LES DOSSIERS TECHNIQUES

Sécurité des Salles Serveurs

-

Critères et Contraintes de Conception

6 février 2009

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Table des Matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la révision de ce document, tout particulièrement :

Robert	*BERGERON*	**Capgemini**
Jean-François	*CAPELLE*	**UTE**
Muriel	*COLLIGNON*	**IBM**
Guy	*KHOUBERMAN*	**Retraité de l'ACOSS**
Gérard	*PETITIT*	**GRAS-SAVOYE**
Alain	*POLACH*	**Retraité du CNPP**
Alexandre	*STANURSKI*	**Rittal**

Ainsi que les membres du comité de relecture.

1. Introduction

Ce document est destiné à toutes personnes impliquées dans l'aménagement ou le réaménagement de salles serveurs et décrit les critères et les contraintes de conception.

Le document comprend trois chapitres principaux et trois annexes :

- Un chapitre « Projet » qui développe la marche à suivre et les responsabilités de chacun des acteurs.
- Un chapitre « Conception » qui décrit les besoins, les contraintes relatifs au choix du site aux aménagements intérieurs ainsi que les règles et procédures de sécurité.
- Un chapitre « Maintenance et évolutions » qui traite des évolutions non seulement des équipements mais aussi de la législation et de la réglementation.
- Les annexes comprennent des « Fiches Pratiques » qui précisent, par famille de risques, les causes, les conséquences et les parades. Elles constituent un support aux analyses de risques et aux choix de solutions.

Ce document est un canevas général qui couvre l'aménagement ou le réaménagement de salles serveurs. Il facilite le dialogue avec les spécialistes de chaque domaine, auxquels il est préférable de faire appel pour ce type de projet.

2. Le projet

2.1 Facteurs déclenchant

La décision de lancer un nouveau projet de construction ou de réaménagement d'un centre informatique ou de salles serveurs peut avoir de nombreuses origines.

Dans tous les cas, le Responsable de la Sécurité des Systèmes d'Information (RSSI) doit être attentif aux différents événements déclenchant qui pourraient avoir un impact sur les systèmes d'information. (Déménagement ou réaménagement des locaux). Il doit intervenir le plus en amont possible et être impliqué dans les projets et décisions stratégiques.

2.1.1 Facteurs indépendants de la gestion des systèmes d'information

Les facteurs indépendants peuvent être externes ou internes à l'entreprise ou à l'organisation concernée, mais n'interviennent pas dans le périmètre de gestion et de décision du DSI ou du RSSI.

Les principaux facteurs de ce type sont dépendants de la stratégie d'entreprise :

- Nouvelle politique interne de l'entreprise.
- Fusion d'entreprises ou restructuration.
- Externalisation.
- Création d'un nouveau site.
- Création d'entreprise.
- Décentralisation.
- Délocalisation.
- Déménagement.

Cette évolution de la stratégie d'entreprise peut être orientée par :

- Des décisions administratives, des réglementations et des lois telles que :
  - L'expropriation ou le réaménagement du territoire peuvent déboucher sur un déménagement.
  - Des problèmes environnementaux, tels que le bruit, la pollution peuvent également amener des décisions administratives de cessation d'activités sur le site.
- Des contraintes externes. (fin de bail, voisinage agressif, plaignant, etc.).
- Des facteurs économiques. (prix du m², opération immobilière, ROSI[1], etc.).
- Un sinistre important.
  Un sinistre qui nécessite la reconstruction totale ou partielle du site.

[1] Cf : le document CLUSIF : « Retour sur Investissement en Sécurité des Systèmes d'Information : Quelques clés pour argumenter »

- Contraintes environnementales connues (sous-sols instable, risque de crues, risques sismiques, etc.).
- Les évolutions de l'environnement de l'entreprise en dehors de son contrôle et génératrices de risques.
  - implantation d'une activité à risque dans le voisinage,
  - réhabilitation d'un quartier ou d'une zone d'activité,
  - modifications des sols pouvant entraîner des mouvements de terrains,
  - etc.
- Une prise de conscience ou augmentation d'un risque "externe" important perçu par l'entreprise.

2.1.2 Facteurs liés à la gestion des systèmes d'information

Les facteurs liés à la gestion des systèmes d'informations font partie intégrante du périmètre de gestion et de décision du DSI ou du RSSI. Cependant, la prise en compte de ces facteurs n'échappe pas à l'étude des contraintes associées au projet d'entreprise (priorité d'investissement, facteurs indépendants, etc.).

Les principaux facteurs de ce type sont :

- Décisions administratives, réglementations et lois (environnement, sécurité des personnes, etc.).
- Plan directeur informatique dégageant la nécessité de procéder à de nombreuses améliorations des systèmes.
- Etablissement du plan de secours (nouvelle salle, salle de management en cas de crise).
- Résultats d'un audit destiné à évaluer les performances des salles ou leur niveau de sécurité.
- Décision de changement de matériel (Obsolescence, arrêt de la maintenance, etc.).
- Un changement ou évolution (technologie, taille, etc.) des systèmes.
- Contraintes internes (besoin accru de confidentialité, de disponibilité, de fiabilité et de continuité de service, etc.).
- Conditions de travail inadaptées.
- Changement d'architecture des systèmes d'information.
- Regroupement de moyens informatiques.
- Externalisation des moyens informatiques.
- Etc.

2.2 Diagnostic et décision

Un diagnostic préalable est nécessaire pour prendre en compte l'organisation, les flux, les incidents et les dysfonctionnements. Pour que ce diagnostic soit pertinent, il est nécessaire de prendre en compte, outre l'existant, les missions et contraintes des futures salles serveurs.

2.2.1 Constat de l'existant

Ce constat doit mettre en évidence, pour chacune des activités de traitement de l'information, les éventuelles anomalies ou insuffisances actuelles de fonctionnement ou d'organisation (par exemple sur le plan de l'efficacité, du coût, de la qualité). Il doit prendre en compte les améliorations attendues, et les dispositions concrètes à mettre en œuvre.

Cette analyse doit concerner :

- La protection des personnes.
- La protection des biens matériels et immatériels.
- L'adéquation des locaux (vétusté, implantation, etc.).
  - l'architecture globale des bâtiments et la position des salles au sein des bâtiments,
  - les contraintes structurelles (emplacement, confinement, confidentialité, réglementation),
  - l'analyse de l'adéquation entre l'objectif de disponibilité et les installations techniques existantes. (Climatisation, alimentation électrique, systèmes de détection incendie, d'extinction, parafoudre, résistance des faux-planchers, etc.),
  - l'analyse de l'adéquation entre les objectifs de sécurité de l'information et l'existant (contrôle d'accès, détection d'intrusion, etc.),
  - les besoins propres aux études, au développement et à la maintenance des applications (séparation des environnements, télémaintenance, etc.).
- Le fonctionnement du système d'information.
  - l'historique et la nature des incidents,
  - les diagnostics sur les coûts de fonctionnement et d'exploitation,
  - l'exploitation des systèmes et des réseaux.
- L'organisation et les procédures.
- Les nouveaux besoins identifiés.

