très complexes et offrant des fonctionnalités "critiques". En effet, un particulier, une famille ou un micro-entrepreneur gèrent très souvent en ligne leurs opérations bancaires en utilisant un PC relié au WEB par un routeur internet. Si ces utilisateurs n'ont pas prévu de redondance ou de mode dégradé, une panne du routeur web ou du PC peut les priver de cette fonction essentielle à un moment où cette interruption est très gênante. Or, un mode dégradé très simple et relativement rapide à mettre en œuvre consiste à intégrer sur un smartphone l'application de gestion correspondant à la banque gérant les comptes, même si en pratique, on ne l'utilise pas.

Bien sûr, presque tout le monde dispose d'un smartphone, mais les personnes qui l'utilisent pour gérer leurs comptes bancaires sont beaucoup moins nombreuses. Si, au moment de la panne de PC ou de

routeur, l'utilisateur est obligé de télécharger l'application bancaire "ad hoc" et de la paramétrer avant de l'utiliser, l'interruption de service durera au moins quelques dizaines de minutes alors que si le recours au smartphone comme mode dégradé A ÉTÉ PRÉVU et l'application INSTALLÉE À L'AVANCE (et si l'on a appris à s'en servir) cette interruption se réduira à une ou deux minutes.

III.5.2.6.METTRE EN PLACE UNE ORGANISATION DU M.C.O EFFICACE:

III.5.2.6.1.INTRODUCTION:

Quelle que soient la taille d'un S.I. et son degrés de criticité, il est toujours bon d'envisager les conséquences d'une défaillance totale ou partielle de celui-ci et d'étudier les mesures permettant de remédier à ses conséquences afin de déterminer comment ces mesures peuvent être mises en application.

L'activité de Maintien en Condition Opérationnelle (M.C.O), englobe à la fois les activités de MAINTENANCE (entretient courant, révisions, dépannage) et les actions de MISE À NIVEAU OPÉRATIONNELLE (actions d'adaptation nécessitées par l'évolution de l'environnement ou des normes techniques ou réglementaires ou encore par l'obsolescence des solutions techniques employées).

EXEMPLE: *dans le domaine des transmissions de données le remplacement de la boucle de cuivre par la fibre optique par le fournisseur d'accès peut impliquer des évolutions pour certains équipements d'un S.I: ces évolutions sont indispensables pour maintenir ce S.I. en condition opérationnelle.*

III.5.2.6.2.EXPOSÉ DE LA PROBLÉMATIQUE:

Pour dimensionner et organiser les équipes de Maintien en Condition Opérationnelle d'un S.I, quelle que soit sa taille, il convient d'abord de répondre à la question préalable suivante:

Compte-tenu:

- *Du nombre et du degrés de qualification des personnels qu'il est (ou sera) possible d'employer **en interne** à l'activité de M.C.O, éventuellement après une **courte** formation d'adaptation (quelques jours),*
- *Des moyens matériels d'analyse et de dépannage qu'il sera possible de fournir à ces personnels en interne (outils matériels, logiciels de test, etc.),*
- *De la rapidité d'intervention et de résolution des problèmes imposée par les missions du S.I,*
- *Des moyens financiers qu'il est (ou sera) possible d'allouer à l'activité du M.C.O,*

→ *Quelles actions de M.C.O pourront être réalisées en interne?*

→ *Quelles actions de M.C.O nécessiteront l'intervention d'opérateurs extérieurs (sous-traitants)?*

Pour mener à terme cette première étude, il nous semble nécessaire de bien connaître la classification des différentes actions de maintenance et les degrés de qualifications des personnels amenés à les exécuter. La norme AFNOR X 60-010 classe les interventions de maintenance en cinq "NIVEAUX", en fonction des capacités techniques exigées pour les personnels concernés. Le tableau ci-dessous résume ce classement:

REMARQUE: *par rapport au texte de la norme, les textes contenus dans ce tableau ont été remaniés pour les rendre plus compréhensibles à des non initiés.*

NIVEAU	TYPE D'INTERVENTION	LIEU D'INTERVENTION HABITUEL	TYPE DE PERSONNEL NIVEAU DE QUALIFICATION MINIMAL
I	Interventions ne posant pas de problème de sécurité (ni démontage ni ouverture du capot) et ne nécessitant pas la connaissance du fonctionnement interne des matériels: • Réglages et paramétrages simples; • Changement de consommable.	Sur place	Exploitants habituels du matériel. La mise à disposition d'un recueil de procédures d'utilisation est conseillée.
II	Opérations peu complexes de maintenance préventive ou corrective mais pouvant présenter des problèmes de sécurité (interventions "capot ouvert", par exemple): • Réglages et paramétrages; • Réparation par ÉCHANGES STANDARDS (limitée à des "composants modulaires").	Sur place	Technicien de maintenance informatique habilité. (habilitation par l'encadrement, éventuellement après une courte formation d'adaptation).
III	Actions complexes nécessitant une bonne connaissance des matériels: • Identification et diagnostic de pannes et réparation par ÉCHANGE STANDARD; • Réglage d'appareils de mesure.	Sur place ou dans un atelier de maintenance.	Technicien de maintenance Informatique spécialisé, formé aux matériels.
IV	Actions complexes nécessitant une connaissance approfondie des matériels et du domaine technique: • Travaux importants de maintenance corrective ou préventive; • Réglage et étalonnage d'appareils de mesure complexes.	Atelier spécialisé avec outillage, bancs de mesure et documentation	Équipe de maintenance informatique avec encadrement technique spécialisé.
V	• Rénovation; • Reconstruction.	constructeur ou reconstructeur. Atelier spécialisé avec outillage	Personnels qualifié, proches de la fabrication

III.5.2.6.2.1.Commentaires généraux sur ce tableau:

- La notion d'ÉCHANGE STANDARD désigne une méthode de dépannage qui consiste à effectuer "à priori" le remplacement du composant que l'on suspecte d'être défaillant par un composant identique en état de marche (neuf ou reconditionné), AVANT toute tentative de dépannage de ce composant. Par exemple, un mécanicien auto qui suspecte une panne de démarreur va effectuer le remplacement de ce démarreur sans chercher dans un premier temps à le dépanner. Cette méthode a l'avantage de permettre un dépannage très rapide si l'on dispose immédiatement d'un composant de remplacement (c'est à dire si l'on dispose d'un LOT DE RECHANGE);

- L'appellation "composant modulaire" employée ici pour le niveau II désigne un composant "compact", encapsulant une fonction bien définie, que l'on peut facilement extraire de l'architecture globale ou replacer dans cette architecture uniquement grâce des opérations de débranchement-rebranchement de câbles, de dévissage-revissage ou de déclipsage-reclipsage (sans qu'il soit nécessaire de dessouder ou de cisailler des connexions).

III.5.2.6.2.2.Commentaires sur le niveau I:

Le premier niveau d'intervention ne nécessite aucune connaissance de la structure interne des équipements. En revanche, il nécessite une bonne connaissance de leurs fonctionnalités et de leur utilisation. De ce fait, les exploitants habituels de ces équipements sont en général capables d'assurer les interventions de niveau I, aidés le cas échéant par un recueil d'instructions d'utilisation ou par un technicien informatique les guidant à à distance (Help Desk).

III.5.2.6.2.3.Commentaires sur le niveau II:

Le deuxième niveau d'intervention demande des personnels techniciens et titulaires d'une habilitation pour effectuer les actions concernées (après une courte formation en interne, par exemple). En effet:

- D'une part, ces actions peuvent nécessiter d'opérer "capot ouvert", avec les risques inhérents à ce type d'intervention (courts circuits, électrocution, détérioration mécanique). Elles exigent donc une connaissance au moins générale de l'architecture et du fonctionnement interne des matériels;
- D'autre part, ces actions, effectuées d'une manière inadéquate, peuvent aggraver les problèmes au lieu de les résoudre. Par exemple, effectuer l'échange standard d'un module sans être sûr que le défaut constaté ne provient pas de l'environnement de ce module (ex: défaut de l'alimentation électrique ou d'une broche du socket) peut amener à endommager ou même détruire le module de rechange.

III.5.2.6.2.4.Commentaires sur le niveau III

Le troisième niveau d'intervention exige des personnels techniques spécialisés et ayant une connaissance approfondie des matériels (architecture et fonctionnement), de façon à pouvoir analyser les dysfonctionnements et en déduire des mesures correctives. Ces personnels doivent également maîtriser le paramétrage des matériels de façon à pouvoir les régler de manière optimale.

III.5.2.6.2.5.Commentaires sur les niveaux IV et V:

Les niveaux 4 et 5 concernent des actions complexes qui exigent des personnels qualifiés sur les matériels concernés ainsi que des moyens d'intervention très conséquents (ateliers spécialisés, outils d'investigation et de diagnostics, bancs d'essai, etc.). Il est difficile de maintenir à pied d'œuvre ces moyens dans une entreprise non spécialisée dans le M.C.O. De ce fait, ces actions sont le plus souvent sous-traitées.

III.5.2.6.2.6.Prise en compte de la politique de l'entreprise en matière de ressources humaines:

La décision d'assurer des tâches relevant du M.C.O en interne doit tenir compte de la politique générale de l'entreprise en matière de ressources humaines.

En effet, une entreprise propriétaire d'un S.I. peux ne pas souhaiter employer en interne trop de personnels techniques si son activité principale est éloignée de la technique (activités commerciales, administratives ou financières, par exemple). De ce fait, elle peut parfaitement préférer favoriser la

sous-traitance du M.C.O, quitte à payer plus cher, car elle ne désire pas supporter les contraintes liées à la gestion et au maintien à niveau de personnels techniques (salaires plus élevés que la moyenne de l'entreprise, besoins élevés en matière de formation, difficulté à évaluer l'évolution du besoin, etc).

III.5.2.7.PRÉVOIR LES MOYENS HUMAINS ET MATÉRIELS DE L'ACTIVITÉ DE M.C.O:

III.5.2.7.1.Démarche générale:

La démarche générale peut être menée comme suit:

- Nous disposons d'une part, du recueil des besoins effectué lors de la création du système, enrichi des nouvelles exigences exprimées par les utilisateurs lors de ses évolutions successives. Ces sources vont nous permettre de déterminer la rapidité d'intervention et de résolution des dysfonctionnements nécessaire pour remplir les différentes missions dévolues au S.I. dans la version à prendre en compte;
- D'autre part, conformément à ce qui a été recommandé précédemment, nous avons élaboré l'inventaire des moyens humains et matériels dont nous disposons ou dont nous pensons pouvoir disposer en interne pour assurer le M.C.O du système;
- Enfin, nous sommes informés de la politique de l'entreprise concernant l'embauche et la gestion d'effectifs de personnels techniques dans le domaine de l'informatique.

Remarquons que pour assurer totalement en interne les tâches relevant d'un niveau d'intervention, il est non seulement nécessaire de posséder les compétences humaines et les ressources et outils correspondant à ce niveau, mais aussi de les **posséder en quantité suffisante** pour pouvoir intervenir dans les délais exigés: en particulier, les moyens humains doivent être dimensionnés pour tenir compte des absence pour maladie, congés et formations et des périodes non ouvrables pendant lesquelles le S.I doit rester opérationnel.

En nous référant au tableau et aux études mentionnées ci-dessus, nous devons être capables de déterminer dans quels niveaux d'intervention de M.C.O nous pourrions être capables d'intervenir avec nos moyens propres, et par là même, de déterminer les besoins en matière de sous-traitance du M.C.O.

III.5.2.7.2.Cas de la maintenance de niveau I:

L'accès à l'intérieur du boîtier d'un équipement électrique ou électronique comporte des risques (chocs électriques, dommages causés à l'équipement, etc.). De ce fait, dans un cadre professionnel, une telle action ne doit être confiée qu'à des personnels techniques HABILITÉES pour effectuer de telles opérations.

C'est sur la base de cette constatation que le tableau ci-dessus spécifie que la maintenance de niveau I ne concerne que des interventions simples **ne nécessitant pas le démontage ni l'ouverture de l'équipement**. Sous réserve de cette restriction, les actions de maintenance de niveau I peuvent le plus souvent être assurée par les exploitants des équipements eux mêmes.

Par exemple:

- *Les utilisateurs d'une imprimante à jet d'encre sont en général capables de changer eux-mêmes une cartouche de couleurs (moyennant peut-être une petite démonstration de quelques minutes ou la fourniture d'une notice d'utilisation);*
- *Les personnes utilisant un ordinateur à des fins de bureautique sont en général tout à fait capables de lancer un logiciel de prise en main à distance afin de bénéficier de l'assistance d'une personne externe ou interne à l'entreprise;*
- *De même, ces personnes sont en général capables de "rebooter" leur matériel en cas de dysfonctionnement ou de vérifier les branchements d'alimentation électriques ou les branchements de liaisons de données externes.*

Très souvent, la maintenance de niveau I est donc confiée entièrement ou partiellement aux exploitants des équipements. Cette solution a pour avantages la rapidité d'intervention (ces personnes se trouvent sur place) et l'absence de surcoût (les formations ou démonstrations nécessaires peuvent le plus souvent être réalisées en interne). Cependant, si cette solution est relativement bien acceptée dans les petites entreprises car le personnel y est habitué à une certaine polyvalence, elle se heurte souvent dans des structures plus importantes à des réticences, car les personnels y sont peu habitués à outrepasser leurs fonctions.

A contrario, embaucher au sein de l'entreprise des personnels de maintenance informatique permet de disposer sur le site d'une équipe de M.C.O qui, au fil du temps, pourra acquérir une expertise inégalable des problématiques particulière du S.I. de l'entreprise et de leur résolution. Cependant, nous avons vu que la condition nécessaire à de telles embauches est que cette démarche n'entre pas en contradiction avec la politique de gestion des ressources humaines. Une autre condition est que l'entreprise puisse supporter le coût d'une telle mesure. En effet, la conservation d'une équipe de maintenance informatique interne peut engendrer des charges fixes importantes (salaires et charges sociales, dépenses de formation, dépenses de gestion administrative, etc.).

Il est possible également de recourir à des sous-traitants intervenants sur site. Cependant, cette solution est coûteuse et se heurte le plus souvent aux délais d'intervention: par exemple, lorsqu'une cartouche d'imprimante est vide, il semble peu pratique d'attendre le déplacement d'un sous-traitant pour régler le problème.

Une solution très répandue consiste, moyennant une compensation quelconque, à trouver des personnels volontaires pour effectuer de la maintenance niveau I en plus de leurs tâches habituelles: Par exemple, il est souvent possible dans un groupe "secrétariat", de trouver un personnel volontaire pour assurer la maintenance de niveau I du groupe tout en conservant ses anciennes attributions, moyennant l'obtention d'un avantage particulier (promotion, prime de fonction, etc.). Suivant les besoins, il peut être utile que ces personnels puissent s'appuyer sur une entreprise d'assistance à distance (service de type HELP DESK).

III.5.2.7.3.Cas de la maintenance de niveau II:

Les actions de maintenance au niveau II peuvent exiger l'ouverture ou même le démontage partiel des équipements afin, par exemple, de procéder à l'échange standard d'un composant présentant un caractère MODULAIRE (donc, facile à démonter et remonter sans opération "destructrice" telle que le dé-soudage ou le découpage).

EXEMPLES: *Dans le domaine de l'informatique, nous pouvons citer: l'ÉCHANGE STANDARD d'un disque dur interne, d'un ventilateur ou même (à la limite), le remplacement d'une alimentation à l'intérieur d'une tour de PC.*

Ces opérations exigeant une connaissance générale de l'architecture des équipements informatiques et des précautions à respecter lors d'une intervention "capot ouvert", elles doivent être pratiquées par un technicien de maintenance informatique habilité. De ce fait, il n'existe que deux façons d'assurer la maintenance de niveau II:

- Soit l'embauche en interne de techniciens de maintenance informatique habilités;
- Soit la conclusion d'un CONTRAT D'INFOGÉRANCE avec une entreprise spécialité dans cette activité et pouvant intervenir sur le site.

MAINTENANCE ASSURÉE UNIQUEMENT EN INTERNE:

Les charges fixes importantes induites par la présence en interne de techniciens de maintenance peuvent être mises en balance avec:

- Le coût d'une sous-traitance de maintenance de niveau II (le coût de la sous-traitance augmentant en fonction de la qualification des personnels concernés);
- L'avantage de disposer au sein de l'entreprise de personnels capables d'intervenir immédiatement sur le site (sous réserve que les demandes d'interventions ne soient pas trop nombreuses par rapport à l'effectif) et la possibilité pour ces personnels d'intervenir en soutien des personnels chargés du niveau I.

MAINTENANCE ENTIÈREMENT ASSURÉE PAR INFOGÉRANCE:

Le recours à une société d'INFOGÉRANCE pour traiter l'ensemble des actions de M.C.O de niveau II semble, à première vue, présenter de nombreux avantages, surtout pour une entreprise dont l'activité n'est pas du domaine technique:

- Elle n'implique aucune augmentation concernant le budget de formation;
- Elle permet à l'entreprise de se décharger sur le sous-traitant de l'épineux problème du maintien de la capacité "assistance-dépannage" pendant les périodes d'absence des personnels (vacances, maladies, etc.);

Cependant, le coût de la sous-traitance du M.C.O d'un Système Informatique ne se résume pas au coût mensuel du contrat d'infogérance. En effet:

- La négociation d'un contrat d'infogérance avec un fournisseur nécessite, en même temps qu'une bonne appréciation des besoins présents et futurs de l'entreprise, une connaissance suffisante des problématiques liés aux activités de M.C.O. Si une entreprise grande ou moyenne qui ne dispose pas de ces compétences en interne peut supporter un surcoût ponctuel pour se faire aider dans cette tâche par un consultant, cette solution est la plupart du temps trop onéreuse pour une petit entreprise ou un entrepreneur individuel;

- En général, une société d'infogérance ne s'engage auprès d'un client qu'après avoir AUDITÉ le système informatique de celui-ci. En conclusion de cet audit, la société peut conditionner son acceptation à la MISE À NIVEAU de l'installation. Ces mises à niveau, qui peuvent concerner la sécurité, l'ambiance de fonctionnement, la correction des obsolescences techniques, le stock de pièces détachées, etc, peuvent potentiellement se révéler très coûteuses;

- L'application d'un contrat d'infogérance nécessite une surveillance continue de la part du client afin de s'assurer que les prestations fournies sont bien conformes aux termes du contrat et de résoudre les litiges possibles entre les personnels de l'entreprise d'infogérance et les utilisateurs du S.I. Cette surveillance nécessite d'y affecter, au moins à temps partiel, des personnels en interne: ceci peut impliquer des charges salariales supplémentaires;

- Les contrats d'infogérance prévoient une rémunération fixe (annuelle, mensuelle) qui est principalement calculée en fonction du nombre de postes de travail, du nombre d'heures journalières ou hebdomadaires où l'assistance (sur site ou à distance) doit être disponible, des délais d'intervention sur site, etc.). Cependant, cette rémunération ne couvre pas l'ensemble des prestation de M.C.O nécessaires: par exemple, les interventions nécessitant le retour du matériel en atelier ou l'achat de pièces de rechange peuvent induire des surcoûts importants.

SYNTHÈSE:

D'un point de vue purement organisationnel, le recours à une solution d'infogérance exige moins d'engagement à long terme de la part de l'entreprise que la constitution d'une équipe de maintenance interne. Cependant, la mise en place et le suivi de l'exécution du contrat peuvent ponctuellement

mobiliser une part importante du temps de travail des personnels de l'entreprise chargés de la maîtrise d'ouvrage.

Sur le plan financier, déterminer quelle solution est la plus économique à égalité de prestations ne peut se faire qu'au cas par cas car le résultat dépend en grande partie du type d'activité de l'entreprise et des exigences en matière de continuité du service.

Une solution mixte basée sur une petite équipe de M.C.O locale s'appuyant sur un contrat d'infogérance bien calibré a l'avantage de créer ou de conserver en interne un noyau de compétences qui pourra intervenir à la fois directement sur les dysfonctionnements du S.I. et indirectement sur les questions d'organisation et de suivi du M.C.O.

REMARQUE: Procéder à un échange standard suppose soit que l'on possède en stock le composant ou l'équipement concerné, soit que celui-ci puisse être livré "en urgence". Lorsque, dans le cadre d'une intervention de niveau II, il a été procédé à un échange standard, le composant ou l'équipement en défaut peut:

- Soit pris en charge par le M.C.O interne si celui-ci possède les moyens matériel et humains pour effectuer le dépannage (ce qui implique qu'il peut effectuer une maintenance au niveau III;
- Soit confié à un opérateur capable d'effectuer son reconditionnement (en général, c'est le constructeur ou un sous-traitant de celui-ci).

Une fois reconditionné, le composant est intégré ou réintégré dans le STOCK DE RECHANGES du S.I. Nous voyons apparaître ici l'importance de la gestion d'un stock de rechange pour la réactivité du M.C.O de l'entreprise.

III.5.2.7.4.Cas de la maintenance au niveau III:

Le tableau AFNOR présenté plus haut indique que la maintenance de niveau III doit être pratiquée par des Techniciens Informatique spécialisés **formés aux matériels sur lesquels ils doivent intervenir**. Cette précision indique que, contrairement au niveau II qui n'exige qu'une connaissance de l'architecture générale des équipements informatiques, le technicien intervenant au niveau III doit être capable non seulement d'identifier un composant défaillant, mais aussi de trouver la cause **interne** de son dysfonctionnement (en vue d'une remise en état, par exemple).

Dans le domaine de l'informatique digitale, du fait de la miniaturisation et de l'intégration des composants, il est rare de pouvoir réparer "sur site" un équipement en panne (par exemple, procéder au remplacement d'un composant soudé sur une carte mère d'ordinateur ne peut être effectué correctement que dans un atelier de maintenance dûment équipé).

De ce fait, le dépannage sur site se fait presque toujours par un échange standard du composant en défaut (si celui-ci est suffisamment compact et modulaire pour être extrait et remplacé par simple débranchement-rebranchement ou déclipsage-reclipsage) ou par échanges standard de l'équipement complet si la première manœuvre est impossible. Le composant ou l'équipement en panne peuvent alors:

- Soit être pris en charge par le M.C.O interne s'il possède les moyens matériel et humains pour effectuer le dépannage;
- Soit être confié à un opérateur capable d'effectuer son reconditionnement (en général, c'est le constructeur ou un sous-traitant spécialisé).

Les arguments en faveur ou en défaveur de l'entretien en interne d'une équipe de M.C.O capable d'interventions au niveau III sont de même nature que ceux qui ont été employés pour le niveau II. Une

difficulté supplémentaire induite par la solution locale est la nécessité de posséder et de gérer un STOCK DE RECHANGES suffisant, alors que dans la solution externe, c'est le sous-traitant qui prend en charge cette contrainte.

III.5.2.7.5.Maintenance aux niveaux IV et V:

Les actions de maintenance des niveau IV et V de maintenance informatiques se caractérisent essentiellement par leur complexité qui les apparentent à de vrais projets d'évolutions. Ils concernent surtout:

- Les mises à niveau et rénovations nécessaires pour adapter les S.I. à l'évolution de leurs environnements techniques, réglementaires et opérationnels et éviter les obsolescences (maintenance préventive);
- Les remises en état importantes nécessitées par des événements importants affectant l'aptitude du site à remplir ses missions ou nécessitant des changements profonds (destruction partielle par inondation ou incendies, déplacement du site, etc.).

Tous ces travaux ne peuvent être pris en compte que par des équipes techniques hiérarchisées et qualifiées s'appuyant sur des structures adaptées. Pour que de telles équipes puissent être rentables et conservent leur efficacité dans le temps, il est nécessaire qu'elles supportent une charge de travail importante et régulière, ce que peut d'entreprises sont capables de leur assurer en interne.

De ce fait, exception faite des grandes entreprises disposant de systèmes informatiques importants et comprenant des équipements complexes et peu répandus, la maintenance aux niveaux IV et V est assurées par des entreprises spécialisées qui peuvent rentabiliser le coût de leurs équipes sur un grand nombre de clients.

III.5.2.8.DÉFINIR UNE POLITIQUE DE REMPLACEMENT DES ÉQUIPEMENTS:

III.5.2.8.1.PRINCIPE ET OBJECTIFS VISÉS:

Nous avons vu précédemment que la probabilité de dysfonctionnement d'un équipement informatique qui fonctionne dans des conditions conformes aux préconisations du constructeur croît essentiellement avec la durée d'utilisation de cet équipement depuis sa mise en service (ou sa remise en service après dépannage).

Dans la pratique, même à l'intérieur d'enceintes "ultra sécurisés", il est impossible de protéger entièrement les équipements des agression en provenance de l'environnement ou des utilisateurs. Ces agressions contribuent à augmenter la probabilité de dysfonctionnement en fonction de leur nombre et de leur gravité.

De ce fait, nous pouvons dire que ce que l'on appelle communément le VIEILLISSEMENT ou le DEGRÉS D'USURE d'un matériel donné progresse en fonction de deux facteurs principaux:

- La DURÉE D'UTILISATION des composants depuis leur mise (ou remise) en service;
- L'intensité de leur EXPOSITION AUX AGRESSIONS du milieu (effet cumulatif de ces agressions).

Partant de ces constatations, nous pouvons en déduire qu'une manière d'éviter la survenue de dysfonctionnements dus au vieillissement des matériels est, avec la protection contre les agressions du milieu, de remplacer systématiquement ceux-ci AVANT QUE LA PROBABILITÉ DE DYSFONCTIONNEMENT NE DEVIENNE TROP IMPORTANTE.

Ce remplacement "anticipé" peut être déclenché quand au moins une des deux conditions suivantes ont été atteintes:

- Au bout d'une durée d'utilisation déterminée;
- Lorsqu'un certain degrés de vieillissement est constaté.

Dans les deux cas, cette politique doit permettre de réduite les risques de dysfonctionnement d'un équipement, à condition de pouvoir évaluer avec une précision suffisante sa durée d'utilisation totale ou son degrés de vieillissement à un instant T.

III.5.2.8.2.APPLICATION A UN SYSTÈME INFORMATIQUE:

A l'échelle d'un système Informatique, l'application de ce principe de gestion nécessite de définir chacun des composants matériels qui peuvent faire l'objet d'un tel remplacement.

A priori, pour rendre les opérations de remplacement faciles et peu risquées, il est préférable que ces composants soient compacts, si possible enfermés dans un boîtier qui leur est propre et connectés au reste du S.I. par des "sockets" facilement connectables et déconnectables. En effet, contrairement à un remplacement destiné à pallier au dysfonctionnement d'un composant, le remplacement anticipé concerne des composants en état de marche: si l'opération présente un danger quelconque, il peut sembler illogique et contre productif de prendre ce risque uniquement pour diminuer la probabilité de panne.

De ce fait:

- Le remplacement anticipé ne doit pas concerner des composants "enfouis" dont l'extraction nécessiterait de dessouder et ressouder leurs connexions avec le reste de l'architecture électronique;

- L'état du composant en question doit pouvoir être évalué facilement sans qu'il soit nécessaire de procéder à des opérations de démontage potentiellement dangereuses. L'idéal est que cet état soit observable depuis l'extérieur du composant, par des manipulations "non invasives".

Pour illustrer ce propos, voici, quelques exemples de composants compatibles avec une politique de remplacement anticipé:

- Un équipement complet (U.C d'ordinateur, routeur, connecteur réseau, etc.);
- Un périphérique externe: unité de stockage de données (disque dur externe, N.A.S), imprimante, scanner, etc;
- Un onduleur;
- Des composants internes facilement extractibles, comme des barrettes de R.A.M, des ventilateurs de boîtier ou des disques durs internes peuvent être ajoutés à cette liste.

III.5.2.8.3.DIFFÉRENTES POLITIQUES DE REMPLACEMENT ANTICIPE DE COMPOSANTS:

III.5.2.8.3.1.Remplacer systématiquement les équipements au bout d'une durée d'utilisation déterminée:

Le paramètre le plus représentatif de la durée de vie moyenne d'un équipement est son M.T.T.F (medium Time To Fault). Dans des conditions nominales d'utilisation, le M.T.T.F dépend surtout de la qualité de réalisation de l'équipement. L'accès à la valeur du M.T.T.F (ou du M.T.B.F qui, dans le cas d'un composant d'électronique digitale est très proche du M.T.B.F) est relativement aisé (par la notice produit, le site web du constructeur, etc.). Cependant, cette durée de vie moyenne peut se trouver raccourcie par de mauvaises conditions d'utilisation, sans oublier qu'un important facteur de vieillissement des matériels est le nombre de mises sous tension/mises hors tensions.

Une solution pour réduire le nombre de pannes est donc de procéder au remplacement anticipé d'un composants lorsque sa durée d'utilisation a atteint une certaine fraction de son M.T.T.F. La valeur de cette fraction doit être choisie en fonction des conditions d'utilisation du matériel: elle doit être forte si les conditions d'utilisation sont bonnes, plus faible si ces conditions sont mauvaises. Cette solution a l'avantage d'individualiser les dates de renouvellement des matériels.

La section de l'annexe consacrée au rappel des principes mathématiques régissant la fiabilité des matériels informatiques établit que la probabilité qu'un équipement ait un dysfonctionnement avant que la durée T d'utilisation ne soit atteinte est:

$$F(t) = 1 - e^{[\log(1/2) / \theta] * T}$$

Le tableau ci-dessous utilise cette formule pour calculer quelques exemples de probabilité de panne en fonction de la durée d'utilisation atteinte:

Durée d'utilisation (T) du composant depuis sa mis en service	Calcul de la probabilité de panne avant T	Probabilité de panne avant que T ne soit atteint:
T = MTTF de l'équipement	$F(T) = 1-e^{(\log(1/2)/MTTF)*MTTF} = 1-0,5 = 0,5$	50,0%
T = MTTF/2	$F(T) = 1-e^{(\log(1/2)/MTTF)*MTTF/2} = 1-0,707 = 0,293$	29,3%

T = MTTF/3	$F(T) = 1-e^{(\log(1/2)/MTTF)*MTTF/5} = 1-0,7=0,206$	20,6%
T = MTTF/10	$F(T) = 1-e^{(\log(1/2)/MTTF)*MTTF/10} = 1-0,961=0,039$	3,9%

De ce tableau, nous pouvons déduire:

- Que si l'on remplace les matériels informatiques dès que leur M.T.T.F a été atteint, on réduit à 50 % la probabilité de survenue d'une panne pendant leur utilisation;
- Que cette probabilité tombe autour de 29% si le remplacement est effectué quand la moitie du M.T.T.R a été atteinte;
- etc.

NOTA: *Ces valeurs sont évidemment valides que pour des conditions d'utilisation conformes aux spécifications des constructeurs. Elles peuvent être considérablement majorées si ces conditions ne sont pas respectées.*

Cependant, pour appliquer cette règle, il est nécessaire d'évaluer également la date de mise en service du composant et sa durée d'utilisation réelle à un instant donné.

- La DATE DE MISE EN SERVICE peut être déterminée approximativement:
  - à partir de la date d'achat du composant ou de l'équipement auquel ce composant appartient. Pour cela, on peut se référer à divers documents, dont la facture d'achat, les documents de réception, etc.
  - A partir de la date de retour de reconditionnement pour les équipement ayant subi ce type de traitement.
  - REMARQUE: Dans le cas des unités de traitement informatiques (P.C, stations de travail, etc.), la date de mise en service peut être évaluée à partir de la date du B.I.O.S qui est accessible dans les données S.M.A.R.T de l'équipement. Pour un équipement WINDOWS on dispose pour cela des commandes msinfo32 (sous O.S Windows) ou smartctl (sous Linux), mais il existe bien d'autres outils;
- En ce qui concerne la Durée d'Utilisation Réelle (D.U.R) à un instant donné, celle-ci peut être approchée en calculant la Durée Écoulée depuis la Mise en Service (D.E.M.S) et en minorant celle-ci en fonction de l'utilisation journalière réelle de l'équipement. Par exemple, lorsqu'on estime qu'un équipement est (en moyenne) en service 12 heures par jour et 5 jours par semaine, sa durée d'utilisation réelle sera estimée à: **D.U.R = D.E.M.S * (12*5) / (24*7)**;

REMARQUE: *cette politique est évidemment génératrice de surcoûts, car elle aboutit à retirer du service des équipements en état de marche. De ce fait:*

- *Il est inutile de l'appliquer à des équipements pour lesquels une interruption courte du service n'a aucune conséquence grave sur le fonctionnement global du S.I. Seuls les équipement dont la continuité de fonctionnement présente une CRITICITÉ élevée pourront donc être concernés (voir l'annexe A.M.D.E.C pour la définition de la criticité);*
- *Lorsqu'un équipement fait partie d'un cluster d'équipements redondants à chaud, appliquer cette politique n'est justifié que dans le cas où le niveau de fiabilité exigé est exceptionnellement élevé.*

III.5.2.8.3.2.Remplacer les équipements sur détection de la dégradation de certains paramètres:

Certains équipements complexes permettent la mesure et la visualisation des valeurs de certains de leurs paramètres de fonctionnement. C'est le cas, par exemple:

- Des unités de traitement informatiques: PC, stations de travail, etc. pour lesquelles il existe des logiciels de visualisation de l'état interne (voltages, température), comme CPU-ID Hwmonitor ou la visualisation des données S.M.A.R.T, par exemple;
- Des unités de stockage de données (disques durs, clefs USB, etc.) pour lesquelles les systèmes d'exploitation ou certains logiciels (comme Crystal Disk Info pour Windows ou SmartCtl pour Linux) permettent l'inspection de paramètres internes (capacité totale, capacité libre, recherche de secteurs en erreur) et de gestion (défragmentation, etc.).

Dans ce cas, le remplacement d'un équipement peut être déclenché par la détection d'une dégradation conséquente des paramètres de fonctionnement (par exemple, une dérive importante de tensions d'alimentation, ou une température de fonctionnement anormalement élevée).

III.5.2.8.3.3.Remarques:

- *Cette politique nécessite de disposer de personnels affectés au moins partiellement à ces travaux de contrôle, ce qui, potentiellement, augmente les charges fixes d'exploitation;*
- *Remplacer un équipement ne veut pas dire "le jeter au rebut": par exemple, dans le cadre d'une procédure de maintenance, l'équipement défectueux ou remplacé par anticipation peut être reconditionné puis réintégré au stock après un test de fonctionnement;*
- *Un composant est dit RECONDITIONNÉ si, au-delà de la simple correction du dysfonctionnement qui a motivé l'action de l'équipe de M.C.O, celle-ci s'est également attachée à détecter et corriger les points d'usure qu'il présentait (décrassage, remplacement de composants internes ou de connexions présentant des signes de fatigue, etc.). De ce fait,le M.T.T.F d'un composant reconditionné peut être considéré comme très proche de celui d'un composant neuf de même type.*

III.5.2.9.ADAPTER LES ÉQUIPEMENTS AUX ÉVOLUTIONS TECHNIQUES ET RÉGLEMENTAIRES:

Même en l'absence d'exigences nouvelles en provenance des utilisateurs, l'environnement de fonctionnement d'un S.I. est soumis à des évolutions à caractères techniques, commerciales ou réglementaires. Pour que le S.I. continue malgré tout à remplir ses missions et conserve ses performances, il peut alors être nécessaire de lui appliquer des modifications.

Ces évolutions consistent à remplacer les équipements ou les composants frappés d'obsolescence par des équipements ou des composants plus récents capables de remplir les mêmes fonctions mais satisfaisant aux nouvelles exigences (techniques, commerciales, réglementaires). Ce type d'évolution est parfois qualifié de Mise à Hauteur Ordinaire (M.H.O).

EXEMPLES:

- *La disparition progressive de la connexion internet par la "boucle de cuivre" dans la zone occupée par le S.I. peut nécessiter l'adaptation des équipements matériels d'interfaçage réseaux à la fibre optique;*
- *Une évolution des normes de sécurité électriques est susceptible d'entraîner des adaptations pour de nombreux équipements d'un S.I;*
- *En général, les fournisseurs de matériels ne sont tenus d'assurer la maintenance ou de fournir pièces détachées et consommables adaptés que pendant une certaine période (de l'ordre de 10 ans). Passé ce délais, l'équipement ne peut plus être maintenu par manque de pièces de*

rechange ou ne peut plus être exploité par manque de consommable (penser aux cartouches d'imprimantes). On dit qu'il est obsolescent. Il faut alors envisager une solution de rechange.

La Mise à Hauteur Ordinaire (M.H.O) est une condition nécessaire pour assurer le Maintien en Condition Opérationnelle (M.C.O) à moyen et long terme.

III.5.2.10.ADOPTER UNE CONCEPTION ARCHITECTURALE FAVORISANT LE REMPLACEMENT RAPIDE DES ÉQUIPEMENTS EN DÉFAUT:

- Une conception architecturale des matériels qui permet aux personnels de maintenance un accès rapide et aisé aux composants a pour effet de minimiser la durée des dépannages. En particulier, le choix de boîtiers "surdimensionnés" permet souvent un accès rapide et aisé;
- Le choix de composants ayant des capacités "plug and play" minimise également la durée des dépannages et permet parfois d'effectuer des remplacements de composants sans arrêter le fonctionnement des équipements concernés;
- Il est également recommandé de prévoir dès la conception du S.I. des dispositifs permettant de tester et dépanner les matériels extraits de leur implantation opérationnelle (ce type de dispositif est évoqué plus en détails dans l'étude des "actions correctives").