Cette analyse, une fois réalisée, aboutit au recensement des risques existants et à la prise en compte du retour d'expérience (ex. incidents vécus).

Dès la conception des salles, les besoins en personnel doivent être anticipés de façon à déterminer les recrutements et les formations nécessaires à la mise en exploitation future.

2.2.2 Orientations principales du projet

Différentes options peuvent influencer fortement le déroulement du projet :

- Le (ou les) facteur(s) déclenchant va (vont) induire différents scénarios :
  - modification du centre existant,
  - extension du centre existant,
  - regroupement logique de serveurs ou virtualisation des systèmes d'information,
  - déménagement vers un autre centre déjà aménagé ou à aménager,
  - création d'un nouveau centre dans un immeuble existant,
  - création d'un centre de toutes pièces.

- Le choix de l'option de la propriété pleine et entière ou celui de la copropriété (hébergement dans un site ou un immeuble existant) ou encore celui de la simple location va impacter la liberté de manœuvre.
- La décision de faire appel ou non à des collaborations externes (voir liste ci–après) est également importante et il conviendra d'en arrêter le degré d'implication et de préciser très clairement leur mission. L'efficacité de ces collaborations sera d'autant plus grande qu'elles interviendront tôt dans le processus d'élaboration du projet.
- Le Responsable de la Sécurité des Systèmes d'Information (RSSI) doit être impliqué dès le début du projet.

2.2.3 Décision (nouveau site, réaménagement, etc.)

En fonction de l'analyse de l'existant et de la prise en compte des facteurs déclenchant, la décision peut être :

- Réaménagement des locaux existants.
- Aménagement d'une nouvelle salle.
- Déménagement vers de nouveaux sites.
- Externalisation.
- Délocalisation.

2.3 Organisation du projet

La démarche décrite ci-après sera sensiblement la même pour la construction d'un nouveau bâtiment à usage informatique ou pour l'aménagement d'un ou plusieurs locaux existants. Certaines des étapes décrites pourront alors se révéler sans objet.

De manière très concrète, voici la démarche synthétique qui peut être adoptée pour organiser et dérouler un projet de conception, réalisation ou de réaménagement d'un centre informatique ou d'une salle serveurs. Nous recommandons que le responsable de la sécurité soit impliqué dans toutes les phases du projet.

- Recensement de tous les acteurs.
- Définition d'objectifs clairs en termes de capacité, de continuité de service et de sécurisation du futur site ou de la future salle, les traduire sous forme de cahier des charges techniques.
- Recensement des risques et des parades associées à mettre en œuvre pour respecter les besoins exprimés y compris ceux de la sécurité (Via une analyse de risques).
- Choix du mode de réalisation (Maîtrise d'œuvre (MOE) ou Clé En Main (CEM)), les termes sont explicités en annexe.
- Elaboration d'un avant-projet puis d'un projet.
- Validation du projet.
- Consultations.
- Lancement de la réalisation.

- Suivi de la réalisation, en particulier le responsable sécurité doit veiller au maintien de la sécurité des informations pendant les travaux, surtout en cas de réaménagement.
- Gestion des aménagements apportés au projet en cours de réalisation (surtout sur les projets de longue durée).
- Mise à jour des consignes de sécurité si nécessaire.
  - incendie,
  - contrôles d'accès et surveillance vidéo avec éventuelle demande d'autorisation à la CNIL (Commission Nationale Informatique et Libertés) ou aux autorités,
  - etc.
- Réception des travaux.
- Déménagement ou aménagement du site (vérifier la présence de clauses de responsabilité dans les contrats de maintenance pour le déménagement des matériels).
- Mise en place de la gestion technique du site (maintenance, procédures et consignes, gestion technique centralisée, etc.).
- Mise en production et suivi durant l'année de parfait achèvement.

2.3.1 Les phases du projet

Les différentes phases de l'organisation et du déroulement chronologique de la conception – réalisation sont principalement les suivantes:

Phase Expression des besoins / programme

- Expression des besoins et contraintes du maître d'ouvrage des systèmes d'information.
- Reformulation et traduction en termes de bâtiment technique.
- Validation.

Phase Faisabilité

- Evaluation de la faisabilité du projet au regard de l'implantation ou des locaux envisagés y compris les contraintes environnementales.
- Réorientation éventuelle du projet.

Phase Esquisse / avant projet sommaire

- Choix du type de réalisation (MOE ou CEM).
- Proposition de MOE avec honoraires ou lancement d'une consultation en conception-réalisation.
- Dimensionnements principaux du projet (surfaces, puissance, redondance, évolution, etc.).
- Création du plan sommaire et architecture des locaux.
- Pré-dimensionnement des différents locaux et volumes.
- Description sommaire des aménagements envisagés.
- Etablissement du budget prévisionnel global.

- Réalisation du macro-planning.
- Validation.

Phase Avant projet détaillé / Projet

- Choix du type de réalisation (MOE ou CEM).
- Etudes spécifiques préliminaires (sol, environnement, etc.).
- Sollicitation des différents organismes de contrôle et bureau d'études externes (Sécurité et Protection de la Santé, contrôle technique, acousticien, structures, fluides, etc.).
- Planification détaillée.
- Mise au point des partenariats externes nécessaires.
- Description et plans détaillés du projet.
- Intégration de la capacité de maintenance et de la gestion technique des installations dès cette phase.
- Etablissement du budget poste par poste.
- Proposition CEM ou finalisation du dossier d'appels d'offres.
- Validation.

Phase Consultations et choix des entreprises

Selon le mode de réalisation, cette phase sera conduite en interne ou par un MOA ou ensemblier externe.

- Elaboration et communication des cahiers des charges de consultation.
- Consultation des différentes entreprises.
- Dépouillement et recadrage des offres.
- Choix des entreprises avec contrôle des certifications.

Phase lancement réalisation

- Lancement des études d'exécution avec le Maître d'œuvre et les entreprises retenues.
- Mise en place de la cellule de synthèse du projet.
- Choix de la coordination des travaux, identification des acteurs et interlocuteurs.
- Préparation et mise en place du chantier (réunion préalable à l'ouverture du chantier, Plan Particulier de Sécurité et de Protection de la Santé (PPSPS), inspection commune, planification et découpage en phases détaillées, panneau de chantier, plan de chantier, constats divers, etc.)
  Le responsable sécurité veillera à maintenir un niveau de sécurité compatible avec les exigences de sécurité : mise en place de mesures compensatoires liées au caractère exceptionnel des travaux.
- Planification des différentes réunions de chantier et de pilotage.
- Mise en place des installations de chantier.