III.5.2.11.CONSTITUER ET BIEN GÉRER LE STOCK DE RECHANGES:

III.5.2.11.1.INTRODUCTION:

Bien que les ACTIONS PRÉVENTIVES puissent réduire la probabilité des dysfonctionnements matériels dans de larges proportions, il est évident qu'elles ne l'annulent pas. Il faut donc prévoir des actions CORRECTIVES capables non seulement de rétablir les SERVICES INTERROMPUS, mais aussi le NIVEAU DE SÉCURITÉ ANTÉRIEUR au dysfonctionnement, et ceci dans des délais compatibles avec les exigences exprimées par les Maîtres d'Ouvrage du S.I.

En particulier, lorsque une redondance à chaud est prévue pour une fonction donnée, la survenue d'un dysfonctionnement concernant un ou plusieurs de ces équipements redondants doit entraîner la réparation ou le remplacement de ceux-ci dans les plus brefs délais, même si, du fait de la redondance à chaud, le fonctionnement du S.I. ne s'en trouve pas affecté. En effet, si le FONCTIONNEMENT n'est pas affecté, la FIABILITÉ se trouve dégradée jusqu'à ce que l'ensemble des équipements redondants soient de nouveau en état.

III.5.2.11.2.COMMENT MAÎTRISER ET MINIMISER LES DÉLAIS DE DÉPANNAGE:

Lorsque, malgré toutes les actions PRÉVENTIVES exposées précédemment, un dysfonctionnement d'origine matérielle survient, l'une des condition nécessaire pour permettre un retour à l'état opérationnel dans des délais maîtrisés et minimisés est de pouvoir procéder à l'échange des composants concernés par des composants de même type issus d'un STOCK DE RECHANGES disponible localement.

***NOTA:** ces composants peuvent être neufs ou "reconditionnés" (c'est à dire, remis à l'état neuf): on parle alors d'ÉCHANGE STANDARD.*

En effet, il est évidemment impossible de garantir la durée de la réparation d'un composant car celle-ci dépend de nombreux paramètres (en particulier ceux qui influent sur la disponibilité des matériels et des opérateurs humains et les délais de livraison). A contrario, la durée de remplacement d'un composant dont on dispose d'une rechange dans le stock est assez prévisible. La condition pour qu'une telle démarche soit possible est de disposer pour ces composants d'un stock de rechanges matérielles suffisant et en état de fonctionner.

Il n'est pas question ici d'exposer les principes généraux de la gestion des stocks. Cependant nous rappellerons deux points essentiels pour la gestion des composants de rechange d'un Système Informatique dont la disponibilité présente un caractère critique:

- Le cycle de vie des composants de rechange;
- L'importance d'effectuer des statistiques de panne.

III.5.2.11.3.ÉLABORATION DU STOCK DE RECHANGE INITIAL:

Lors de la constitution initiale du stock de rechanges d'un S.I, il est possible d'évaluer approximativement le nombre de rechanges dont on doit disposer pour chacun des composants utilisés dans le S.I. en tenant compte:

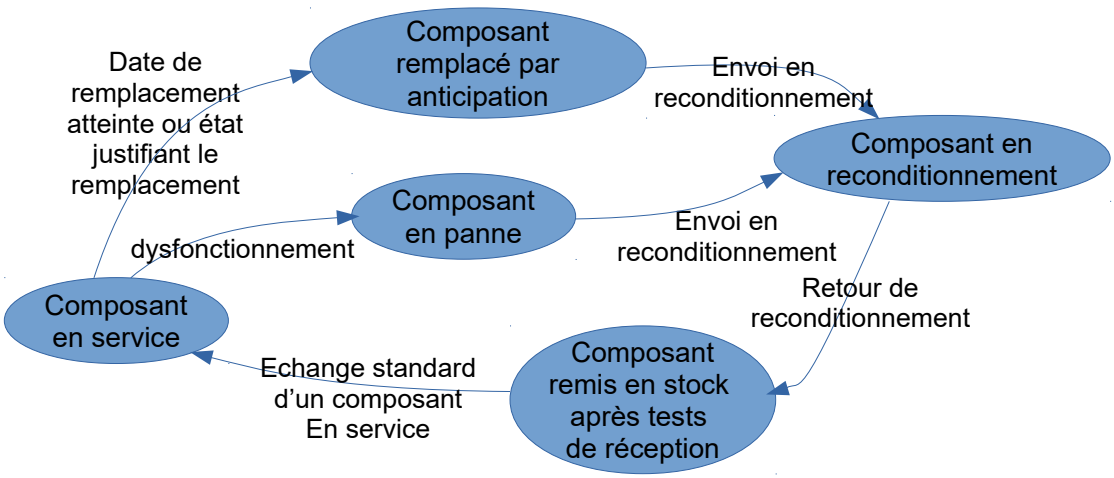
- De la CRITICITÉ des MODES DE DÉFAILLANCE attachés à ce composant (voir l'annexe A.M.D.E.C);
- De la durée de la boucle [envoi en réparation → retour de réparation → remise en stock] pour ce type de composant;
- Des statistiques de dysfonctionnement tenues à jour depuis le début de l'exploitation du S.I.

III.5.2.11.4.CYCLE DE VIE DES COMPOSANTS DE RECHANGE:

Il peut être résumé par la procédure suivante:

- Lorsqu'un composant donné:
  - Subit un dysfonctionnement;
  - Ou atteint la durée d'utilisation prescrite pour un remplacement anticipé;
  - Ou présente des signes de vieillissement justifiant son remplacement;

  Il est remplacé par un composant de rechange prélevé dans le stock;
- Le plus tôt possible, le composant remplacé est envoyé en atelier de M.C.O (en interne ou chez un sous-traitant);
- SI l'atelier juge que le composant est reconditionnable, il est reconditionné puis renvoyé au client;
- SINON, un autre composant, de même type ou compatible, neuf ou reconditionné, est renvoyé au client;
- Le composant retourné est replacé dans le stock après avoir subi les tests de réception adéquats.



IV.SÉCURISATION CONTRE LES DYSFONCTIONNEMENTS MATÉRIELS PASSAGERS:

IV.1.DÉFINITION D'UN DYSFONCTIONNEMENT PASSAGER:

Nous qualifierons de DYSFONCTIONNEMENT PASSAGER un dysfonctionnement qui altère pendant une courte période (de quelques secondes à quelques minutes) le fonctionnement ou les performances d'un équipement, puis disparaît sans qu'il ait été nécessaire d'effectuer une intervention de maintenance sur cet équipement.

IV.2.MÉCANISMES DES DYSFONCTIONNEMENTS PASSAGERS:

IV.2.1.INTRODUCTION:

Le fait que les dysfonctionnements définis au sous-chapitre précédent puissent disparaître sans intervention de maintenance tend à indiquer qu'ils ne sont pas provoqués par des "pannes franches" de composants matériels (dysfonctionnements matériels permanents). Dans ces conditions, les causes les de ces dysfonctionnements appartiennent la plupart du temps aux 4 catégories suivantes:

- ***Causes d'origine logicielles:*** Le dysfonctionnement d'un ou de logiciels en cours d'exécution (application ou système d'exploitation);
- ***Actions malveillantes (***du type "attaques par déni de service, par exemple);
- ***Dégradation temporaire des conditions d'utilisation:*** par exemple, le dépassement temporaire de la température maximale d'utilisation dû à l'exécution d'un logiciel particulièrement gourmand en cycles d'exécution;
- ***Dépassement des capacités de l'infrastructure matérielle:*** saturation temporaire du débit du réseau interne, manque d'espace de stockage en mémoire vive ou sur un support permanent, etc.

IV.2.2.CAUSES D'ORIGINE LOGICIELLES:

IV.2.2.1.DYSFONCTIONNEMENTS PASSAGERS DE LOGICIELS APPLICATIFS:

Cette catégorie de cause peut être due au mauvais fonctionnement d'un des LOGICIELS D'APPLICATION en cours d'exécution: erreur de programmation ("bug" logiciel), mauvaise gestion des accès aux ressources, effets de bord avec un autre logiciel en cours d'exécution, infestation par un virus, etc.

REMARQUES:

- *Les logiciels n'étant, à priori, pas concernés par le vieillissement ou les détériorations dues aux conditions d'utilisation, ce type de défaut concerne surtout les logiciels nouveaux présentant des failles dans leur conception ou les logiciels ayant récemment subi une "montée en version". Cependant, ils peuvent aussi être affectés par les évolutions du système d'exploitation (par exemple, en cas d'absence de compatibilité ascendante);*
- *Les actions malveillantes telles que les infestations par les virus ou les "chevaux de Troie" seront étudiées au chapitre II du tome 2 du présent ouvrage;*

La mise en évidence de ce type de dysfonctionnement est assez facile: il suffit pour cela que l'arrêt de l'exécution du ou des logiciels suspectés rétablisse un fonctionnement normal.

IV.2.2.2.DYSFONCTIONNEMENTS PASSAGERS DU SYSTÈME D'EXPLOITATION:

En revanche, si le dysfonctionnement passager provient du SYSTÈME D'EXPLOITATION, la mise en évidence de cette cause est beaucoup plus difficile. En effet, le système d'exploitation est constamment sollicité par tous les logiciels d'applications tournant sur l'équipement ainsi que par tous les matériels dont il assure le contrôle. Un dysfonctionnement du système d'exploitation peut donc se répercuter sur le fonctionnement de l'ensemble des entités matérielles et logicielles de l'équipement ou sur un sous-ensemble de celles-ci.

Comme le système d'exploitation est composé d'entités logicielles (contrôleurs, pilotes de périphériques, scheduler, etc.), l'apparition d'un dysfonctionnement le concernant est, en l'absence d'actions malveillantes (traitées au tome II), plutôt à mettre en relation avec une "montée en version" récente (défaut de compatibilité ascendante) ou au remplacement récent d'un composant matériel (incompatibilité de ce composant avec l'O.S, driver non adapté, etc.)

IV.2.3.ACTIONS MALVEILLANTES:

Certaines actions malveillantes n'ont pas pour but d'empêcher complètement le fonctionnement des équipements qu'elles ciblent. C'est le cas notamment de toutes celles qui visent à surveiller les activités des utilisateurs, à recueillir leurs données ou à utiliser leurs capacités de traitement à l'insu des propriétaires.

En effet, ce type d'action consiste la plupart du temps:

- Soit à introduire dans les codes sources des système d'exploitation ou des applications, des séquences de code capables d'accéder aux ressources de la machine hôte afin d'utiliser sa capacité de calcul ou de communiquer les données à des systèmes extérieurs au S.I, via le réseau internet;
- Soit à ouvrir clandestinement des interfaces systèmes (ou shells) à distance permettant aux "hacker" d'accéder aux ressources internes du système d'exploitation.

Dans les deux cas, l'intérêt des pirates informatiques auteurs de ces intrusions est que celles-ci restent le plus longtemps possible ignorées des utilisateurs légitimes. De ce fait, les failles introduites (sous formes de virus, "chevaux de Troie", etc.) doivent être conçues pour passer inaperçues des utilisateurs. Ceci implique qu'elles ne doivent provoquer que des perturbation très discrètes du fonctionnement des équipements ciblés. Cependant, elles peuvent provoquer temporairement une baisse des performances de ceux-ci (ralentissement de la vitesse d'exécution des applications, par exemple).

La sécurisation des S.I. contre les actions malveillantes sera étudiée au chapitre III du tome II du présent ouvrage.

IV.2.4.DÉGRADATION TEMPORAIRE DES CONDITIONS D'UTILISATION:

Nous avons vu précédemment que de mauvaises conditions d'utilisation d'un S.I. (température, humidité, poussières, mauvaise qualité de l'alimentation électrique, etc.) peuvent contribuer à la survenue de dysfonctionnements matériels permanents, soit immédiatement, soit par accélération du vieillissement des matériels.

Certains de ces facteurs peuvent également provoquer des dysfonctionnements temporaires des équipements. Par exemple, une hausse passagère de la température des locaux en dessus du maximum tolérable peut affecter temporairement les performances des équipement sans endommager ceux-ci au point de provoquer un dysfonctionnement permanent.

IV.2.5.DÉPASSEMENT DES CAPACITÉS DE L'INFRASTRUCTURE MATÉRIELLE:

Certains dysfonctionnements passagers peuvent avoir pour cause le dépassement temporaire des capacités de l'infrastructure matérielle. De tels dépassements peuvent concerner:

- Le débit maximum des MÉDIAS RÉSEAUX internes du S.I (on parle alors souvent de "congestion"): ce type d'anomalie se traduit surtout par un allongement de la durée apparente d'exécution des requêtes (retard à l'affichage de pages web ou d'images video en streaming, par exemple);
- La puissance de traitement maximale des PROCESSEURS. Ce type de dysfonctionnement peut être causé par l'exécution d'applications très gourmandes en puissance CPU et soumises à des contraintes d'exécution en "temps réel" (les jeux video, par exemple). Ils se traduisent par un allongement des temps de réponse aux sollicitation des utilisateurs ou par une perturbation temporaire de l'affichage des images;
- La capacité maximale de stockage des SUPPORTS DE DONNÉES (disques durs, S.S.I). L'impossibilité pour une application d'accéder à un espace de stockage (pour y déposer des fichiers temporaires, par exemple), peut entraîner le blocage de l'exécution de cette application jusqu'à ce que des zones de stockage soient libérées par d'autres applications;
- La capacité maximale des MÉMOIRES VIVES. Ce type de dysfonctionnement peut empêcher certaines applications de charger la totalité de leur code exécutable en mémoire vive avant d'être exécutées. De ce fait, le système d'exploitation ne charge ce code que par segments, en fonction de l'avancement de l'exécution. Cette pratique, qui impose d'effectuer de nombreux accès aux supports de données, occasionne toujours un fort ralentissement de l'exécution de l'application concernée.

IV.3.PROTECTION CONTRE LES DYSFONCTIONNEMENTS MATÉRIELS PASSAGERS:

IV.3.1.INTRODUCTION:

La protection contre les dysfonctionnements passagers dont l'origine est logicielle sera traitée au chapitre II du tome II tandis que la protection contre les actions malveillante sera traitée au chapitre IV du tome II.

La protection contre la dégradation des conditions d'utilisation a été traitée au chapitre III du présent document.

Reste à étudier la protection contre les dysfonctionnements passagers dus au dépassement des performances de l'infrastructure matérielle qui est traitée dans la suite du sous-chapitre.

IV.3.2.PROTECTION CONTRE LES DÉPASSEMENTS DES CAPACITÉS DE L'INFRASTRUCTURE MATÉRIELLE:

IV.3.2.1.Présentation générale:

Ce type de dysfonctionnement passager est provoqué la plupart du temps par l'incapacité d'un équipement du S.I. de traiter totalement un "pic d'activité" qui lui est imposé à un moment et pendant une période donnés par les sollicitations de son environnement:

- En général, ce type de situation se traduit d'abord par une augmentation du "temps de réponse" de l'équipement;
- Si le pic d'activité s'atténue, il est possible de revenir à un fonctionnement normal. En revanche, s'il persiste assez longtemps, certaines sollicitations peuvent être ignorées;
- A l'extrême, la situation peut évoluer vers un dysfonctionnement logiciel provoqué en général par le dépassement de la capacité d'une mémoire tampon (erreur de type "stack overflow").

NOTA: *remarquons que si ce type de dysfonctionnement se manifeste généralement par une erreur LOGICIELLE (erreur de type "stack overflow"), son origine est bien MATÉRIELLE (incapacité d'un équipement matériel de traiter un pic d'activité).*

Les paragraphes suivants étudient les mécanismes des dysfonctionnements passagers les plus fréquents:

IV.3.2.2.Dépassement du débit maximum des MÉDIAS RÉSEAUX internes du S.I:

IV.3.2.2.1.CAUSES:

Nous avons vu plus haut que la plupart des Systèmes d'Information sont bâtis autour d'une infrastructure réseau interne qui permet la communication entre les divers équipements matériels de ceux-ci:

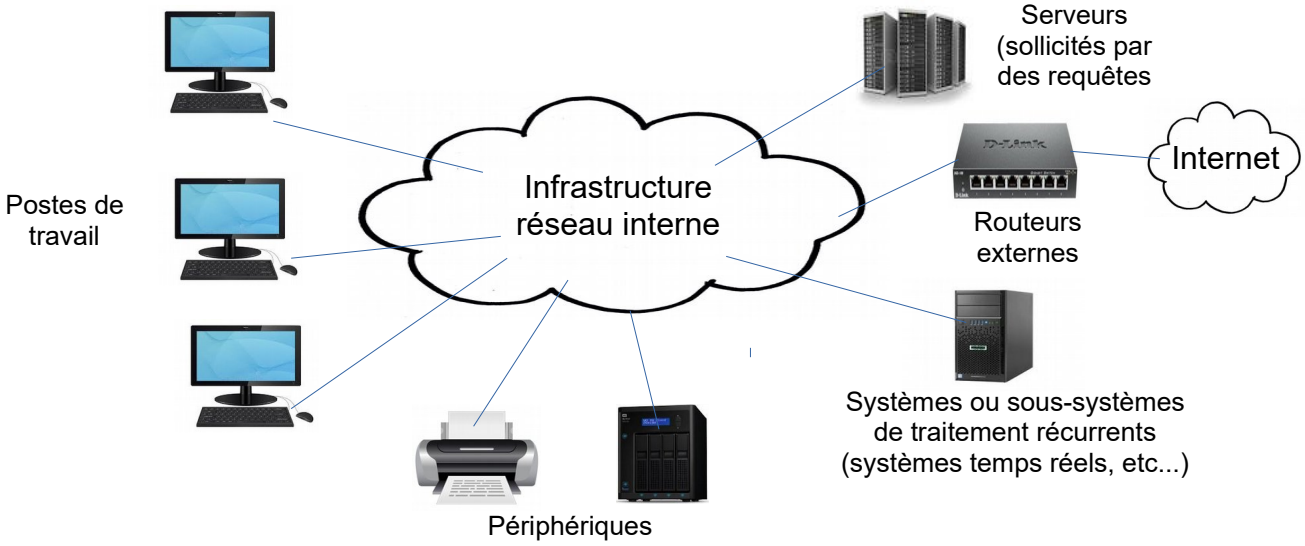


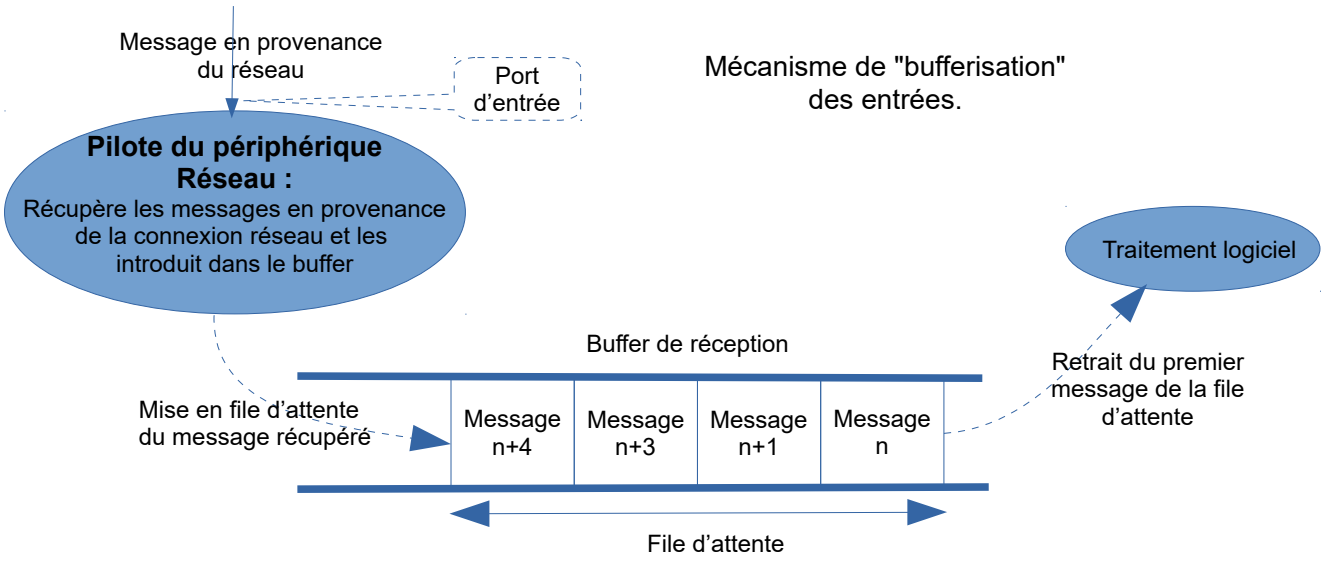
Schéma de principe d'un S.I organisé autour d'une infrastructure réseau