Ce qui incombe notamment au Maître d'Ouvrage (avec l'assistance du Maître d'œuvre) :

- Dépôt du permis de construire.
- Interface avec le bureau de contrôle.
- Coordination de la sécurité.

- Déclaration d'installation classée.
- Déclaration d'ouverture de chantier.
- Déclarations diverses (CNIL, préfecture, etc.)
- Demandes de branchements (électricité, eau, gaz, téléphone, etc.)

Phase réalisation

- Lancement des travaux.
- Prise en compte des recommandations faites dans les chapitres suivants et dans les fiches de risques.
- Pilotage du chantier (les membres du comité de projet).
- Suivi hebdomadaire de chantier avec les entreprises, constitution du dossier photographique des réseaux cachés.
- Gestion des modifications apportées au projet en cours de réalisation.
- Préparation du dossier de réalisation des essais, tests et opération de réception.

Phase réception

- Réalisation des tests et essais.
- Collecte des Dossiers des Ouvrages Exécutés (DOE).
- Contrôle de la mise en place des équipements et liaisons de sécurité.
- Réception avec ou sans réserves.
- Obtention du certificat de conformité sans réserve des organismes de contrôle.
- Levée des réserves si possible avant l'emménagement.
- Formation des futurs exploitants du site.
- Quitus aux entreprises.

Phase mise en production

- Mise en production des dispositifs de sécurité du site.
- Visites réglementaires (pompiers, assureurs, Commission Hygiène, Sécurité et Conditions de Travail (CHSCT), etc.)
- Emménagement des matériels.
- Tests de fonctionnement des matériels.
- Emménagement des personnels.

Période de garantie

- Selon qu'il s'agit d'une construction neuve ou d'un réaménagement, la période de garantie doit suivre la législation en vigueur.

Remarque importante:

Compte tenu de leur complexité, ces différentes phases du projet doivent être accompagnées voire conduites par un Maître d'Œuvre expérimenté dans ce type de projet (interne ou externe).

Une assistance à Maîtrise d'ouvrage spécialisée pour les phases de programmation puis pour l'accompagnement ultérieur sera sans doute également souhaitable voire nécessaire.

2.3.2 Différents acteurs / Fonctions

2.3.2.1 Attribution des rôles

Il est indispensable, pour le bon déroulement du projet, de préciser les rôles, attributions et responsabilités des différents acteurs : qui est responsable de quoi ? Qui est l'interlocuteur de qui ? Qui assiste aux différentes réunions ? Comment la communication sera organisée entre les différents acteurs ?
Simultanément, dans le cadre de la construction d'un centre sécurisé, on peut également recommander instamment la mise en pratique, par les différents acteurs, des concepts d'Assurance Qualité. La construction d'immeuble s'accompagne de plus en plus souvent de la mise en place de plan d'Assurance Qualité par les différents intervenants.

De manière générale, un tel projet requiert la mobilisation et la participation de la plupart des fonctions de l'entreprise voire de fonctions externes à l'entreprise notamment en terme d'expertise et de réalisation.

2.3.2.2 Acteurs / Fonctions de l'entreprise

Les fonctions qui seront associées au déroulement et à la validation des principales étapes du projet, constitueront la base du Comité de Suivi de projet.

Fonction direction générale

La Fonction direction générale prend les décisions et effectue les inévitables arbitrages entre les autres fonctions de l'entreprise. Elle représente ou se fait assister par les fonctions juridiques (contrats, réglementation, assurances..), économiques (négociation, achats, ..), financières (budgets, financement,..) et organisationnelles de l'entreprise.
C'est le pouvoir de décision et, par définition, le *Maître d'ouvrage*.

Cette maîtrise d'ouvrage sera la plupart du temps déléguée, soit à un cadre de l'entreprise, soit à la fonction « immobilier » ou informatique, soit à une société externe (besoin d'expertise complémentaire)

Ce *Maître d'ouvrage délégué* aura le pilotage du comité de suivi de projet qui constitue, de fait, la véritable équipe de maîtrise d'ouvrage.

La Fonction Systèmes d'Information

La fonction Systèmes d'information a un rôle capital puisqu'elle doit :

- Préciser l'expression de ses besoins, contraintes et objectifs (*cahier des charges*), notamment en matière de disponibilité et niveaux de services attendus. Le cahier des charges devra contenir la liste exhaustive des matériels à héberger avec leurs principales caractéristiques : dimensions, poids, puissance électrique, type d'alimentation (nombre de prises, format, ampérage), dissipation, nombre de prises réseau. Cette liste sera indispensable pour définir le nombre et l'implantation des baies et dimensionner les utilités (climatisation, électricité, câblage).
- Valider la prise en compte de ces besoins dans le cahier des charges du projet.
- Vérifier que le cahier des charges est respecté pendant tout le cycle de vie du projet.

- Assurer la continuité de la production pendant les travaux (si nécessaire).
- Préparer et conduire les déménagements de matériels informatiques.
- Participer au pilotage et à la coordination du projet.
- Participer à l'analyse de risques.
- Participer à la réception de la fin des travaux.

En particulier, elle doit prendre en compte tous les problèmes d'interfaces entre la fonction Système d'Information et les différentes fonctions utilisatrices. Cet aspect revêt une acuité toute particulière si le site informatique est séparé physiquement du reste de l'entreprise.

Notamment, dans le cas de projets de type "réaménagement" de salles où l'exploitation continue, c'est fréquemment le Responsable de la Fonction Systèmes d'Information qui est amené à assumer la fonction de Maître d'ouvrage délégué en l'absence de la fonction « immobilier » (Cf. plus loin).

La fonction « immobilier » ou les services généraux

Lorsque la fonction « immobilier » ou services généraux existe, c'est à elle que revient logiquement la délégation de maîtrise d'ouvrage. Elle est également associée en amont au choix des options propriété/copropriété / location, etc.).

Il convient cependant de prendre garde au caractère particulier de cette construction et de ne pas sous-estimer les spécificités des systèmes d'information et la complexité technique d'un tel projet. La fonction « immobilier » doit s'entourer des expertises nécessaires.

Elle traite notamment les aspects suivants:

- La prise en compte des besoins exprimés par les fonctions Système d'Information et Sécurité.
- La prise en compte des contraintes réglementaires et légales.
- Le choix des entreprises pour la construction ou les aménagements.
- La participation au projet conjointement avec les fonctions Systèmes d'Information et Sécurité.
- La gestion de l'avancement des travaux au jour le jour.
- Le respect et le contrôle des procédures de sécurité pendant toute la durée des travaux.
- L'organisation des déménagements des matériels informatiques en étroite collaboration avec la fonction Systèmes d'Information.
- La participation à la réception des travaux.

Les fonctions métier

Les fonctions métier recouvrent les responsabilités de chaque secteur d'activité de l'entreprise.

La consultation des fonctions métier garantit la prise en compte des besoins et contraintes des utilisateurs dans le cadre de la conception et de la mise en œuvre du projet (Arrêt d'exploitation, localisation du site, etc.).