La quantité d'informations circulant à un instant donné à travers les différents composants matériels de l'infrastructure réseau interne du S.I. (routeurs et médias) dépend évidemment de la quantité de messages échangés par les différents équipements du S.I entre eux mais aussi avec le "monde extérieur" (ici, il s'agit du W.E.B, par l'intermédiaire de routeurs externes). Or, le débit maximal d'informations de l'infrastructure réseau interne en un point du réseau interne est forcément limité par les capacités physiques des différents médias et nœuds d'interconnexions physiques dont dépend le débit instantané en ce point.

A priori, nous pouvons supposer que, lors de la conception du système, les capacités de transmission de ces différents éléments physiques ont été dimensionnées pour répondre aux "pics" de sollicitations prévisibles au moment de sa réalisation. Cependant, s'agissant d'un Système Informatique travaillant lui-même à l'intérieur d'un système d'information ouvert sur un réseau public (internet), il est très difficile de déterminer l'évolution du volume de sollicitations internes et externes auxquelles il devra être capable de répondre à moyen et long terme. Il est donc assez probable que le réseau interne d'un tel système puisse, d'une manière temporaire ou à terme, présenter des dysfonctionnements dus à la saturation de ses capacités de transport d'informations.

IV.3.2.2.2.MÉCANISME ET CONSÉQUENCES:

De tels dysfonctionnements, appelés souvent "congestions" présentent des caractéristiques très semblables à ce qui a été décrit plus haut, dans le paragraphe d'introduction: d'abord, une diminution des temps de réponse, puis une perte de messages, pouvant évoluer soit vers une panne franche de type "stack overflow" si la cause de la congestion persiste, soit vers un retour à un fonctionnement normal si cette cause disparaît. Ces symptômes sont la plupart du temps à imputer au mécanisme LOGICIEL de "bufferisation" qui est appliqué par les systèmes d'exploitation à l'acquisition des messages en provenance du réseau. Le schéma ci-dessous présente ce mécanisme:



COMMENTAIRES:

- Les messages en provenance du réseau sont acquis par un logiciel "pilote de périphérique" intégré au système d'exploitation;
- Ce logiciel place chacun de ces messages en file d'attente dans un "buffer de réception";
- Les logiciels qui utilisent ces messages réseaux viennent les retirer dans la file d'attente "à leur rythme", au fur et à mesure de leurs besoins;
- De ce fait, s'il arrive plus de messages réseaux que les logiciels de traitement ne peuvent en récupérer dans la file d'attente, la longueur de cette file va augmenter. Dans le cas inverse, elle va diminuer.

Remarquons d'abord que l'augmentation de la longueur de la file d'attente provoque un retard dans la prise en compte des messages par les logiciels de traitement. Ce retard provoquera une augmentation du "temps de réponse" de l'équipement aux sollicitations en provenance du réseau.

D'autre part, un "buffer de réception" est un espace mémoire qui possède forcément une contenance FINIE. De ce fait, si la longueur de la file d'attente dépasse cette contenance, deux types de dysfonctionnement peuvent être observés:

- SI le logiciel du pilote de périphérique teste le dépassement de capacité du buffer avant d'introduire un nouveau message en file d'attente, ce nouveau message sera IGNORÉ. De ce fait, des informations ne seront pas traitées: ceci peut être un dysfonctionnement grave si ces données font partie d'échanges à caractère "transactionnel" (échanges entre banques, par exemple);
- SINON, il va placer le nouveau message EN DEHORS de la zone mémoire allouée au buffer. Cette action peut avoir pour résultat:
  - SI l'emplacement choisi se situe à l'intérieur de la zone de travail du processus concerné, des données ou instructions appartenant au système d'exploitation ou à d'autres applications pourront être détruites. Ce type de dysfonctionnement provoque un "plantage" signalé en général par le message BUFFER OVERFLOW (dépassement de la capacité du buffer) ou par des messages de type ILLEGAL OPCODE (instruction inconnue ou "illégale");
  - SINON si la zone de mémoire visée se situe à l'extérieur de la zone allouée au processus, une alarme de VIOLATION DE MÉMOIRE apparaît;
  - Dans les deux cas, l'exécution du logiciel va se trouver interrompue, le seul moyen de la reprendre étant un "reboot" du système.

IV.3.2.2.3.REMÉDIATION:

IV.3.2.2.3.1.Augmenter la capacité des buffer d'entrée:

En général, les systèmes d'exploitation permettent (par paramétrage des entrées/sorties), de fixer la contenance des buffets associés à chaque entrée. Une des solutions pour améliorer le fonctionnement est donc d'augmenter suffisamment cette contenance pour éviter (ou au moins, rendre très improbable) son dépassement.

Cependant, cette solution ne résout pas le problème de l'augmentation du temps de réponse. En effet, l'augmentation de la longueur de la file d'attente des messages a pour conséquence d'augmenter le temps d'attente maximum des messages de la file, provoquant de ce fait une augmentation du temps de réponse à ces messages.

De ce fait, si l'augmentation du volume du buffer diminue la probabilité de perdre des données, elle favorise en revanche un allongement du temps de réponse.

IV.3.2.2.3.2.Augmenter la rapidité d'exécution de l'équipement:

Une autre solution consiste à augmenter la vitesse d'exécution de l'équipement: en effet, les logiciels de traitement s'exécutant plus rapidement, ils videront plus vite la file d'attente. Cette augmentation peut être obtenue de diverses manières:

- L'augmentation de la vitesse d'exécution d'un logiciel peut être obtenue par le remplacement de l'équipement par un équipement plus performant en termes de puissance de calcul (cette solution très simple est évidemment la plus onéreuse).
- Cependant, dans certains cas, il est possible d'obtenir un résultat analogue en augmentant la capacité de la mémoire vive. En effet, disposer d'une plus grande quantité de mémoire vive

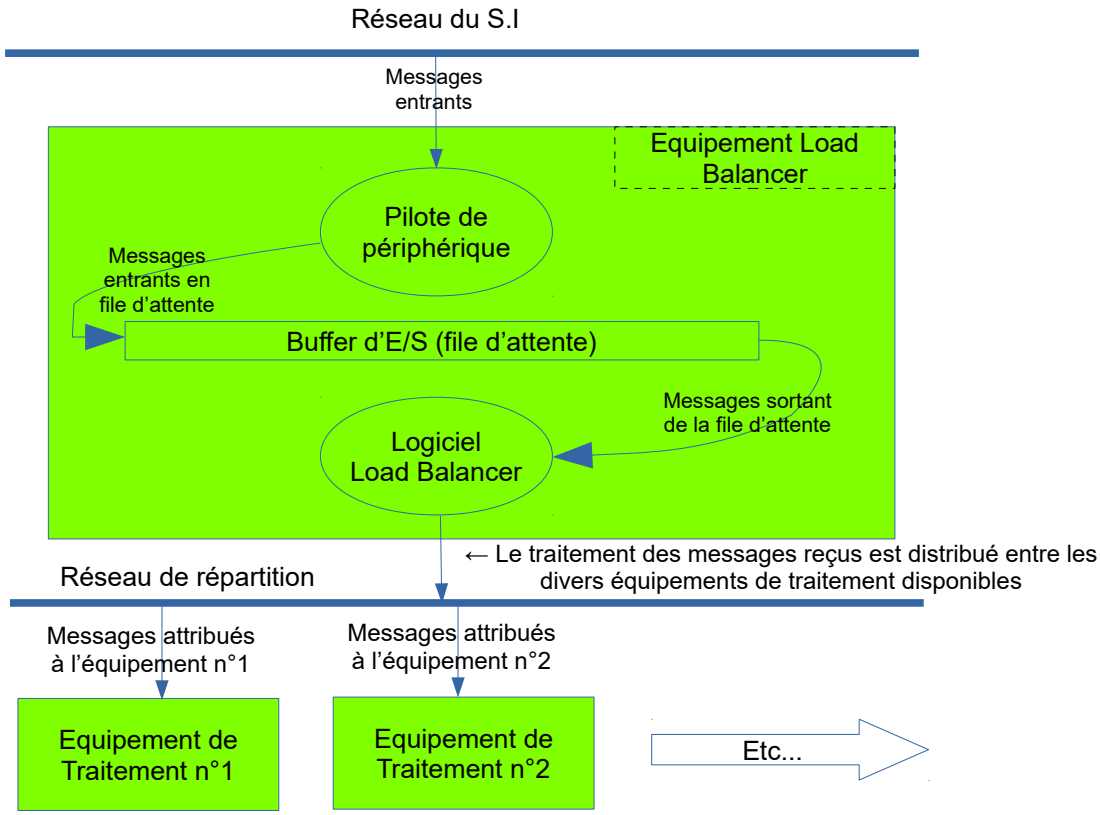
permet d'augmenter la taille de la partie des "exécutables" qui peut être chargée dans cette mémoire, diminuant de ce fait le besoin de "swapping" des logiciels.

- Le remplacement des "cartes" de mémoires vives par des mémoires plus performantes peut également augmenter la vitesse d'exécution de l'équipement en diminuant le temps d'accès des instructions aux données qu'elles utilisent. Cette solution peut bien sûr se combiner avec la solution précédente.

NOTA: *Le SWAPPING est une technique qui permet de diviser l'exécutable d'un logiciel en plusieurs "pages" si celui-ci est plus volumineux que la mémoire disponible au moment de l'exécution. De ce fait, à un instant donné, seule la page concernée par l'exécution peut être chargée en mémoire. Quand cette page n'est plus concernée par l'exécution, elle est recouverte par une autre page. Cette technique qui exige des lectures fréquentes sur le disque dur, permet d'exécuter un logiciel plus volumineux que la mémoire disponible mais ralentit considérablement la vitesse d'exécution.*

IV.3.2.2.3.3.Augmenter le nombre de processeurs de traitement*:*

Enfin, il est possible d'augmenter le nombre d'équipements de traitement en les gérant par un "load balancer". Cette technique peut être représentée par le schéma suivant:



COMMENTAIRES:

- La solution consiste à placer en position "frontale" par rapport aux entrées en provenance du réseau 1 (sur lequel arrivent les messages à traiter), un équipement appelé LOAD BALANCER (répartiteur de charge). Le pilote de périphérique de cet équipement récupère les messages en provenance du réseau et les introduit dans la file d'attente du buffer d'entrée;

- Le logiciel Load Balancer de l'équipement se charge de récupérer les messages dans la file d'attente et de les expédier vers les équipements de traitement en veillant à les répartir de façon à égaliser autant que possible les charges de traitement de ces équipements.
- Les avantages de cette solution sont:
  - D'augmenter la puissance de traitement disponible, donc la vitesse de traitement, et donc, le temps de réponse;
  - D'être très évolutive: toute augmentation de la demande peut être résolue par l'adjonction d'un équipement supplémentaire;

REMARQUE: La solution n'est pas forcément très onéreuse car les logiciels des équipements de traitements sont identiques et les équipements rajoutés peuvent être de même puissance ou de puissance inférieure aux équipements préexistants.

IV.3.2.3.Dépassement de la puissance de traitement maximale des PROCESSEURS:

IV.3.2.3.1.CAUSES:

De nos jours, la plupart des équipements informatiques, mais aussi de nombreux autres équipements comme les automobiles ou certains appareils électroménagers, sont équipés de PROCESSEURS. Rappelons que ceux-ci sont les composants complexes capables d'exécuter les INSTRUCTIONS du CODE MACHINE composant les FICHIERS EXÉCUTABLES associés aux LOGICIELS. Les équipements informatiques composant un système informatiques sont équipés de C.P.U (Central Processing Units) et de G.P.U (Graphic Processing Units).

Actuellement, la plupart de ces PROCESSEURS sont équipés de plusieurs CŒURS (les "exécuteurs fixes" du modèle de VON NEUMAN), ce qui leur permet d'exécuter simultanément plusieurs instructions. Ceci revient à dire que ces processeurs sont capables d'exécuter SIMULTANÉMENT plusieurs "fils d'exécution" (appelés aussi "threads").

IV.3.2.3.2.MÉCANISMES ET CONSÉQUENCES:

Les SYSTÈMES D'EXPLOITATION actuels sont MULTITÂCHES. Ceci revient à dire qu'ils permettent d'exécuter simultanément plusieurs PROCESSUS LOGICIELS, eux-mêmes pouvant être composés de plusieurs threads (rappelons qu'un processus logiciel est un programme informatique en cours d'exécution). Cette simultanéité peut être RÉELLE s'il existe au moins autant de CŒURS que de threads à exécuter, ou APPARENTE dans le cas contraire.

Dans ce dernier cas, le système d'exploitation organise le partage de l'utilisation des différents CŒURS par les différents PROCESSUS grâce à un composant logiciel appelé SCHEDULER (ou planificateur de tâches), selon les modalités suivantes:

- Lorsque plusieurs processus actifs simultanément sont considérés comme ayant la MÊME PRIORITÉ opérationnelle, ils se partagent le temps d'exécution à parts égales. Le partage s'effectue par créneaux de temps relativement courts (la plupart du temps, 100 ms) de façon à ce que l'utilisateur ait l'impression que ces processus s'exécutent simultanément. C'est la gestion en TEMPS PARTAGÉ (Time Shearing ou Time Slicing);
- En revanche, lorsque deux groupes de processus ont des PRIORITÉS DIFFÉRENTES, les processus de priorité la plus faible doivent ATTENDRE que tous les processus de l'autre groupe soient terminés avant d'accéder au C.P.U (On dit que les priorités les plus fortes PRÉEMPTENT le C.P.U au détriment des priorités plus faibles qu'elles).

Ces différentes considérations permettent d'expliquer le comportement des équipements informatiques à mesure que la charge de travail demandée au C.P.U s'approche, voire dépasse sa capacité maximale de traitement:

- Quand la charge de travail demandée au processeur s'approche de la charge maximale qu'il peut assurer **sans la dépasse**r, les tâches dont les priorités sont les plus élevées peuvent, du fait de la PRÉEMPTIVITÉ, continuer de s'exécuter normalement. Cependant, le SCHEDULER trouvant de moins en moins de "puissance CPU" disponible pour exécuter les tâches de priorité plus faible, celles-ci peuvent se trouver ralenties, parfois même arrêtées;
- Puis, si la "puissance C.P.U" exigée pour l'exécution des tâches de plus hautes priorité arrive à dépasser les capacité du processeur en place, le SCHEDULER ne trouve plus aucune disponibilité pour exécuter les tâches de priorité plus faible: celles-ci se trouveront donc bloquée. D'autre part, les tâches de priorité haute se trouveront ralenties;
- Dans certains cas, si la surcharge du C.P.U se prolonge, le fonctionnement du système d'exploitation peut être affecté d'une manière irréversible, du fait de possibles dépassements de capacités des tables de ressources systèmes.

Du point de vue des utilisateurs, le dépassement de la capacité d'exécution du C.P.U se traduira donc d'abord par un ralentissement des tâches de priorité faible, puis par un blocage complet de ces tâches (absence de réponse aux sollicitations extérieures, images figées, etc.). Si la surcharge persiste, les tâches de priorité supérieure peuvent à leur tour être concernées, jusqu'à provoquer un dysfonctionnement fatal de l'instance du système d'exploitation en cours d'exécution, nécessitant de ce fait le réamorçage du système.

IV.3.2.3.3.REMÉDIATION:

IV.3.2.3.3.1.Dans des situations d'urgence:

Lorsqu'une surcharge du C.P.U survient alors que la situation opérationnelle nécessite la préservation de l'exécution de certaines tâches en cours (par exemple, des tâches assurant le contrôle de processus opérationnels ou assurant la sécurité), il est possible d'intervenir immédiatement et en temps réel par des commandes d'administration système:

- Pour récupérer de la puissance C.P.U en arrêtant des tâches non essentielles. Sous Windows, l'interface "gestionnaire des tâches" peut être utilisé dans ce but. Sous les systèmes Unix/Linux, la commande kill propose les mêmes possibilités;
- Pour favoriser l'exécution de ces tâches au détriment des autres, en haussant leur priorité d'exécution. Sous Windows, le "gestionnaire des tâches" (onglet "détail") permet de modifier la priorité d'une tâche en cours d'exécution. Sous Unix/Linux, la commande "renice" offre des possibilités similaires.