La fonction sécurité.
La fonction sécurité recouvre :

- La sécurité des biens et des personnes.
- La sécurité du Système d'Information.
- La protection de l'environnement.

Elle est particulièrement importante et nécessaire sur un tel projet pour lequel la sécurité constitue un des pré-requis de la conception.

Elle doit notamment :

- Conduire l'analyse de risques.
- Exprimer ses besoins et contraintes en sécurité.
- Vérifier la sécurité des conditions de travail.
- Veiller à maintenir la sécurité des informations efficace pendant les travaux.
- Participer à la réception des travaux sur les aspects sécurité.
- Contrôler les personnels (interne et externe) travaillant sur le projet.
- Vérifier que les mesures imposées par les contraintes réglementaires sont bien prises en compte et appliquées.

La fonction ressources humaines.
Dans ce cadre, la fonction ressources humaines a pour rôles principaux :

- La vérification des conditions de travail.
- La liaison avec les partenaires sociaux.
- La participation à la validation des accès physiques.
- Le respect du contrat de travail (en cas de déplacement du site…).

Les partenaires sociaux (CE, CHSCT).
Les meilleures chances de ne pas nourrir un conflit source de retard résident dans leur implication, très tôt, dans le projet.
Par exemple, si ce dernier implique un déménagement, il faut prendre en compte rapidement les aspects sociaux : transport, restauration, etc. De même, les partenaires sociaux doivent être associés à la détermination de nouvelles conditions de travail éventuellement imposées par des contraintes de sécurité plus draconiennes.

Fonction Chef de projet.
La Fonction Chef de Projet est essentielle à la réussite du projet.
Le Chef de Projet est le garant de la méthodologie employée, de la maîtrise du déroulement et de la validation des différentes étapes, du respect de la planification, des coûts et des objectifs. Il doit savoir s'entourer des expertises nécessaires internes ou externes.

C'est le pilote et le chef d'orchestre du projet.

2.3.2.3 Acteurs externes

Le choix de ces acteurs dépend de la nature et du contexte du projet. La liste ci-après n'est pas exhaustive. Des circonstances particulières peuvent en effet conduire à faire appel à des partenaires très spécialisés.

Les principaux acteurs externes sont les suivants :

- Promoteur, aménageur ou propriétaire.
- Investisseurs.
- Maître d'ouvrage délégué (éventuellement).
- Bureaux de contrôle.
- Cabinet de Coordination Chantier.
- Cabinet(s) de conseil spécialisé(s).
- Architecte.
- Maître d'œuvre.
- Bureaux d'études.
- Assureurs.
- Interlocuteurs liés à l'environnement réglementaire (élus locaux -permis de construire, installations classées-, pompiers, etc.).
- Opérateurs de communication, les fournisseurs d'énergie, les messageries, etc.
- Services départementaux (voirie, DDE, pompiers, service des eaux, les collectivités locales, les conseils généraux, etc.).
- Le syndic de l'immeuble ou de parc d'activités (éventuellement).
- Constructeurs (entreprise générale, ensemblier, etc.).
- Fournisseurs de matériels informatiques et d'équipements techniques.
- Les déménageurs.
- Sous-traitants techniques.
- Réalisateurs des travaux.
- Coordonnateur SPS (coordonnateur en matière de Sécurité et de Protection de la Santé sur les chantiers).
- Etc.

2.3.2.3.1 Maîtrise d'œuvre

Le Maître d'œuvre est l'architecte du projet mandaté par le maître d'ouvrage. Son rôle est de superviser le projet aussi bien dans sa phase de conception que dans sa phase de réalisation : il s'agit alors de maîtrise d'œuvre de conception et/ou de réalisation.

Ces deux phases peuvent être distinctes mais le plus souvent elles sont réalisées par le maître d'œuvre pour assurer la cohérence de projets aussi complexes.

En raison de la teneur spécifique et très technique des projets de réalisation de salles serveurs, le maître d'œuvre est le plus souvent un spécialiste expérimenté du domaine.

Au sens de la loi MOP (Loi n° 85-704 du 12 juillet 1985 - relative à la maîtrise d'ouvrage publique et à ses rapports avec la maîtrise d'œuvre privée. (Loi MOP) et Ordonnance n° 2004-566 du 17 juin 2004 - portant modification de la loi n° 85-704 du 12 juillet 1985 relative à la maîtrise d'ouvrage publique et à ses rapports avec la maîtrise d'œuvre privée), le rôle du maître d'œuvre est strictement encadré.

Démarche

Il s'agit d'une démarche classique tripartite maître d'ouvrage / maître d'œuvre / entreprises qui permet de séparer clairement les rôles de chacun durant toutes les phases du projet, de la conception à la réception des ouvrages.

Les contrats sont directement établis entre le maître d'ouvrage et les entreprises.

Conception-réalisation
En général, le choix s'oriente vers un prestataire unique pouvant effectuer aussi bien les prestations de conception que de réalisation de l'ouvrage en ingénierie intégrée.

Les avantages de ce choix sont :

- Un gain de temps.
- Une maîtrise des coûts et des délais.
- Une simplification contractuelle.
- Une meilleure cohérence du projet entre la conception et les techniques mises en œuvre.

Les points à surveiller sont :

- La qualité qui peut éventuellement passer après l'intérêt économique du concepteur-réalisateur.
- Les compétences techniques du maître d'ouvrage pour apprécier la pertinence des solutions proposées.

Critères d'évaluation des acteurs externes

- Démarche projet.
- Démarche qualité.
- Pérennité des acteurs externes (assise financière, solvabilité, etc.).
- Expérience.
- Compétences.
- Références vérifiables par des visites sur site.
- Quantité et qualification des ressources (conception, réalisation).
- Choix de sous-traitances.

Cellule de synthèse
Dans un tel projet complexe et à forte valeur ajoutée technique, il est conseillé de mettre en place une cellule de synthèse dont le rôle est de valider la cohérence des différents lots techniques et leur synchronisation.

Cette cellule est la garante du respect de la qualité, des coûts et des délais. Elle est soit intégrée soit externe à la maîtrise d'œuvre.

2.3.2.3.2 Assistant spécialisé à maître d'ouvrage

Son rôle est d'assister le donneur d'ordre en lui apportant les connaissances techniques spécialisées pour apprécier la complexité d'un tel projet. L'assistant conseille le maître d'ouvrage vis-à-vis du maître d'œuvre ou du concepteur-réalisateur, de l'étude de faisabilité jusqu'à la réception des ouvrages, voire lors de la phase de mise en service.

3. Conception

3.1 Besoins, contraintes et éléments d'aménagement

Les besoins et contraintes de conception sont liés aux flux et à la criticité des activités qui conditionneront le niveau de sécurité des lieux.

3.1.1 Analyse des flux

L'analyse préalable des flux doit permettre d'étayer ultérieurement l'organisation physique du centre. Cette analyse doit porter sur :

Les flux physiques :

- Analyse des passages de câbles, des canalisations et des différentes gaines (alimentation électrique, gaz et liquides, réseaux courants faibles - alarmes techniques, détection incendie, surveillance -, réseaux data – cuivre et fibre otique – pour lesquels il faut prévoir des points de pénétration, gaines et chemins de câbles adéquats et exploitable - capacité, rayons de courbure -, etc.).
- Circulation des documents de saisie (bordereaux, etc.).
- Lieu de stockage et de consommation des fournitures.
- Circulation des documents édités (listings, mailings, etc.).
- Circulation et transports des supports de sauvegarde.
- Circulation des matériels (résistance du faux-plancher).
- Accès aux locaux : rôle du quai de chargement et déchargement pour les livraisons (accès des camions), voiture du personnel, voiture des visiteurs.
- Evacuation des poubelles (contenant des informations confidentielles ou non).
- Etc.

Les flux logiques :

- Communication entre les éléments du système.
- Communication avec d'autres systèmes du site.
- Communication avec l'extérieur du site.
- Etc.

Les flux humains :

- Accès et circulation des différentes catégories de personnel du centre.
- Fonctions nécessitant l'accès de personnels extérieurs au centre.
- Idem pour les personnels extérieurs à l'entreprise.
- Etc.

Cette analyse des flux est importante, notamment sur le plan de la productivité (limitation de la complexité) et de la sécurité (par exemple, vérification de la capacité à fiabiliser et sécuriser les chemins majoritaires, recherche d'un cloisonnement "stratifié" (par couches) ou "concentrique", etc.).

3.1.2 Choix du site (déménagement ou réaménagement)

Le choix du site sera fondé sur des critères économiques ou politiques et sur les résultats de l'analyse de risques prenant principalement en compte les critères suivants :

- Les risques industriels et environnementaux.
- Les risques naturels.
- Les risques socio-économiques et socio-culturels.

Les risques industriels et environnementaux

- Pollution et explosif.
  - vérifier qu'un site en classification SEVESO II n'existe pas à proximité. *(Voir URL Internet dans l'annexe bibliographique)*
- Aéronautique.
  - proximité d'une zone aéroportuaire,
  - alignement par rapport aux pistes,
  - etc.
- Transport possible de substances dangereuses selon l'environnement industriel.
  - proximité d'une route à fort trafic,
  - proximité d'une voie de chemin de fer, d'une gare de triage,
  - proximité d'un canal, d'un appontement,
  - proximité d'un port,
  - proximité d'un oléoduc ou d'un gazoduc,
  - etc.
- Nucléaire.
  - centrale,
  - pollution radioactive,
  - etc.
- Chocs mécaniques.
  - vibrations induites par le passage des avions,
  - vibrations dues au passage des camions, des trains, du métro,
  - proximité d'une carrière,
  - etc.
- Acoustique.
  - proximité d'un environnement ou d'un lieu bruyant.
- Electrique et Electromagnétique.
  - barrages hydrauliques,
  - passage d'une ligne à haute tension,
  - proximité d'antennes,
  - etc.

Les risques naturels :

- Risques météorologiques.
  - lieu de tempêtes fréquentes,
  - couloir d'avalanche,
  - inondations,

- sécheresse,
- incendie : feux de forêt,
- zone à indice kéraunique élevé,
- etc.

- Mouvements mécaniques de terrain :
  - coulée de boue,
  - sécheresse des sols,
  - réhydratation des sols,
  - affaissement dû à des grottes ou zones creuses,
  - sismicité ou volcanisme,
  - action des vagues,
  - etc.

Les risques socio-économiques et socio-culturels.

- Chemins réguliers de manifestations.
- Prise en compte de l'environnement social et culturel.
- Etc.

3.1.3 Implantation des locaux

Le choix de l'emplacement de la salle serveur dans le bâtiment est délicat, il convient de prendre en compte :

- Les contraintes des infrastructures des bâtiments dans le cas d'une copropriété (propriétaire ou locataire).
- Les conditions environnementales (vibrations, pollution, poussières, rayonnements, explosion, incendie, inondations, foudre, bruits, etc.).
- La proximité d'une zone accessible au public dans le bâtiment.
- L'accessibilité pour les intervenants (fournisseurs, maintenance des matériels, personnel, livraisons, visiteur, etc.).
- La dimension de la salle.
- Les lieux de stockage (matériels, consommables, etc.).
- Le lieu de stockage des médias.
- L'emplacement des locaux techniques et les liaisons avec la salle.
- Les alimentations de la salle (électrique, télécommunication, etc.).
- L'environnement climatique de la salle.

Pour prendre en compte les points ci-dessus, il convient de :

- Prendre en compte la réglementation légale (immeuble de grande hauteur, établissement recevant du public, établissement à régime restrictif, etc.).
- Analyser, dans le cadre d'une copropriété, le règlement, et identifier les points bloquants éventuels, s'informer sur les nuisances possibles dues aux autres occupants.
- Choisir l'emplacement de la salle de telle façon qu'elle ne soit pas dans une zone accessible au public ou visible de l'extérieur, et éviter un fléchage indiquant sa situation.
- Eviter les sous-sols (risques d'inondation), les salles sous terrasses (risques d'infiltration), les rez-de-chaussée (facilité d'intrusion), les étages élevés (difficulté d'accès). Il est également conseillé de compartimenter les locaux et de ne pas mettre

dans le même local l'ensemble des équipements (serveurs, équipements de télécommunication, équipements de type onduleurs, imprimantes, etc.).

- S'assurer qu'il n'y a pas de risques d'inondation dans les gaines techniques ou en provenance des étages supérieurs (canalisations, sanitaires, appareils ménagés alimentés en eau sous pression, etc.).
- Prendre en compte les contraintes liées à l'installation des réseaux locaux (répéteurs, etc.).
- Choisir un emplacement qui facilite l'accès (notamment pour l'installation des machines : hauteur sous-plafond, dimension des portes) et le contrôle des intervenants. (contrôle d'accès, pas d'accès donnant sur une zone non contrôlée, largeur des couloirs, des portes, etc.). Limiter les interventions dans la salle serveurs par la mise en place de couloirs techniques y attenant.
- S'informer sur la résistance au sol pour l'installation des machines.
- S'assurer que les chemins d'accès qui mènent à la salle et la salle elle-même supportent le poids des machines.
- S'assurer que les chaînes techniques aient un niveau de sécurité compatible avec celui requis pour la salle. En particulier, s'assurer du niveau de sécurité des chemins de câbles, des canalisations et des équipements techniques, notamment de copropriété.
- Envisager la redondance des alimentations (électriques, télécommunications, etc.).
- Prévoir une centralisation des alarmes (techniques, intrusion, incendie, etc.) dans un local occupé 24h/24h et 7j/7j ou un renvoi vers un service d'astreinte.
- Placer les données enregistrées (enregistrement vidéo, journal d'accès, etc.) dans un local protégé. L'accès aux données doit être protégé.
- Prévoir, dans le cas d'informatique industrielle, la protection du local serveur vis-à-vis de l'environnement (pollutions diverses).