REMARQUE: *Ces manipulations nécessitent des connaissance et une pratique de l'administration système assez élevées. De plus, elles n'ont d'effet que pour l'exécution en cours: elles ne constituent donc que des palliatifs provisoires.*

IV.3.2.3.3.2.Remédiations pérennes:

Comme précédemment, il est possible d'augmenter la vitesse d'exécution du C.P.U en augmentant la capacité de la mémoire vive ou en remplaçant les cartes de mémoires vive par des modèles dont le temps de réponse est plus court. Ces mesures permettent de retarder le remplacer des équipements en cause par des équipements dotés de C.P.U plus puissants et de capacités mémoires supérieures.

V.ANNEXES: RAPPELS DE NOTIONS INFORMATIQUES:

V.1.NOTIONS DIVERSES:

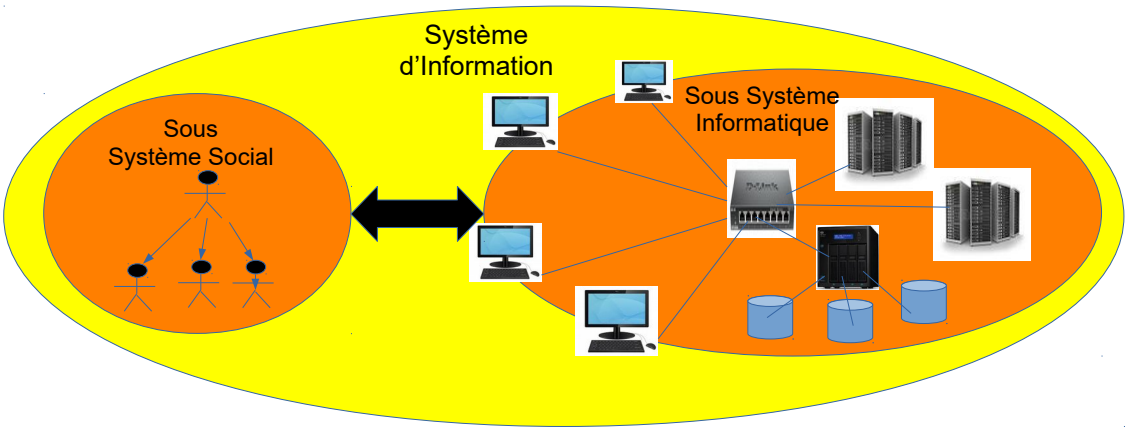
V.1.1.SYSTÈMES D'INFORMATION ET SYSTÈMES INFORMATIQUES:

Un SYSTÈME D'INFORMATION peut être défini comme un ensemble de ressources matérielles et humaines dont le but est d'aider une organisation à but économique ou social (entreprise, association, administration, etc.) à collecter, stocker, traiter et distribuer les informations qu'elle produit ou qu'elle utilise dans le cadre de son activité.

Un tel SYSTÈME D'INFORMATION peut être décomposé en deux sous-systèmes:

- Un sous-système SOCIAL organisant et coordonnant les activités des personnels de l'organisation humaine utilisatrice;
- Un sous-système TECHNIQUE rassemblant autour d'un ou plusieurs RÉSEAUX INFORMATIQUES divers équipements matériels ou logiciels destinés à supporter l'exécution des traitements informatiques contribuant aux activités de l'organisation. Ce sous-système TECHNIQUE est en général appelé SYSTÈME INFORMATIQUE pour le distinguer du SYSTÈME D'INFORMATION englobant.

Le schéma ci-dessous précise ces différentes notions:



REMARQUE: *Dans le cadre du présent ouvrage, nous utiliseront le sigle SDI pour désigner un système d'information et le sigle SI pour désigner un système informatique.*

V.1.2.NOTION DE PROCESSUS D'AFFAIRE:

Dans le cadre d'un SDI, on appelle PROCESSUS D'AFFAIRE (ou encore PROCESSUS MÉTIER) un ensemble d'activités corrélées ou interagissant entre elles en vue de la réalisation des différentes AFFAIRES traitées par l'organisation. Un processus d'affaire est donc une manière de réaliser certaines des activités exercées par l'organisation.

Un processus d'affaire exige donc l'intervention des PERSONNELS de l'organisation, ceux-ci s'aidant des fonctionnalités offertes par le SYSTÈME INFORMATIQUE pour accomplir leurs tâches.

V.1.3.NOTION DE SYSTÈME INFORMATIQUE QUALIFIÉ:

Nous considérerons ici qu'un logiciel informatique est QUALIFIÉ lorsqu'il a satisfait à un ensemble de vérifications qui permettent d'assurer que ce logiciel est apte à être utilisé dans les conditions PRÉVUES PAR SON CAHIER DES CHARGES.

Cette procédure de qualification comprend des tests fonctionnels effectués en environnement opérationnel dans toutes les configurations prévues par le cahier des charges et des tests de robustesse qui permettent de vérifier la résistances aux erreurs (erreurs de paramétrage, par exemple) et la régularité du service dans la durée (taux de pannes ou durée d'indisponibilité compatibles avec les spécifications du cahier des charges).

Par extension, nous dirons qu'un système informatique est QUALIFIÉ lorsqu'il a satisfait à un tel ensemble de tests de qualification. Ceci n'implique pas que ces systèmes soient exempts de toute faille de conception ou de fonctionnement, mais suggère tout de même que ces failles sont très peu nombreuses et concernent des cas d'utilisation suffisamment improbables pour ne pas avoir été détectées par des tests de qualification d'un niveau adapté aux exigences des utilisateurs.

***NOTA**: Cette notion de qualification est importante car elle induit une différence de méthodologie dans la recherche des dysfonctionnement suivant que le système cible est ou non qualifié: concernant un système qualifié, la probabilité pour qu'un dysfonctionnement soit dû à un défaut de conception est à priori très faible. Il est donc préférable de rechercher en priorité une cause externe.*

Cependant, si une cause interne semble dans ce cas hautement improbable, elle ne doit jamais être totalement rejetée car il est impossible lors du test d'un système complexe de qualifier à 100% l'ensemble des cas d'utilisation.

V.1.4.NOTION DE PROCESSUS LOGICIEL:

En informatique, le terme PROCESSUS LOGICIEL représente une INSTANCE D'EXÉCUTION d'un PROGRAMME INFORMATIQUE donné. Un processus associé à l'exécution d'un programme n'existe donc que durant l'exécution de ce programme. Dans le cadre d'un système d'exploitation MULTITACHES, plusieurs instances d'exécution d'un même programme peuvent s'exécuter simultanément dans la même machine.

V.1.5.NOTION DE BUFFER EN INFORMATIQUE:

En informatique, le terme BUFFER (en français: TAMPON) désigne une zone de la mémoire vive d'un ordinateur qui est allouée à un PROCESSUS donné pendant tout ou partie de son temps d'exécution.

Lors de l'exécution d'un PROCESSUS, des zones de mémoire vive (des BUFFERS) peuvent être alloués PROVISOIREMENT et DYNAMIQUEMENT à ce processus pour permettre son exécution. Par exemple:

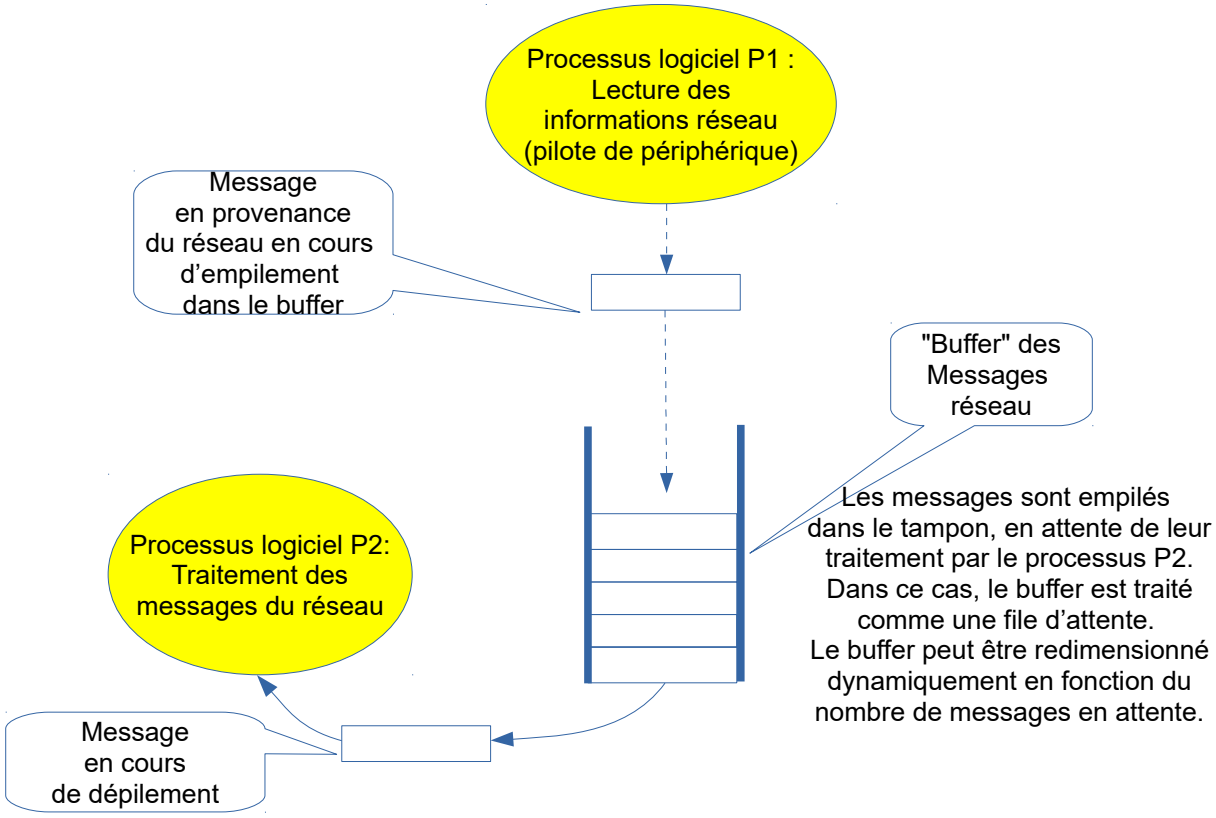
- Pour stocker provisoirement des données lues à partir un équipement d'entrée-sortie avant le traitement de celles-ci ou pour stocker des messages à émettre vers un équipement d'entrée-

sortie en attendant que la date d'émission soit atteinte ou que l'équipement récepteur soit prêt à les traiter (BUFFERS d'ENTRÉE-SORTIE);

- Pour accueillir des segments de code exécutable d'un programme volumineux qui ne peut, faute de place, être entièrement mis en mémoire en début d'exécution (exécution d'un programme en OVERLAY);
- Pour gérer en mémoire une donnée complexe (un tableau, un arbre, etc) dont on ne connaît pas le volume maximum lors du lancement de l'exécution du programme;
- Etc.

EXEMPLE DE BUFFER DYNAMIQUE:

Traitement des données réseau.



REMARQUE: *dans le cas présenté, la longueur de la file d'attente dépend de la différence entre le débit des messages réseau entrant et le débit des messages traités par P2. SI P2 est trop lent, la file d'attente va s'allonger et pourra excéder la capacité maximale du buffer, entraînant un dysfonctionnement du logiciel (Erreur de type STACK OVERFLOW).*

V.2.ÉLECTRONIQUE ANALOGIQUE ET ÉLECTRONIQUE DIGITALE:

V.2.1.INTRODUCTION ET RAPPELS:

A l'intérieur d'un système électronique, l'information traitée est toujours représentée par un signal électrique dont les variations de la TENSION instantanée représentent la valeur de la grandeur physique que le signal transporte.

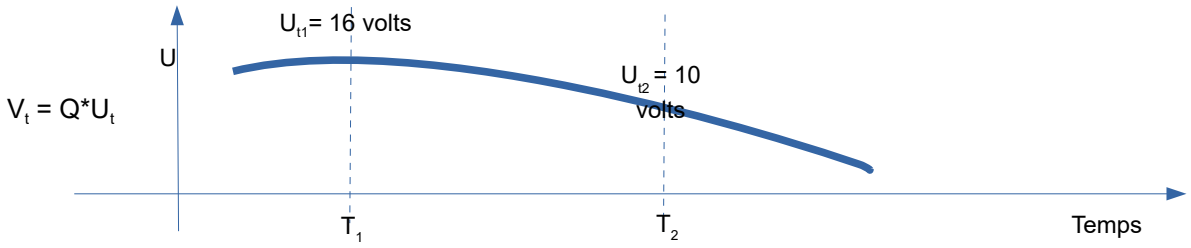
Il existe deux manières de représenter une grandeur (et ses variations) par un signal électrique:

A- La représentation ANALOGIQUE, dans laquelle la tension instantanée U du signal est directement proportionnelle à la valeur instantanée V de la grandeur représentée:

$$V_t = Q*U_t$$

- V_t: valeur instantanée de la grandeur à l'instant t;
- U_t: valeur instantanée de la tension à l'instant t;
- Q: coefficient de proportionnalité entre les deux valeurs.

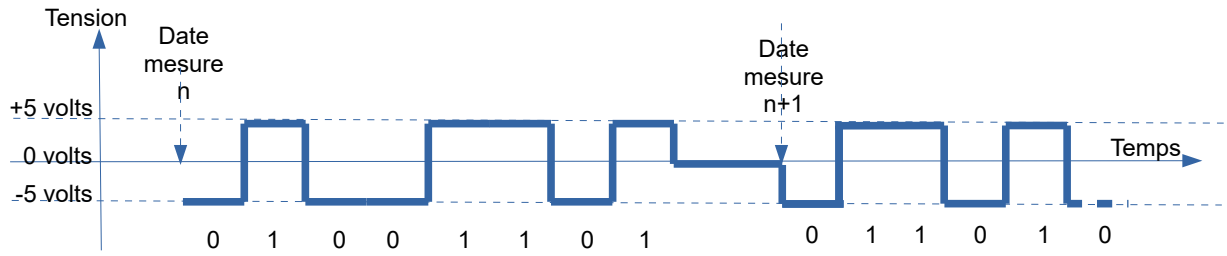
Dans ce cas, la variation du signal prend la forme d'une courbe continue U = f(t):



Notons que la représentation analogique permet une transmission des valeurs "en continu", la tension U, mesurée à une date t quelconque représentant la valeur V transmise à cet instant t.

B- La représentation DIGITALE dans laquelle la valeur de la grandeur à un instant t est représentée par un nombre codé en BINAIRE. Dans ce cas, les variations de la tension du signal représentent la suite des DIGITS composant ce nombre binaire. Dans ce cas, les variations du signal représentent un tracé "en créneaux" variant entre deux valeurs représentant respectivement les digits 0 et 1.

EXEMPLE:



Dans ce cas, les valeurs de la grandeur ne sont par transmises en continu, mais "par valeurs discrètes" (par exemple, avec une période de transmission de 100ms). Le signal présente donc des suites de "trains de digits" ressemblant à celui qui est représenté ci-dessus, chacun de ces trains codant une valeur de la grandeur à une date de mesure donnée.

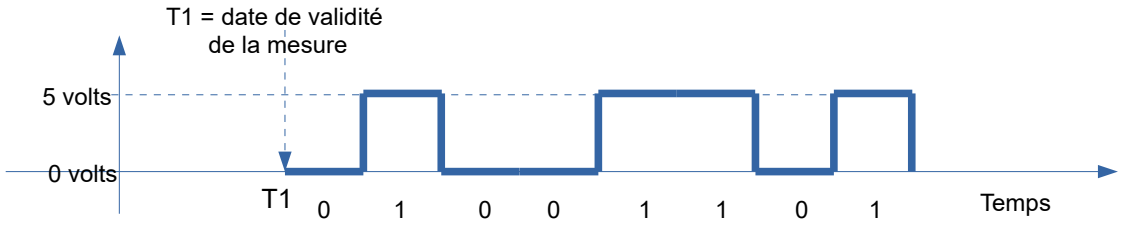
V.2.2.L'ÉLECTRONIQUE DIGITALE:

L'électronique DIGITALE exploite des signaux électriques dont la tension ne prend que deux valeurs. Chacune de ces valeurs représente un "digit" de la numération binaire (1 ou 0).

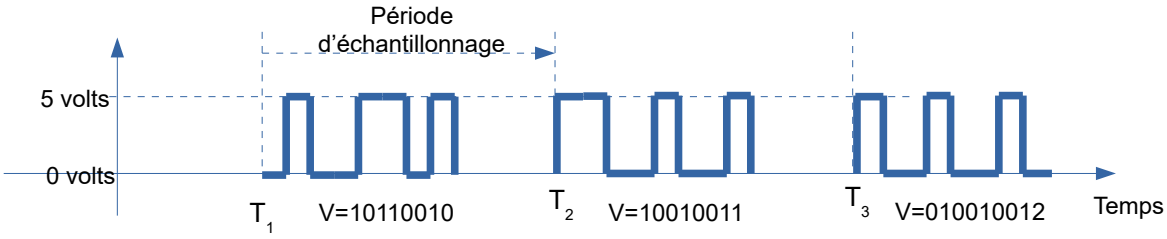
Par exemple, dans un signal codé en logique binaire TTL, le digit 1 est en théorie représenté par un signal de tension 5 volts tandis que le digit 0 est représenté par un signal de tension 0 volt.

Les grandeurs acheminées par ces signaux sont représentées par des suites de digits binaires.

EXEMPLE: un signal dont la valeur varie dans le temps suivant la courbe ci-dessous, transporte la valeur binaire 10110010, qui représente le nombre 178 en décimal.

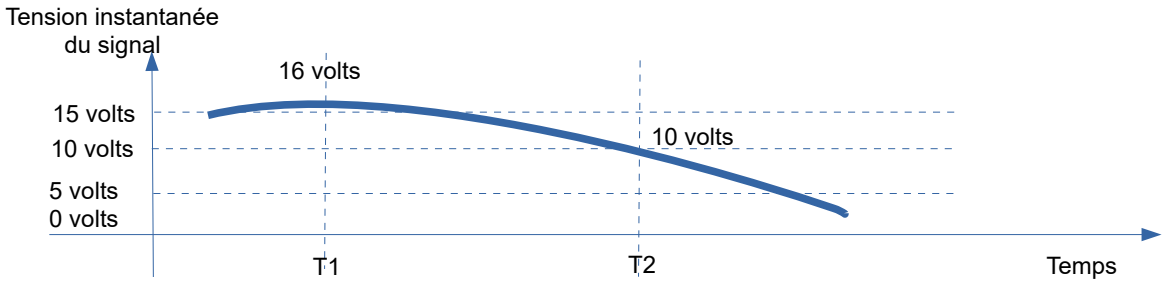


Remarquons que cette valeur est la valeur instantanée de la grandeur concernée, mesurée à un instant donné (ici, l'instant T1). Pour représenter l'évolution dans le temps d'une grandeur, il est nécessaire de convenir d'une période d'échantillonnage et de transmettre le "train d'impulsions" représentant la valeur de la grandeur mesurée à chacune de ces périodes:



V.2.3.L'ÉLECTRONIQUE ANALOGIQUE:

La principale différence entre ÉLECTRONIQUE DIGITALE et l'ÉLECTRONIQUE ANALOGIQUE est que dans le cadre de cette dernière, les signaux codent non pas des digits binaires, mais directement des valeurs physiques: celles-ci sont proportionnelles à la tension électrique du signal. Par exemple, si par convention, on définit qu'un volt de tension représente 10 degrés Celsius, un signal de 16 volts représentera une température de 160 degrés Celsius. Dans le temps, le signal prendra la forme d'une ligne continue exprimant directement la valeur de la grandeur représentée en fonction du temps:



Interprétation:

- A l'instant T1, la tension du signal est de 16 volts. Elle code donc la valeur de température 160 degrés Celsius;
- A l'instant T2, la tension est de 10 volts. Elle code donc la valeur de température 16 degrés Celsius.

Remarque: nous pouvons voir que contrairement aux signaux digitaux où les valeurs transmises le sont d'une manière discrète, les valeurs sont transmises en électronique analogique sont transmises d'une manière continue.

V.2.4.COMPOSANTS DIGITAUX ET AUTRES COMPOSANTS:

V.2.4.1.DÉFINITIONS:

Tous les composants et sous-composants ACTIFS d'un Système Informatique sont des équipements électriques ou électroniques (ils ont besoin d'une alimentation électrique pour fonctionner). Cependant, nous pouvons distinguer deux types de composants:

- Une majorité de ces composants fonctionnent entièrement suivant les principes de l'électronique digitale. ***Par exemple:*** les BIOS, les BUS, les équipements de liaison réseau, etc;
- Le reste des composants peut intégrer à la fois des parties digitales, des parties analogiques et des parties mécaniques. ***Par exemple:*** les disques durs, les convertisseurs digitaux-analogiques, etc.

Cette distinction se justifie par le fait que, du point de vue de leur fiabilité, ces deux types de composants se comportent de façon assez différente. Les deux sous-chapitres suivants détaillent ces différences.

V.2.4.2.CARACTÉRISTIQUES PRINCIPALES DES COMPOSANTS DIGITAUX:

Les composants d'un S.I qui fonctionnent entièrement selon les principes de l'ÉLECTRONIQUE DIGITALE exploitent des signaux codant des digits binaires. De ce fait, ces signaux sont sensés ne prendre que deux valeurs de tension (exemple: -5 volt et +5 volts). Cependant, pour tenir compte des

variations des tensions fournies par les alimentations électriques en fonction de leur vieillissement et des conditions ambiantes, les composants digitaux sont conçus pour admettre une large marge d'erreur sur ces deux valeurs:

EXEMPLE: *Pour un signal codé en logique TTL, le niveau logique bas (codant le zéro) doit être compris entre 0 V et 0,8 V, tandis que le niveau logique haut doit être compris entre 2,0 V et 5 V*.

Du fait de ces tolérances, ces composants peuvent fonctionner parfaitement même si les signaux sont détériorés par le vieillissement ou parasités par l'ambiance de fonctionnement, tant que les valeurs de codage restent à l'intérieur de ces seuils de tolérance. Lorsque l'écart devient trop important, le composant (ou l'ensemble de composants auquel il appartient) cesse tout simplement de fonctionner. Le remplacement du composant défaillant rétablira pleinement le fonctionnement et la fiabilité: les composants électroniques sont donc ENTIÈREMENT RÉPARABLES. De ce fait, entre le début de leur utilisation (mise en fonction initiale ou remise en fonction après réparation) et la survenue d'une panne, le fonctionnement global ne se dégrade pratiquement pas.

REMARQUE: *ceci ne veut pas dire que ces composants ne vieillissent pas, mais du fait de leur fonctionnement digital le vieillissement n'impacte pas le service rendu avant la survenue d'une panne. En effet, nous verrons plus loin que leur TAUX DE PANNE (probabilité pour qu'une panne survienne pendant un intervalle de temps donné) est constant. En revanche, leur FIABILITÉ diminue dans le temps.*

CONCLUSION: du point de vue de leur fiabilité, les composants digitaux présentent donc les caractéristiques suivantes:

- Pour un observateur externe, leurs fonctionnalités et performances ne semblent pas se dégrader dans le temps: ils sont entièrement fonctionnels jusqu'à ce qu'ils tombent en panne;
- Ils sont entièrement réparables: la réparation d'un composant rétablit toutes ses fonctionnalités et sa fiabilité initiale.

V.2.4.3.CARACTÉRISTIQUES PRINCIPALES DES COMPOSANTS NON DIGITAUX:

Il existe cependant des composants d'un S.I qui ne sont pas "entièrement digitaux". Il s'agit en particulier de tous les périphériques intégrant des parties mécaniques: imprimantes, disques durs mécaniques (par opposition aux Solid State Disks qui sont entièrement digitaux, etc.), mais aussi de ceux qui fonctionnent complètement ou partiellement en électronique analogique (en particulier, les boîtiers d'alimentation et les convertisseurs digitaux-analogiques).

Contrairement aux composants entièrement digitaux qui fonctionnent parfaitement jusqu'à ce que les tensions des signaux sortent des limites, les performances des composants non entièrement digitaux se dégradent continûment en fonction de leur durée d'utilisation: ce fait impacte le service rendu, car:

- Dans le cas de composants dont les signaux de sortie sont analogiques, les tensions instantanées de ceux-ci sont proportionnelles aux grandeurs qu'ils représentent. Toute détérioration dans le mécanisme de conversion entraîne donc une erreur dans les données fournies;
- Dans le cas de composants comportant des parties mécaniques, il faut remarquer que ces parties mécaniques sont commandées par des signaux analogiques (par exemple, les signaux de positionnement des têtes de lecture des disques durs mécaniques). La remarque

précédente s'applique donc. D'autre part, les parties mécaniques sont forcément soumises à une usure mécanique qui altère plus ou moins leur fonctionnement et leurs performances.

EXEMPLES:

- L*a capacité d'enregistrement d'un disque dur mécanique subit une attrition au fur et à mesure de son utilisation: certaines zones d'enregistrement peuvent être détériorées par des poussières, par des chocs dus aux têtes de lecture, etc. Sa capacité d'enregistrement diminue donc progressivement. Le firmware embarquée permet souvent de mettre hors circuit ces zones et, dans certaines conditions, de régénérer l'information. Cependant, à partir d'une certaine usure, trop de surface se trouve détériorée pour que le fonctionnement puisse être assuré;*
- *Les convertisseurs digitaux-analogiques comprennent des composants non digitaux dont les caractéristiques peuvent varier dans le temps (par exemple, des transistors de puissance ou des capacitances dont les performances diminuent dans le temps et sont sensibles à l'environnement). La fidélité et la précision de la conversion peuvent donc diminuer dans le temps.*

De plus, ces composants ne sont en général PAS COMPLÈTEMENT RÉPARABLES:

EXEMPLE: *Il est en général possible de reformater un disque dur mécanique en panne suite à une détérioration trop importante de sa surface, mais le reformatage enlève au disque une partie de sa capacité d'enregistrement initiale.*

L'usure de ces composants peut être mise en évidence en surveillant les caractéristiques de leurs "données de sortie": celles-ci ont tendance à se dégrader dans le temps. De même, leur TAUX DE PANNE (probabilité pour qu'une panne survienne pendant un intervalle de temps donné) augmente avec la durée d'utilisation. De ce fait, le remplacement de ce type de composant peut s'avérer nécessaire même s'il n'est pas tombé en panne, pour conserver des performances acceptables.

CONCLUSION:

Du point de vue de leur fiabilité, ces composants présentent donc les caractéristiques suivantes:

- Contrairement aux composants digitaux qui conservent leurs performances jusqu'à ce qu'ils tombent en panne, les performances de ces composants se dégradent continûment et peuvent devenir insuffisantes par rapport au niveau d'exigence requis bien avant qu'une panne "franche" survienne;
- Ils ne sont pas entièrement réparables: à moins d'effectuer un échange standard, la réparation d'un composant ne rétablit pas forcément toutes les capacités de celui-ci.

V.3.VIEILLISSEMENT DES MATÉRIELS ET EFFETS SUR LA FIABILITÉ:

V.3.1.INTRODUCTION:

La notion de VIEILLISSEMENT, appliquée à un composant électrique ou électronique, est une notion intuitive qui fait surtout référence à la diminution de sa FIABILITÉ dans le temps. La suite de ce paragraphe rappelle la définition rigoureuse de certains concepts attachés à cette notion.

V.3.2.NOTION DE M.T.B.F:

La plupart du temps, les constructeurs de composants électroniques basiques ou complexes expriment le niveau de fiabilité de leurs produits par la valeur du "Medium Time Between Failures" de celui-ci. Le M.T.B.F, exprimé en HEURES, est représentatif de la moyenne arithmétique des durées qui s'écoulent entre deux pannes de ce composant s'il fonctionne en continu et si le composant est entièrement remis en état après chaque panne.

REMARQUE: le M.T.B.F est une donnée STATISTIQUE: même si le M.T.B.F est évalué à 25000 heures, rien ne garantit qu'une panne ne survienne pas au bout de 50 heures d'utilisation. Simplement, une telle panne est dans ce cas très peu probable, et en tout cas, beaucoup moins probable que si le M.T.B.F était de 150 heures. Il est également possible (mais également très peu probable) que la panne ne survienne qu'après 150000 heures d'utilisation.

NOTA: Ce M.T.B.F n'est cependant significatif qu'à condition qu'un certain nombre de conditions environnementales soient respectées. Celles-ci concernent en général:

- La plage de températures de fonctionnement recommandée;
- La conformité de l'alimentation électrique et des prises de terre;
- L'ambiance radioélectrique;
- L'humidité;
- Les poussières;
- Les contraintes mécaniques (chocs, vibrations, etc.).

Si ces conditions ne sont pas respectées, le M.T.B.F peut être très notablement raccourci.

Ces conditions de fonctionnement sont la plupart du temps spécifiées par les constructeur. Leur respect est une des conditions de validité de la GARANTIE CONSTRUCTEUR.

V.3.3.NOTION DE DURÉE DE VIE:

La durée de vie d'un composant est la durée pendant laquelle on peut espérer utiliser ce matériel à condition que:

- Les conditions d'utilisation énoncées par le constructeur soient respectées;
- La maintenance préventive prévue soit correctement effectuée;
- Les dysfonctionnements soient corrigés autant qu'il est possible (maintenance corrective).

La durée de vie d'un composant peut donc comprendre plusieurs cycles de remise en état après panne après son début d'utilisation jusqu'à ce qu'il ne soit plus possible de rétablir un fonctionnement correct.

V.3.4.NOTION DE M.T.T.F et M.T.T.R:

Le M.T.T.F (Mean Time To Failure) ou "temps moyen avant panne" est également utilisé. La différence avec le M.T.B.F. est qu'il est représentatif de la durée s'écoulant entre sa première mise en fonction

(éventuellement après dépannage) et la première panne. La différence entre M.T.B.F et M.T.T.F est le M.T.T.R (Mean Time To Repair), c'est à dire le délai moyen de remise en service après la survenue d'une panne:

$$M.T.B.F = M.T.T.F + M.T.T.R$$

En pratique, pour les composants électroniques, M.T.B.F et M.T.T.F ont des valeurs très voisines car la durée de dépannage est très courte (elle se réduit souvent au remplacement de l'élément défectueux).

REMARQUE:

Le TAUX DE DISPONIBILITÉ est, pour une durée D donnée, le pourcentage de cette durée pendant lequel le système est disponible. On peut donc écrire:

$$\text{Taux de disponibilité} = \frac{M.T.B.F}{M.T.B.F+M.T.T.R} = \frac{M.T.B.F}{M.T.T.F}$$

V.3.5.TAUX DE PANNE:

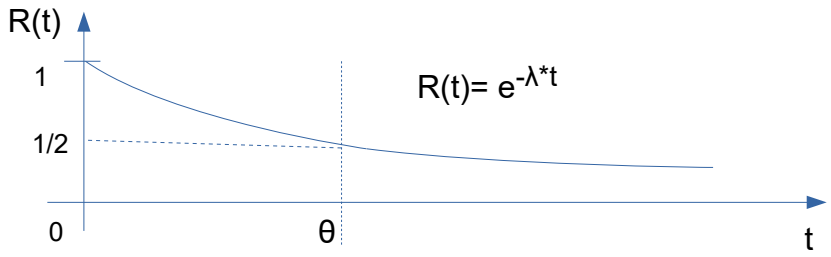
Le TAUX DE PANNE d'un composant matériel est une donnée statistique mesurant le nombre moyen de pannes auquel il faut s'attendre dans un intervalle de temps donné. Dans le cas d'un composant électronique, le taux de panne est considéré comme constant (ce n'est pas le cas pour un composant analogique ou mécanique).

V.3.6.LOI DE FIABILITÉ POUR UN COMPOSANT ÉLECTRONIQUE DIGITAL:

La loi de fiabilité d'un composant R(t) représente la probabilité pour un composant d'être encore en service à l'instant t après sa mise en fonction en continu. Pour un composant électronique, le taux de panne (noté λ) est considéré comme constant. De ce fait, cette loi de fiabilité est la fonction exponentielle:

$$R(t) = e^{-\lambda t}$$

Comme nous pouvons le voir, la fiabilité est égale à 1 (100%) au début du fonctionnement (t=0) et décroît en fonction du temps jusqu'à tendre vers 0 quand t tend vers l'infini:



Statistiquement, si λ est constant, la fiabilité à l'instant θ (M.T.T.F) doit être égale à 0,5, puisque θ représente "le temps moyen avant panne".

$$R(\theta) = e^{-\lambda*\theta} = 1/2$$

avec $e \simeq 2{,}718$

D'où, pour calculer la fiabilité d'un composant de MTTF θ pendant l'intervalle [0, t]:

$$-\lambda*\theta = \log(1/2) \Rightarrow \lambda = -\log(1/2)/\theta$$

d'où, en remplaçant λ par sa valeur -log(1/2)/θ dans l'équation de fiabilité:

$$R(t) = e^{[\log(1/2) / \theta] * t}$$

La fonction F(t), qui exprime la probabilité pour un composant de dysfonctionner avant d'atteindre la durée d'utilisation T peut alors être définie comme suit: F(T) = 1-R(T):

$$F(T) = 1-R(T) = 1 - e^{[\log(1/2)/\theta]*T}$$

REMARQUE: Les valeurs de M.T.B.F et M.T.T.F sont valables pour une exploitation dans des conditions normales d'exploitation (température, humidité, conformité et régularité de l'alimentation électrique, perturbation électromagnétique et électrostatique acceptables, etc.). Si ces conditions ne sont pas respectées, le M.T.B.T et le M.T.T.F peuvent beaucoup diminuer.

V.4.NOTIONS D'ANALYSE DES MODES DE DÉFAILLANCE (A.M.D.E.C):

*V.4.1.*INTRODUCTION:

L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (A.M.D.E.C) est une méthode PRÉVENTIVE principalement destiné à améliorer la SÛRETÉ DE FONCTIONNEMENT des entités qu'elle étudie (produits, processus, procédures, etc.). Sa démarche générale consiste à identifier les défaillances potentielles des entités étudiées (les "modes de défaillance"), puis à chercher des voies d'amélioration permettant d'éviter ces défaillances ou au moins à diminuer leur fréquence ou atténuer leurs effets.

REMARQUE: une défaillance peut être un dysfonctionnement total ou un mauvais fonctionnement (dysfonctionnement partiel);

V.4.2.NOTION DE MODE DE DÉFAILLANCE:

La démarche A.M.D.E.C commence par identifier les divers MODES DE DÉFAILLANCE que peut présenter l'entité étudiée. Ces modes de défaillance peuvent être étudiés de deux points de vue différents:

- Un mode de défaillance peut se rapporter à un COMPOSANT ORGANIQUE de cette entité: c'est l'approche ORGANIQUE (par exemple, on peut étudier les modes de défaillance de la pompe d'évacuation d'un lave-linge);
- Il peut également se rapporter à une FONCTION de cette entité: c'est l'approche FONCTIONNELLE (par exemple, on peut étudier les modes de défaillance de la fonction vidange d'un lave-linge).

*V.4.3.*NOTION DE CRITICITÉ:

Dans le domaine de la Sûreté de Fonctionnement, la criticité est définie comme "le produit de la fréquence d'apparition d'une défaillance par la gravité de ses conséquences":

C = F*G (C = criticité, F = fréquence, G = gravité)

Les paramètres F et G sont en général évalués sur une échelle numérique s'étendant le plus souvent, de 1 à 4 ou de 1 à 10 (la valeur 0 n'est jamais utilisée).

V.4.4.ÉVALUATION DE LA CRITICITÉ DES MODES DE DÉFAILLANCE:

V.4.4.1.DÉFINITION DES PONDÉRATIONS ACCORDÉES AUX VALEURS DE F ET G:

Supposons que, dans le cadre de l'A.M.D.E.C d'un système donné, nous ayons à évaluer la criticité des modes de défaillance des entités constitutives de ce systèmes. Pour ce faire, il nous faudra d'abord définir les échelle des valeurs à accorder aux paramètres F (fréquence des défaillances) et G (gravité des défaillances).

Il nous faudra donc construire deux tableaux:

- Le premier de ces tableaux définit une échelle des différentes valeurs à accorder au paramètre F en fonction de la fréquence des défaillances;
- Le deuxième définit de la même façon l'échelle des différentes valeurs à accorder au paramètre G en fonction de la gravité des défaillances.