3.1.4 Aménagements intérieurs

Avant tout aménagement intérieur, prévoir la mise « hors poussières » des installations.

Pour le choix des aménagements intérieurs, il convient de prendre en compte les contraintes liées :

- A la présence humaine permanente ou temporaire dans les salles serveurs qui conditionne :
  - l'installation de vidéosurveillance,
  - le choix du gaz d'extinction automatique,
  - un apport en air neuf (non recyclé) – Code du Travail R232.5.3 ($25 m^3$/h/occupant).
- Aux revêtements intérieurs qui doivent tenir compte :
  - de l'électricité statique,
  - de la résistance au feu,
  - de la production de poussières,
  - etc.
- A l'éclairage qui doit tenir compte :
  - de la compatibilité électromagnétique,
  - de la chaleur dégagée,

- du balisage de sécurité qui doit être sur courant secouru,
- etc.

- Au nettoyage :
  - système intégré,
  - etc.

3.1.5 Eléments d'aménagement

L'aménagement intérieur d'une salle serveur peut être constitué des éléments suivants :

- Faux plancher.
- Faux plafond.
- Système de Détection et Extinction d'Incendie (DEI).
- Système de détection d'eau ou d'humidité.
- Système de contrôle et de régulation de la température et de l'hygrométrie.
- Alimentation électrique.
- Alimentation Sans Interruption (ASI : onduleurs, batteries).
- Redondance des équipements et des alimentations.
- Serveurs « lames » et baies (contraintes d'implantation et d'exploitabilité)
- Evacuation des personnes.
- Système de contrôles d'accès et de surveillance.
- Installation éventuelle d'une cage de Faraday.
- Etc.

3.1.5.1 Faux plancher

Fonctions

- Passage des câbles courants fort/faible.
- Conduite de l'air froid issu de la climatisation de la salle qui ressort devant les baies par des dalles percées (principe d'alternance allée chaude – allée froide).
- Soutenir les matériels (poids, etc.).
- Etc.

Caractéristiques

- Dimensions des dalles : généralement 600x600mm.
- Hauteur : fonction des quantités de câbles à y faire passer et du débit d'air souhaité **(**des formules de calcul sont utilisées dans les logiciels de simulation du marché).
- Détection eau, humidité, notamment à proximité de la climatisation, système d'évacuation, oxydation des vérins des faux-planchers.
- Nature des revêtements (peinture du sol, etc.).
- Tenue à la charge : fonction des équipements qui y seront installés, les plus lourds étant généralement les baies serveurs (jusqu'à deux tonnes / m²) et les Alimentations Sans Interruptions (ASI : onduleurs et batteries) ; pour les équipements les plus lourds, il est possible de recourir à des chaises (dispositif métallique) les faisant reposer directement sur la dalle béton. Il est recommandé d'installer les équipements les plus lourds près d'un mur porteur. Diverses solutions de renfort ou de répartition

peuvent être mises en œuvre par des sociétés spécialisées. Il est conseillé de mettre les ASI dans des locaux séparés.

- Résistance au feu (voir la norme EN-1047-2).
- Pré-câblage (rails, gaines, etc.).
- Séparation courant faible / courant fort.
- Propriétés antistatiques.
- Mise à la terre.
- Les aspects « incendie » sont traités au § « Systèmes de Détection et Extinction d'Incendie ».
- Cloisonnement si nécessaire (grilles).

Alternatives possibles

- Passage des câbles courants fort/faible par un faux plafond ou sur des chemins de câbles installés sur les baies.
- Bouches de climatisation situées au plafond ou sur les murs.

3.1.5.2 Faux plafond

Fonctions

- Passage des câbles courants forts/faibles.
- Conduite de l'air froid issu de la climatisation de la salle qui ressort par des bouches au plafond.
- Canalisations d'eau.
- Reprise de l'air chaud dans l'allée chaude par des grilles placées derrières les baies, l'air chaud est capté par les armoires de climatisation dans le plénum du faux-plafond.
- Fixer les différents équipements de sécurité et passer les câbles associés : détection incendie, capteurs de température, hygrométrie, présence, etc.
- Intégrer l'éclairage.

Caractéristiques

- Hauteur : fonction des quantités de câbles à y faire passer et du diamètre des conduites d'air.
- Les canalisations d'eau en dehors de celles indispensables (climatisation, installation sprinkler) sont à proscrire dans une salle serveurs.
- Etanchéité du vrai plafond et du plancher de l'étage supérieur.
- Résistance au feu *(norme EN-1047-2).*
- Qualité des matériaux.
- Système d'éclairage.

Alternatives possibles

- Passage des câbles courants forts/faibles par un faux plancher ou sur des chemins de câbles installés sur les baies.
- Bouches de climatisation au sol (faux plancher avec dalles percées) ou sur les murs.

3.1.5.3 Système de Détection et Extinction d'Incendie

Fonctions

- Détecter les départs de feu à l'intérieur de la salle serveurs, des baies et des locaux avoisinants.
- Détecter les départs de feu à l'intérieur des faux-planchers et des faux-plafonds.
- Prévoir les asservissements de la climatisation, des contrôles d'accès et des portes coupe-feu.
- Emettre un signal d'alarme permettant de déclencher un plan d'évacuation.
- Eteindre les incendies dans la salle serveurs, les faux-planchers, les faux plafonds et les baies qui s'y trouvent.
- Traitement des alertes (voir le chapitre « risques liés à l'organisation et aux procédures »)

Caractéristiques

- Modes d'extinction existant : sprinklers, brouillard d'eau, gaz.
- Types de gaz d'extinction : CO2 avec les précautions indispensables pour la protection des humains, Inergen, Argonit, etc.
  (le Halon est interdit depuis le 1er janvier 2004)
  Réaliser une veille concernant la pérennité des différents gaz d'extinction automatique couramment utilisés pour le choix du gaz.
- Types de détecteurs d'incendie : détecteur de fumées, de flammes, de chaleur, analyseur d'air. Les détecteurs ioniques devront être remplacés à terme, conformément au décret n°2002-460 du 4 avril 2002 relatif à la protection générale des personnes contre les dangers des rayonnements ionisants.
- Désenfumage.
- Les détecteurs et extincteurs, doivent être placés en ambiance, dans les faux-planchers, dans les faux-plafonds, dans les baies.
- Une installation fixe à gaz impose l'étanchéité du local (porte, trappes et pénétrations diverses) et une trappe de surpression (ou libération de la porte). Un « ventitest » doit être réalisé pour la conformité, visant à mesurer le débit de fuite du local.

Le document CLUSIF « sécurité incendie des équipements techniques » sera utilement consulté.