Un exemple de ces deux tableau est présenté ci-après:

Tableau de pondération de la fréquence d'une défaillance		
FRÉQUENCE	**CARACTÉRISATION**	**PONDÉRATION**
Fréquent	La défaillance survient pratiquement tous les jours	10
Probable	La défaillance survient une à plusieurs fois par semaine	8
Occasionnel	La défaillance survient une à plusieurs fois par mois	6
Rare	La défaillance survient une à plusieurs fois dans l'année	4
Improbable	La défaillance est très rarement signalée au cours du cycle de vie de l'entité	2
Invraisemblable	La défaillance n'a jamais été signalée	1

Tableau de pondération de la gravité d'une défaillance		
GRAVITÉ	**CARACTÉRISATION**	**PONDÉRATION**
Catastrophique	Susceptible d'entraîner: - Des risque mortel pour les êtres humains; - L'interdiction de l'activité; - Des atteintes majeures à l'environnement; - Des pertes financières, pertes d'image ou pertes de clientèle engageant la survie de l'entreprise.	10
Problématique	Susceptible d'entraîner: - Des pertes financières importantes; - Une perte d'image ou de clientèle importantes.	6
Marginale	- Ne touche que des activités secondaires de l'entreprise; - N'entraîne que des pertes financières minimes; - A des répercussions limitées sur l'image ou la clientèle.	3
Insignifiante	Aucune répercussion significative sur la situation financière, l'image ou la clientèle.	1

REMARQUES SUR CES TABLEAUX:

- Les qualificatifs associés aux paramètres S (Fréquent, Probable, Occasionnel, etc.) et G (Catastrophique, Problématique, etc.) ainsi que le nombre de degrés des échelles d'évaluation et les "poids" accordés à ces degrés ne sont donnés ici que pour exemple: les personnels chargés de l'A.M.D.EC peuvent tout à fait augmenter le nombre de degrés ainsi que les qualificatifs et la pondération de ces degrés en fonction de la nature et des spécificités des entités étudiées;
- Les petits textes caractérisant les différents degrés doivent permettre de préciser le sens des qualificatifs associés à ces degrés: ainsi, il est probable que si la défaillance étudiés est la crevaison d'un pneu d'automobile, on accordera à cette défaillance le qualificatif de "fréquent"

dès qu'elle aura tendance à se produire plusieurs fois par an (et non "pratiquement tous les jours");

- Il est possible d'accorder aux paramètres F et G des valeurs qui sont intermédiaires entre deux pondérations: ainsi, si l'on estime que la fréquence d'une défaillance se situe entre "occasionnel" (6 dans le tableau) et "rare" (4 dans le tableau), la valeur du paramètre F peut être fixée à 4,5 ou à 5,2, par exemple.

V.4.4.2.ÉVALUATION DE LA CRITICITÉ:

Nous pouvons alors, à l'aide des informations contenues dans ces deux tableaux, créer un autre tableau calculant les valeurs de C = F*G) en fonction de la pondération des différentes valeurs de F et G :

CRITICITÉ				
	NIVEAU DE GRAVITÉ			
FRÉQUENCE	**Insignifiant (1)**	**Marginal (3)**	**Problématique (6)**	**Catastrophique (10)**
Fréquent (10)	10	30	60	100
Probable (8)	8	24	48	80
Occasionnel (6)	6	18	36	60
Rare (4)	4	12	24	40
Improbable (2)	2	6	12	20
Invraisemblable (1)	1	3	6	10

V.4.4.3.UTILISATION DE CES OUTILS:

Il appartient alors à l'utilisateur de décider, en fonction des missions et fonctionnalités du système étudié comment considérer les valeurs de criticité évaluées pour chaque mode de défaillance. Par exemple, dans le tableau ci-dessus, l'utilisateur peut considérer que les valeurs de criticité supérieures ou égales à 30 sont INACCEPTABLES, alors que celles qui sont inférieures à 30 et supérieures ou égales à 20 sont considérées comme INDÉSIRABLES, les autres étant ACCEPTABLES. Nous pouvons mettre en relief ces seuils d'acceptabilité par des couleurs:

CRITICITÉ				
	NIVEAU DE GRAVITÉ			
FRÉQUENCE	**Insignifiant (1)**	**Marginal (3)**	**Critique (6)**	**Catastrophique (10)**
Fréquent (10)	10	30	60	100
Probable (8)	8	24	48	80
Occasionnel (6)	6	18	36	60
Rare (4)	4	12	24	40
Improbable (2)	2	6	12	20
Invraisemblable (1)	1	3	6	10

Nota: *les valeurs sur fond rouge correspondent aux criticités considérées comme INACCEPTABLES. Les valeurs sur fond jaunes sont les criticités considérées comme INDÉSIRABLES*

, les valeurs sur fond vert étant ACCEPTABLES.

V.4.4.4.EXEMPLE:

Supposons que le mode de défaillance étudié soit la défaillance complète d'un des deux réacteurs d'un moyen courrier bimoteur. Dans ce cadre, supposons que ce type de défaillance soit considéré comme "rare" (valeur = 4) mais pas improbable (valeur = 2). De ce fait, nous accorderons au paramètre F la valeur 3.

D'autre part, si l'avion, compte-tenu de son domaine d'utilisation, est toujours capable de se poser avec un seul moteur sur un aérodrome voisin du lieu de la défaillance, nous pourrions considérerons que le niveau de gravité est critique (valeur = 6), mais loin d'être catastrophique (valeur = 10). De ce fait, nous accorderons au paramètre G la valeur 7.

Nous pouvons donc calculer la criticité C de ce mode de défaillance: C = F*G = 3*7 = 21. Selon la définition des seuils d'acceptabilité définie plus haut, cette criticité serait considérée comme INDÉSIRABLE.

V.4.4.5.UTILISATION DE L'ÉVALUATION DE LA CRITICITÉ:

Dès instant où une criticité n'est pas qualifiée comme ACCEPTABLE, il convient de prendre des mesures, soit pour la diminuer, soit pour supprimer le mode de défaillance. Dans l'exemple ci-dessus, nous pourrions, par exemple, envisager de diminuer la valeur du facteur F en utilisant des réacteurs plus fiables que ceux qui étaient prévus initialement. Supposons que cette option permette de diminuer la valeur de F de 3 à 2,5. La criticité aura alors pour valeur 7*2,5 = 17,5: elle devient ACCEPTABLE.

V.5.NOTIONS SUR L'ALIMENTATION ÉLECTRIQUE DES INSTALLATIONS :

V.5.1.REMARQUE PRÉLIMINAIRE:

Le décret N° 88-1056 du 14 novembre 1988 réglemente les pratiques concernant l'installation des équipements électriques et électronique, dans le but de garantir les personnes et les biens contre les risques d'incendie, de brûlure et d'électrocution inhérents à l'emploi de ce type d'équipement. En particulier, ce décret donne des définitions précises concernant les différentes notions attachées au domaine (notions de masse, terre, phase, neutre, techniques de mise à la masse et à la terre, etc.).

V.5.2.NOTION DE TERRE:

En électrotechnique, le terme TERRE désigne la "masse terreuse" qui supporte une installation électrique. Cette masse terreuse étant en général plutôt bonne conductrice, les charges de même signe qu'elle peut contenir ont tendance à se repousser et à se disperser également dans tout l'environnement tandis que les charges de signe contraire se neutralisent. De ce fait, en l'absence d'autres causes, la densité de charges électriques "à l'équilibre" en un point de cette masse terreuse est très faible.

***REMARQUE**: en un point ou la foudre vient de tomber, cette densité peut devenir passagèrement très élevée, mais du fait de la conductivité, cette charge électrique injectée dans le sol se dissipe très rapidement dans l'environnement (en quelques secondes au plus), faisant retomber cette densité à une valeur très proche de zéro.*

V.5.3.NOTIONS DE POTENTIEL ÉLECTRIQUE ET DE CHAMP ÉLECTRIQUE:

Le POTENTIEL ÉLECTRIQUE est une grandeur scalaire qui reflète d'ÉTAT ÉLECTRIQUE en un point de l'espace. Il se mesure en VOLTS. Nous pouvons considérer que le potentiel en un point de l'espace dépend de la répartition des charges électriques dans l'environnement de ce point.

Par convention, le POTENTIEL ÉLECTRIQUE de la TERRE est considéré comme très proche de 0 volts car la densité de charges électriques y est la plupart du temps très faible (sauf en un point touché par la foudre, mais nous avons vu que les charges injectées se dispersent très rapidement).

Si dans un domaine de l'espace, le POTENTIEL ÉLECTRIQUE n'est pas uniforme, il se crée en chaque point un CHAMP ÉLECTRIQUE. Ce champ électrique est une grandeur vectorielle dont le module est proportionnel à la VARIATION DU POTENTIEL au voisinage du point considéré (plus le potentiel varie, plus le champ électrique est intense). Toute particule électrique "plongée" dans un champ électrique subit une force (force électrostatique) dont le module est proportionnel à l'intensité du champ (E) et à la charge électrique q de la particule et dont la direction est celle du champ électrique en ce point:

$$\vec{F} = q*\vec{E}$$

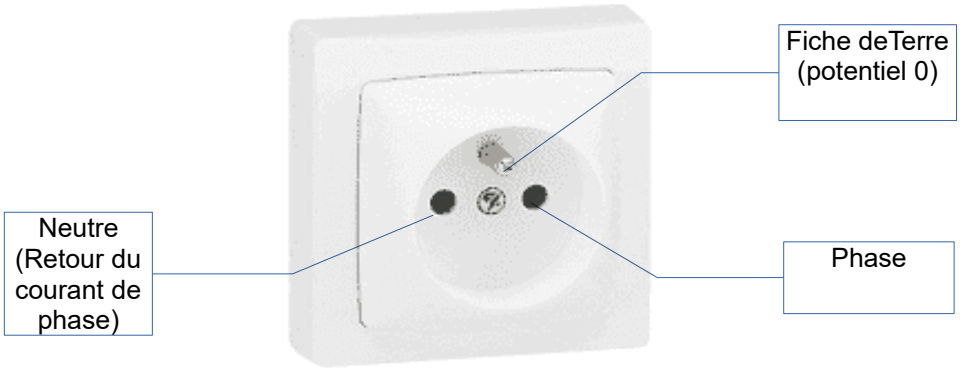
Si, dans un conducteur linéaire, deux points A et B ne sont pas au même potentiel, les charges électriques, du fait de la force électrostatique qui s'exerce sur elles, ont tendance à circuler entre ces deux points, créant ainsi un COURANT ÉLECTRIQUE. La TENSION entre A et B, qui se mesure en VOLTS est égale à la DIFFÉRENCE DE POTENTIEL entre A et B:

$$T_{ab} = V_a - V_b = \text{D.D.P entre A et B}$$

Cette D.D.P peut être assimilée au CHAMP ÉLECTRIQUE régnant dans ce conducteur.

V.5.4.NOTION DE PRISE DE TERRE:

Une "PRISE DE TERRE" est en général constituée d'un élément métallique enfoui dans le sol et relié aux installations par un câble qui permet de transmettre le potentiel de la terre (proche de 0 volts) aux équipements qui en ont besoin. Les prises électriques "trois points" qui permettant d'utiliser le courant alternatif monophasé des fournisseurs d'électricité transmettent le potentiel de la TERRE par l'intermédiaire d'une fiche dédiée:



REMARQUES:

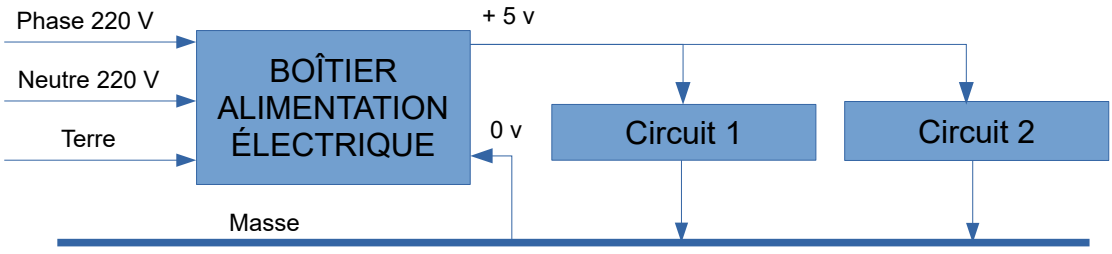
Dans le cas d'une fourniture d'électricité en courant alternatif 220 v, 50 hz, monophasé:

- La PHASE transmet un potentiel variant de -220 à +220 volts à la fréquence de 50 Hz;
- Le NEUTRE est la plupart du temps relié à la TERRE. Il est donc porté au potentiel 0 v;
- La fiche de TERRE transmet le potentiel de la TERRE à l'installation;
- Les équipements fonctionnant en alternatif monophasé sont alimentés entre la PHASE et le NEUTRE;
- Entre le NEUTRE et la TERRE, la circulation d'un courant électrique signale une anomalie de l'équipement (défaut de masse ou de terre, court-circuit).

V.5.5.NOTION DE MASSE ÉLECTRIQUE:

Dans un équipement électrique ou électronique, le terme MASSE ÉLECTRIQUE (ou simplement MASSE) désigne la partie conductrice qui supporte les différents composants actifs de cet équipement (c'est, en général, le châssis métallique de cet équipement). Dans les équipements électroniques digitaux, qui fonctionnent en courant continu, les différents circuits électriques qui les composent sont en général connectés directement à la MASSE. Celle-ci est elle-même connectée à l'un des deux conducteurs fournis par l'alimentation en courant continu de l'équipement. L'autre conducteur est relié directement au circuit. De ce fait, le courant continu fourni par l'alimentation interne traverse les circuits, puis la masse avant de retourner au bloc d'alimentation.

EXEMPLE:



Ce montage présente les avantages suivants:

- Il simplifie le câblage en économisant un conducteur pour le retour du courant;
- Il force tous les circuits au même potentiel de référence (le potentiel de la masse), évitant que des courants parasites ne se forment entre les différents circuits.

EN REVANCHE, dans les équipements électriques qui fonctionnent en courant alternatif, la phase et le neutre sont isolés de la masse. La MASSE n'est reliée qu'à la fiche "terre" des prises trois points.

D'AUTRE PART, les masses des différents équipements d'un même site peuvent être reliées entre elles, assurant ainsi l'ÉQUIPOTENTIALITÉ de toutes le masses.

V.5.6.MISE A LA TERRE DES ÉQUIPEMENTS:

Dans de nombreux équipements, la MASSE (le châssis de l'équipement) est relié à la TERRE. Cette mesure, qui permet de porter la MASSE au potentiel 0 présente les avantages suivants:

V.5.6.1.PROTECTION DES USAGERS CONTRE LES CHOCS ÉLECTRIQUES:

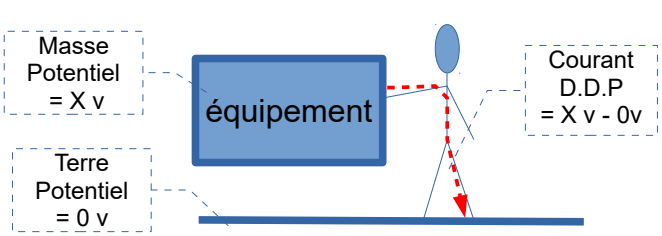
La mise à la terre des masses des équipements permet d'éviter que les personnes amenées, volontairement ou pas, à toucher un élément de la MASSE subissent des chocs électriques.

En général, les opérations de maintenance ou de dépannage des équipements s'effectuent "hors tension". Il existe pourtant des cas où il est nécessaire d'opérer sur des appareils "en tension". C'est le cas, en particulier lorsqu'on procède à une recherche de panne nécessitant la mesure ou la visualisation des signaux de service. Dans ce cas, les personnels opérants sont la plupart du temps en contact avec le SOL (dont le potentiel est proche de celui de la terre) et il est possible qu'ils entrent accidentellement en contact avec la MASSE de l'équipement ou la PHASE de l'alimentation du secteur avec une partie non protégée de leur corps. De ce fait, si les potentiels du sol et de la masse sont très différents, leur corps peut être parcouru par un courant électrique plus ou moins important, pouvant entraîner une électrocution.

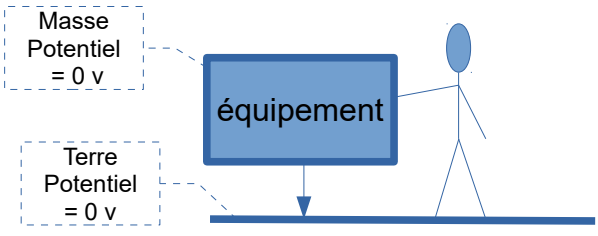
Ce type d'accident peut, bien sûr, concerner n'importe quel usager de l'équipement si les protections constituées par le capot et les isolants des conducteurs sont endommagées.

D'autre part, lorsque plusieurs équipements sont assez proches l'un de l'autre, un usager qui entre en contact avec les deux châssis à la fois peut être parcouru par un courant électrique (même s'il est isolé du sol) si les deux châssis ne sont pas reliés entre eux pour les rendre équipotentiels.

La mise à la terre des châssis permet d'éviter ce type d'accident. Les schémas ci-après mettent en évidence la protection fournie aux usagers de la mise à la terre de la masse:



Masse non reliée à la terre : La masse et la terre peuvent être à des potentiels différents. De ce fait, l'utilisateur qui entre en contact avec la masse peut être parcouru par un courant électrique.



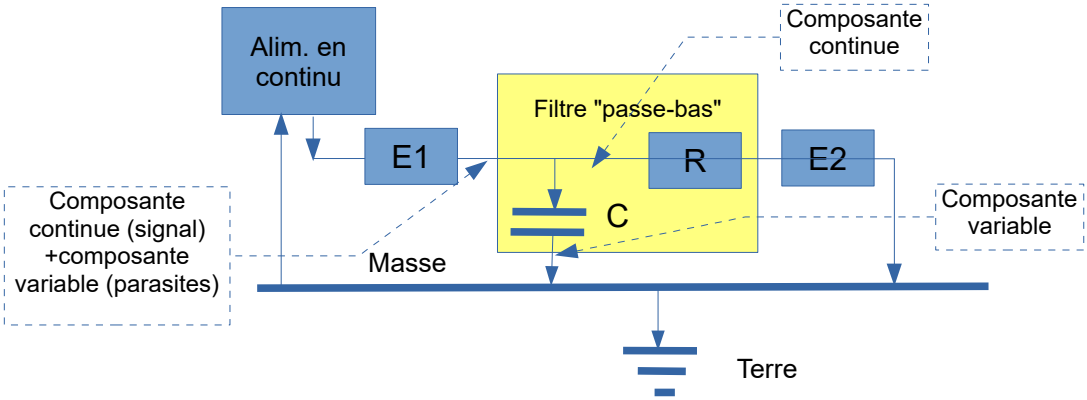
Masse reliée à la terre : masse et terre sont au même potentiel (0). De ce fait, masse et terre sont au même potentiel. Aucun courant ne peut traverser un utilisateur entré en contact avec la masse.

V.5.6.2.ÉLIMINATION DES SIGNAUX PARASITES INDUITS DANS LES CIRCUITS:

La mise à la terre, accompagnée de l'intégration aux circuits de filtres en fréquences permet d'éliminer (ou de réduire fortement) les signaux alternatifs parasites induits dans les circuits de l'équipement par le rayonnement électromagnétique de l'environnement (équipements voisins, fréquences harmoniques des circuits d'alimentation alternatifs, etc.). Par exemple, dans les circuits en courant continu, il suffit d'intercaler entre la masse et la terre un "filtre passe-bas" qui dérive les composantes alternatives vers la MASSE pour éliminer ou fortement réduire celles-ci dans le courant traversant le circuit (à condition que la masse soit reliée à la terre):

EXEMPLE: Soit un circuit alimenté en courant continu est composé des éléments E1 et E2 placés en série. Ce circuit est mis à la masse. Du fait de perturbations d'origine électromagnétique, les courants électriques circulant dans le circuit sont parasités par des courants induits. Or, le fonctionnement de l'élément E2 peut être dégradé par ce type de perturbation.

Pour remédier à ces perturbations, on intercale dans le circuit un "filtre passe bas" dont le but est de dériver vers la terre la "composante alternative" créée par l'induction électromagnétique dûe aux courants de fréquence variable:



Ici, le filtre passe-bas est composé d'une capacité (condensateur C) et d'une résistance R montés en parallèle. Le condensateur ne laisse passer que la composante variable du courant circulant de E1 à E2 alors qu'il bloque la composante continue. La composante variable (parasites) rejoint donc immédiatement la masse, puis se perd dans la terre, alors que la composante continue (signal) traverse la résistance R puis l'élément E2 avant de rejoindre la terre.

Nous voyons donc que la mise de la masse au potentiel de la terre a deux objectifs:

- Éviter les chocs électriques pour les personnes amenées à manipuler ou simplement toucher les équipements sous tension;
- Éliminer les fréquences parasites induites dans les circuits par l'environnement.

V.5.7.BLINDAGE DE MASSE DES CIRCUITS ÉLECTRIQUES:

V.5.7.1.ATTÉNUATION DES RAYONNEMENTS ÉMIS PAR LES CIRCUITS:

Lorsqu'un circuit électriques est parcourus par des courants dont l'intensité est variable dans le temps, ces courants ont tendance à créer un CHAMP MAGNÉTIQUE VARIABLE dans leur environnement.

C'est en particulier le cas des circuits électroniques digitaux qui propagent des signaux électriques pouvant varier à des fréquences très élevées (des centaines de MHZ).

Ces champs électrique variant à des fréquences très élevées produisent des rayonnements magnétiques capables d'induire les circuits voisins. Pour éviter les perturbations entre circuits, une solution est de les BLINDER. Le BLINDAGE DE MASSE est une enveloppe métallique reliée à la masse qui entoure certains circuits électroniques (composants, conducteurs). Il permet de "piéger" dans le blindage les rayonnements émis par le circuit blindé, puis de les évacuer vers la TERRE. Ceci permet d'éviter que le circuit en question ne perturbe les circuits voisins.

V.5.7.2.ATTÉNUATION DES COURANTS INDUITS ISSUS DE L'ENVIRONNEMENT:

D'autre part, le blindage piège les courants induits par les rayonnements issus de l'environnement et les évacue vers la TERRE par un filtre approprié. Il protège ainsi le circuit blindé des perturbations extérieures.

V.5.7.3.UTILITÉ DE LA MISE A LA TERRE:

Nous pouvons constater que pour être efficace, le blindage de masse doit être relié à un réseau de masse électrique, lui-même relié à la terre (sinon, les signaux parasites vont continuer de circuler dans la MASSE).

V.5.8.LES DISJONCTEURS DIFFÉRENTIELS:

Un disjoncteur différentiel est un dispositif de sécurité qui permet de détecter s'il existe une "fuite" de courant dans une installation électrique donnée:

En théorie, dans une installation électrique fonctionnant correctement, l'INTENSITÉ du courant électrique fourni par la PHASE, c'est à dire le nombre d'électrons traversant le circuit, doit être égale à l'INTENSITÉ qui retourne au NEUTRE. En effet, les charges électriques ne sont pas "consommées" par les circuits: c'est seulement leur ÉNERGIE qui est prélevée. De ce fait si une différence existe entre les deux valeurs, c'est forcément qu'une partie du flux d'électrons ne retourne pas au neutre mais "fuit" plutôt vers l'extérieur (vers le SOL, par exemple). Ceci indique:

- Sont qu'un équipement de l'installation est mal isolé;
- Soit que l'équipement concerné est relié électriquement à un autre équipement dont le potentiel électrique est différent (leurs deux masses ne sont pas reliées);
- Soit qu'une personne a provoqué intentionnellement ou non un court circuit en touchant la phase;

Les trois situations, outre le fait qu'elles peuvent provoquer une panne de l'équipement, présentent un danger (potentiellement mortel) d'électrocution;

En comparant constamment les flux électriques entrants et sortants, un interrupteur différentiel permet de détecter ces différences d'intensité et d'éviter leurs conséquences en coupant immédiatement l'alimentation électrique de l'installation.

REMARQUE: *en fait, des différences entre le flux entrant par la phase et celui qui sort par le neutre peuvent apparaître transitoirement lors de certaines actions qui provoquent l'apparition dans les circuits de courants induits (par exemple, le démarrage ou l'arrêt d'un équipement): ces courants induits s'ajoutent ou se retranchent au flux fourni par la phase et modifient l'intensité retournée au neutre. De ce fait, pour éviter les coupures intempestives, les disjoncteurs différentiels sont conçus pour ne réagir que lorsque la différence détectée dépasse un certain seuil (pour les installations domestiques, c'est souvent 30 mA).*

V.6.FOURNITURE DES S.I. EN ÉLECTRICITÉ:

La plupart des Systèmes Informatiques ont pour source principale d'alimentation électrique le réseau public local du pays d'installation. En France, c'est la société Enédis (filiale d'EDF) qui a le monopole de la distribution de l'électricité aux clients des différents fournisseurs. Les exceptions concernent les systèmes qui par leur situation géographique (îles trop éloignées du continent, systèmes embarqués, etc.), ou leurs exigences de sécurité ne peuvent être connectées au réseau public: dans ce cas, elles utilisent des moyens de production qui leurs sont propres.

Les S.I. supportant des fonctionnalités critiques en termes de continuité des services sont souvent équipées d'un système de secours qui leur est propre (avec commutation automatique ou manuelle entre le système principal et le système de secours).

Le système d'alimentation électrique principal et les systèmes de secours doivent, bien sûr, fournir une électricité aux caractéristiques identiques en ce qui concerne les tension, les fréquences et la connexion à la TERRE.

V.7.RAPPELS SUR LES SOLUTION DE SÉCURISATION DES DONNÉE STOCKÉES:

V.7.1.LA TECHNOLOGIE R.A.I.D:

V.7.1.1.PRÉSENTATION GÉNÉRALE:

La technologie logicielle R.A.I.D (Redundant Array of Independent Disks) permet d'opérer une "virtualisation" de l'espace de stockage de plusieurs disques durs. Ceci revient à dire que les espaces de stockage de ces disques vont apparaître pour l'utilisateur sous la forme d'un seul espace de stockage "virtuel". Cette virtualisation permet de répartir les données de chacun des fichiers enregistrés sur plusieurs unités physiques de disques tout en permettant à l'utilisateur de les "voir" comme des espaces d'un seul tenant.

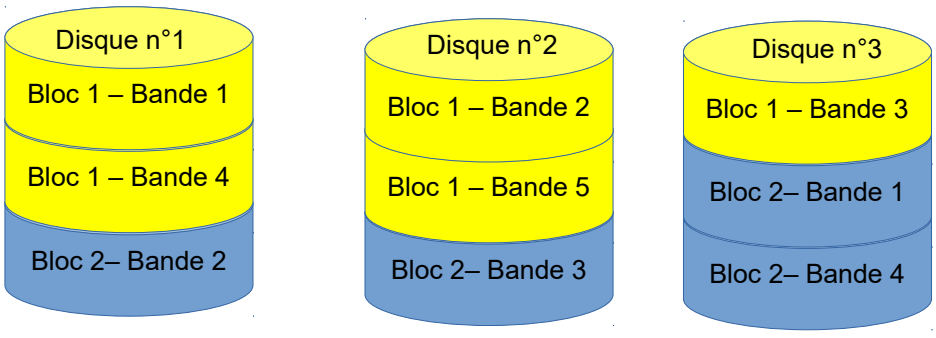
Suivant les "niveaux" de R.A.I.D adoptés, la technologie permet d'améliorer:

- Soit la vitesse d'accès aux données (en permettant la lecture simultanée de plusieurs fragments d'un même bloc par l'utilisation du "stripping");
- Soit la tolérance aux pannes du système de stockage global (en permettant des réplications de données en temps réel et la récupération de données endommagées);
- Soit encore les deux critères en même temps.

REMARQUE: une bonne vingtaine de solutions R.A.I.D existent, certaines étant des combinaisons d'autres solution. Nous n'en présentons ici que 3, parmi les plus caractéristiques:

V.7.1.2.LA SOLUTION RAID 0:

Dans cette solution, les BLOCS de données (les fichiers) sont divisés en BANDES (dans le schéma, le bloc n° 1 est divisé en 5 bandes). Ces bandes sont réparties sur tous les disques gérés par le RAID (ici, 3 disques).



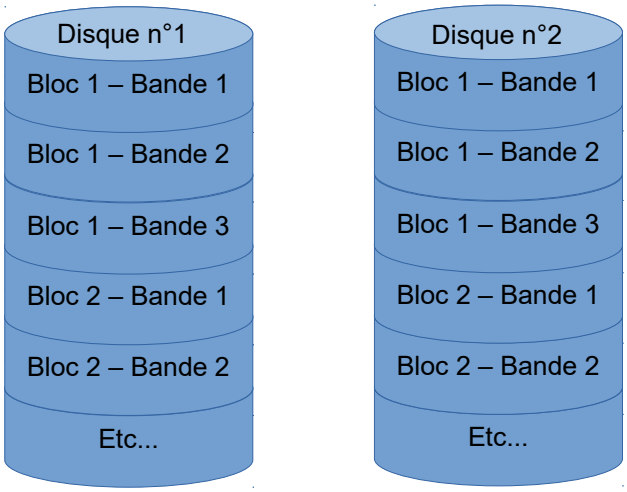
RAID 0 avec 3 disques

Cette technique s'appelle le STRIPPING. Son avantage est de permettre de lire simultanément plusieurs bandes d'un même bloc à partir de plusieurs disques différents, ce qui améliore le temps d'accès aux données. En revanche, le gain de sécurisation est nul par rapport à un seul disque car la défaillance d'un seul des disques du RAID provoque la perte de l'ensemble des données.

V.7.1.3.LA SOLUTION RAID 1:

La solution RAID 1 fragmente également chaque bloc de données (chaque fichier) en BANDES (fragments). Les bandes d'un même bloc sont stockées ensemble sur le même disque et chaque bloc est stocké sur tous les disques du RAID. Toute modification des données effectuée sur l'un des disques est automatiquement répercutée sur les autres disques du RAID. Le RAID 1 permet donc de disposer en permanence d'autant de copies de chaque bloc que le RAID contrôle de disques. Cette fonction est appelée MIRRORING.

L'exemple ci-dessous représente un RAID 1 contrôlant deux disques:



RAID 1 avec 2 disques

AVANTAGES:

- Toute modification apportée aux données du disque n°1 est automatiquement répercutée sur le disque N° 2, et réciproquement. Cette solution (le MIRRORING) permet donc (à la durée de réplication près) de disposer d'autant de copies des données qu'il y a de disques dans le RAID. La solution, qui permet donc de bien sécuriser les données econvient donc bien pour la sauvegarde automatique;
- Les blocs étant "STRIPPÉS", la solution permet d'augmenter la vitesse d'accès au données (comme le RAID 0);

INCONVÉNIENTS:

Il est évident que le RAID 1 n'est pas une solution optimale puisque la capacité totale de l'espace virtuel est égale à la capacité du plus petit des disques en RAID.

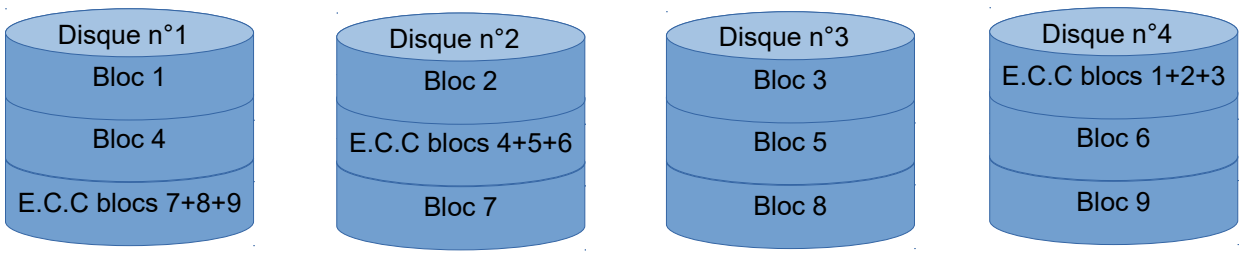
V.7.1.4.LA SOLUTION RAID 5:

Le niveau RAID 5 répartit les BLOCS sur tous les disques du RAID. Pour chacun de ces BLOCS un CODE DE CORRECTION D'ERREURS (En anglais: Error Correction Code ou E.C.C) est élaboré et enregistré dans l'espace virtuel lors de l'écriture.

Lors d'une lecture, l'E.C.C de chaque bloc est recalculé à partir des données du bloc et comparé à l'E.C.C enregistré. Si aucune différence est détectée, cela signifie que les données n'ont pas été altérées. Sinon, la comparaison de la valeur de l'E.C.C avec les données du bloc lues permet dans l'immense majorité des cas de rétablir les données du bloc qui ont été altérées.

Comme les blocs eux-mêmes, les E.C.C de chacun des bloc sont également répartis sur tous les disques disponibles du RAID. Une des restrictions à ce principe est qu'ils ne soient pas enregistrés sur le même disque que le bloc qu'ils représentent: ceci permet d'éviter que le dysfonctionnement d'un disque altère à la fois un bloc et son E.C.C, empêchant ainsi l'autocorrection.

Le schéma suivant donne un exemple de répartition pour un RAID 5 à 4 disques:



RAID 5 avec 4 disques

COMMENTAIRES:

- Le RAID 5 permet d'obtenir des performances en lecture-écriture très proches de celles obtenues en RAI 0, tout en assurant une tolérance aux pannes élevée. C'est un des modes RAID les plus intéressants car il conjugue performance et de fiabilité.
- Cependant, le RAID 5 est surtout intéressant lorsqu'il gère un nombre de disques élevé. Il convient donc aux S.I ayant besoin de beaucoup d'espace de stockage.

V.7.1.5.RAID LOGICIEL ET RAID MATÉRIEL:

Comme son nom l'indique, un R.A.I.D LOGICIEL est un logiciel intégré dans le système d'exploitation d'un équipement qui permet de virtualiser tout ou partie des disques attachés à cet équipement.

Les avantages d'un RAID logiciel sont:

- Un coût de revient très faible: le RAID logiciel est un service intégré (ou intégrables gratuitement) dans les systèmes d'exploitation courants;
- Le nombre de configurations de RAID disponibles n'est pas limité;

Les inconvénients sont:

- Un RAID Logiciel consomme plus de ressources C.P.U qu'un RAID Matériel;

Un RAID MATÉRIEL diffère d'un RAID LOGICIEL par le fait qu'il s'agit d'un composant matériel (carte contrôleur RAID) enfiché dans le BUS d'entrée-sortie de l'équipement et supportant des fonctionnalités analogues à celles d'un RAID LOGICIEL.

Les avantages d'un RAID matériel sont:

- Un RAID Matériel consomme très peu de ressources C.P.U;

Les inconvénients sont:

- Le nombre de configurations de RAID disponibles est forcément limité;
- Les performances sont en général plus faibles que celles d'un RAID logiciel car un contrôleur RAID est la plupart du temps équipé de processeurs inférieurs à ceux d'un ordinateur récent.

V.7.2.LES SERVEURS N.A.S:

V.7.2.1.PRÉSENTATION GÉNÉRALE:

Un N.A.S (Network Attached Storage) est un équipement MATÉRIEL qui héberge une GRAPPE (cluster) d'unités de stockage (disques durs ou S.S.D) et permet de les connecter à un réseau. Vis à vis des hôtes de ce réseau, un N.A.S se comporte comme un SERVEUR DE FICHIER qui leur permet d'accéder (en écriture et en lecture) à tous les supports d'enregistrement de la grappe.

Exemple : Système N.A.S pouvant être équipé de 4 disques.

V.7.2.2.CARACTÉRISTIQUES:

- Un serveur N.A.S peut s'administrer en se connectant à son serveur HTTP interne via un navigateur quelconque depuis n'importe quel poste du réseau;
- Un serveur N.A.S est accessible aux postes clients du réseau pour y stocker ou récupérer des données. Il permet donc la centralisation des données et des sauvegardes. Le dialogue entre les hôtes du réseau et le serveur N.A.S utilise un ou plusieurs des protocoles de transfert de fichiers existants:
  - Common Internet File System (CIFS);
  - Network File System(NFS);
  - Apple Filing Protocol(AFP).
  - File Transfer Protocol(FTP);
  - Etc.
- La gestion centralisée des données sous forme de fichiers permet de faciliter la gestion des sauvegardes des données et de réduire le temps d'administration des postes clients pour la gestion des espaces disques.
- Pour la connexion des disques du cluster, le N.A.S accepte la plupart des connectiques (SCSI, Parallel ATA, SAS, SATA, Fiber Channel).
- La plupart des N.A.S embarquent, en plus du logiciel SERVEUR DE FICHIER et d'un serveur H.T.T.P (interface d'administration), un logiciel R.A.ID qui permet de virtualiser l'ensemble des espaces disques sous la forme d'un seul espace et de sécuriser les données stockées contre la défaillance d'un ou plusieurs disques durs. Le R.A.I.D peut être administré et paramétré via l'interface d'administration;
- Certains N.A.S permettent de remplacer "à chaud" un disque devenu défectueux. Si ce disque fait partie d'un R.A.I.D permettant la régénération automatique des données (exemple: RAID 1),

ce mécanisme peut être suivi de la reconstitution du contenu du nouveau disque à partir de son disque MIROIR.

V.7.2.3.SAUVEGARDE DE DONNÉES:

La sauvegarde de données étant l'une des utilisations principales des N.A.S, ceux-ci sont équipés de dispositifs de sécurisation renforcés: alimentation électrique très fiable et pouvant être redondante, sécurisation des accès par mots de passe, possibilité de remplacer à chaud un disque défaillant avec régénération de son contenu sur le nouveau disque, etc.

De ce fait, l'implantation d'un disque de sauvegarde dans un N.A.S connecté au réseau local permet d'éloigner le support de sauvegarde du support à sauvegarder tout en sécurisant le fonctionnement du support de sauvegarde.

Cependant, l'implantation conjointe dans un N.A.S d'un support de stockage et de son support de sauvegarde n'est pas forcément une bonne solution pour la sécurité, car les deux supports peuvent être dégradés simultanément lors d'un dysfonctionnement du N.A.S.