3.1.5.4 Système de détection d'eau ou d'humidité

Fonctions

La fonction principale des systèmes de détection d'eau et d'humidité est de détecter le plus rapidement possible les fuites, les infiltrations, les défauts du système de climatisation de façon à agir le plus efficacement possible pour protéger les systèmes.
Il peut être utile de consulter le document édité par le CLUSIF « La problématique des risques liés à l'eau ».
(Cf. le paragraphe : faux-planchers).

3.1.5.5 Système de contrôle et de régulation de la température et de l'hygrométrie

Les équipements informatiques (serveurs) ont une plage de température de fonctionnement limitée. En effet, les composants électroniques qu'ils comportent voient leur durée de vie se réduire lorsque la température dépasse un certain seuil. Il est donc conseillé, sinon nécessaire, de maintenir la température ambiante autour d'une vingtaine de degrés Celsius.

Il est recommandé d'installer les baies de façon à avoir des allées chaudes et des allées froides, l'arrivée des blocs de climatisation étant positionnée sur les allées froides.

Pour ce faire, les baies sont installées dos à dos pour les allées chaudes et face à face pour les allées froides, les équipements captant l'air à l'avant et le rejetant à l'arrière.

Un système de régulation de l'humidité de l'air (hygrométrie) est à mettre en place pour pallier le risque d'électricité statique si l'air est trop sec ou de court-circuit ou d'oxydation s'il est trop humide.

Climatisation de la salle

L'approche la plus couramment adoptée consiste à climatiser l'ensemble de la salle et à prévoir une redondance des installations.

Deux possibilités :

- Mutualisation du bloc de secours (n+1) – il peut cependant y avoir plusieurs blocs de secours.
- Doublement de chaque bloc (n+n)

La climatisation doit être convenablement dimensionnée pour que sa puissance de refroidissement soit au moins égale à la dissipation thermique totale des équipements présents dans la salle : serveurs, équipements réseaux, ASI. Au moment de dimensionner la climatisation, il est également souhaitable de tenir compte des évolutions futures de la salle.

La fourniture d'une puissance de refroidissement supérieure ou égale à la puissance totale dissipée n'est pas suffisante pour garantir un bon refroidissement des serveurs. D'autres facteurs sont à prendre en compte : le taux de renouvellement et la densité, souvent inégale (présence de points chauds dans la salle), de serveurs et donc de dissipation thermique dans la salle.

Au-delà de 10 kW par baie, il est recommandé de créer un espace réfrigéré dédié à cette zone ou d'avoir une baie elle-même réfrigérée.

Baies réfrigérées

La solution des baies réfrigérées permet d'atteindre des puissances de refroidissement allant jusqu'à 40kW par baie. Cette solution est aujourd'hui incontournable lorsqu'une baie est remplie de serveurs lames.

L'objectif est d'extraire la chaleur dissipée par les équipements hors de la salle et même du bâtiment. Le vecteur utilisé pour transporter la chaleur est un liquide ou un gaz. Ce vecteur est ensuite refroidi par une centrale de refroidissement suffisamment ventilée, idéalement placée à l'extérieur du bâtiment, puis renvoyé vers les baies réfrigérées (circuit fermé).

Processeurs réfrigérés

Des systèmes de refroidissement liquide directement au niveau des processeurs ont déjà été développés et testés en collaboration avec des fabricants de serveurs. De tels systèmes requièrent la distribution d'un réseau d'eau à l'intérieur même de la baie qui contient les serveurs.

3.1.5.6 Alimentation électrique

Fonctions
Assurer de façon fiable l'alimentation électrique des systèmes d'information.

Caractéristiques
Ce point est traité dans la fiche technique numéro trois. Il pourrait être utile de se reporter aux documents publiés par le CLUSIF :

- « La Sécurité installations électriques des équipements informatiques ».
- « L'Alimentation électrique des systèmes d'information ».

Autres sources d'énergies : une étude peut être menée concernant les alimentations électriques « propres » (éoliennes, soleil, bovins, etc.).

3.1.5.7 Alimentation Sans Interruption

Contexte
Une simple coupure de courant inopinée (malveillante ou non) peut provoquer des dégâts considérables sur un Système d'Information tels que des dommages matériels sur les composants électroniques, des dommages logiciels (notamment sur les verrouillages de données, de licences…), des pertes d'informations (transactions évaporées, perte d'intégrité des bases de données, …).

Fonctions
La fonction première de l'ASI (Alimentation Sans Interruption, en anglais UPS = *Uninterruptible Power Supply*) est de protéger de toute coupure ou microcoupure d'énergie électrique, l'ensemble des éléments actifs (hubs/concentrateurs, switchs/commutateurs, ponts, routeurs, serveurs,…) des salles serveurs.

Une fonction supplémentaire de l'ASI est d'assurer un courant électrique de qualité aux équipements qu'il alimente. Dans ce cas, c'est la partie onduleur de l'ASI qui assurera un courant électrique de tension et de fréquences régulières (230V et 50Hz sans harmonique). Ce seront des filtres qui arrêteront les parasites électriques.

Le système ASI au sens large a donc généralement 3 fonctions :

- **Protection** contre les coupures électriques courtes (d'une dizaine de minutes à généralement moins d'une heure) et contre les micros-coupures électriques (de quelques centièmes de secondes).
- **Régulation** des niveaux haut et bas de tension du courant électrique, du maintien de ses caractéristiques alternatives (fréquence, forme sinusoïdale) ainsi que du filtrage de tout phénomène électrique parasite (harmoniques).

- **Transition**, permettant la mise en route de systèmes d'alimentation relais (mise en fonction d'un groupe électrogène ou de tout autre remplacement de la source d'approvisionnement électrique initiale).

Caractéristiques

Caractéristiques générales

- Poids important à cause des batteries (attention à la répartition de la charge au sol).
- Dégagement important de chaleur (veiller à le maintenir à ~20°C pour une meilleure conservation des performances des batteries).
- Usure et vieillissement des batteries (à contrôler annuellement en condition normale d'utilisation).
- Liaison informatique avec le réseau afin d'informer de toute coupure et éventuellement :
  - Soit d'arrêter « proprement » les systèmes informatiques.
  - Soit de basculer sur une autre source d'approvisionnement électrique.
- Gestion et administration de l'ASI (contrôle du fonctionnement de ses éléments, de la qualité du courant, des remontées d'alertes…..) en adéquation avec le SI en place.
- En cas d'utilisation de batteries à solution d'acide chlorhydrique, prévoir un détecteur d'hydrogène dans la salle des batteries et une bonne aération ou extraction du gaz.

Caractéristiques particulières

Les caractéristiques de l'ASI doivent intégrer la sensibilité des appareils à protéger, l'environnement électrique de la salle (perturbations entre l'arrivée électrique et la distribution dans la salle serveurs) ainsi que la qualité reconnue de l'alimentation électrique d'origine.

Il faut connaître son réseau électrique !

- Eloignement ou non du poste source (la probabilité des défauts est proportionnelle à cette distance).
- Distribution aérienne (probabilité d'avaries : foudre, tempête, contacts d'arbre, d'oiseaux) ou souterraine.
- Prise en compte des risques de coupures ou de saturation de la ligne d'alimentation électrique, pouvant impacter simultanément plusieurs centres serveurs.

Caractéristiques du courant électrique	Solution par l'ASI
Variations lentes de tension résultant des variations de charges du réseau électrique.	Adéquation de la partie régulation de tension
Variations brusques de tension résultant de la commutation de charges fluctuantes (appareils de soudure, démarrage de moteurs électriques…).	Adéquation de la partie onduleur
Creux de tension jusqu'à la micro-coupure (~100ms) résultant de manœuvres ou de courts-circuits sur une autre antenne d'un poste source.	Adéquation de la partie onduleur

Caractéristiques du courant électrique	Solution par l'ASI
Variations impulsionnelles Surtensions de très courtes durées (ms/µs) résultant de fusion de fusibles, surtension atmosphériques, décharges électrostatiques.	Mise en place de filtres
Variations de fréquences Résultant de l'alimentation par une source autonome (groupe électrogène ou autres sources d'énergie) ayant un défaut de régulation ou une surcharge de l'alternateur.	Adéquation de la partie onduleur
Harmoniques Déformation de l'onde de tension. Déformation réinjectée par les appareils d'éclairage, les redresseurs et les systèmes à fréquence variable.	Mise en place de filtres
Déséquilibre de tension Résultant de défaut d'isolement, de courants absorbés non identiques sur toutes les phases (cas de systèmes monophasés raccordés à des réseaux triphasés)	Adéquation de la partie onduleur

Installations

Système ASI

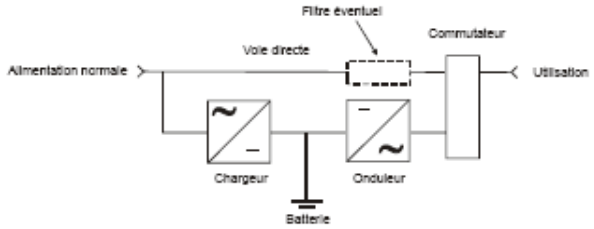
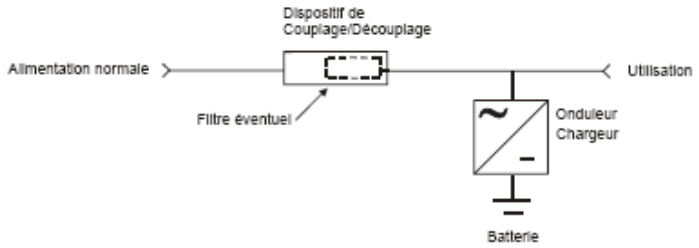
- Alimentation électrique réservée exclusivement aux salles serveurs.
- Câblage d'alimentation électrique (amont, mais surtout aval) protégé de toute perturbation électrique, notamment les câbles parcourus par de fortes pointes d'intensité (ascenseurs, climatisation,…).
- Schéma TN.S recommandé (Neutre directement relié à la Terre + Masses reliées au Neutre par des conducteurs de protection).
- Circuit de Terre isolé et séparé depuis la prise de terre jusqu'aux salles serveurs, potentiel de référence stable et éventuellement blindage du conducteur de liaison entre le circuit et la prise de terre.
- Pièce dont le degré d'hygrométrie de l'air est suffisant pour éviter les charges d'électricité statique (50% à +/-10%).
- Revêtements du sol et des murs anti-électricité statique.
- Emplacement protégé des champs électromagnétiques (tubes fluorescents défectueux, radar, émetteurs radio, transformateurs…).

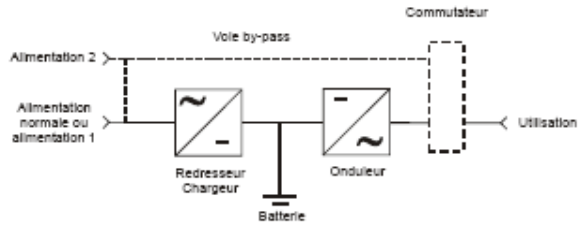
Environnement du système ASI

Les exigences des Equipements Electroniques Sensibles imposent un examen minutieux de leurs implantations.

- Examen de l'alimentation électrique avant et après implantation (caractéristiques électriques, régime de neutre, perturbations, fréquences, harmoniques, etc.).
- Examen du circuit de protection (prise de terre, continuité).
- Examen de l'environnement (parasites, bruits, vibrations, électricité statique, rayonnement).

Solutions possibles

Selon l'environnement électrique	Diverses technologies à des coûts différents sont possibles.
Environnement stable ou peu perturbé	**ASI en attente passive (Off-line ou Passive stand-by)** L'onduleur alimente l'application avec le secteur, simplement filtré mais sans aucune conversion d'énergie. Son principe de fonctionnement est séquentiel (sur secteur/sur batterie). En cas de coupure, de baisse ou hausse de tension, l'onduleur puise son énergie dans sa batterie pour fournir une énergie stabilisée. Son utilisation est inadaptée en cas de perturbations fréquentes (environnements industriels ou fortement perturbés). Avantage : Faible coût, pour environnement tertiaire. 
Environnement perturbé	**ASI fonctionnant en interaction avec le réseau (Line interactive)** En mode normal, l'appareil est géré par un microprocesseur qui surveille la qualité du réseau électrique et réagit aux variations. Un booster et un fader, circuits de compensation de tension, sont activés en cas de variation de l'amplitude de la tension. Avantage : Pallie les baisses ou les hausses de tension prolongées sans sollicitation des batteries. 

Selon l'environnement électrique	Diverses technologies à des coûts différents sont possibles.
Environnement très perturbé	**Double-conversion (On-Line)** Double conversion, technologie adaptée à la protection centralisée de serveurs garantissant une qualité constante quelles que soient les perturbations du secteur. Dans l'onduleur On-Line, la double conversion permanente élimine les perturbations électriques qui peuvent endommager un ordinateur : le courant est entièrement régénéré par transformation d'alternatif en continu, puis à nouveau de continu en alternatif. Il est indispensable pour la protection des installations vitales à l'entreprise et assure une protection permanente. L'onduleur On-Line est compatible avec tout type de charge car il ne génère pas de micro-coupure lors du passage sur batterie. Avantage : Technologie la plus performante, application constamment protégée contre tout type de perturbation, régulation permanente de la tension de sortie (amplitude et fréquence), continuité de service grâce au by-pass. 

Selon la puissance électrique nécessaire	Alimentation mono ou triphasée.
<= 16 kVA	Systèmes disponibles en monophasé et triphasé
> 16 kVA	Systèmes disponibles uniquement en triphasé

<u>Autres sources d'énergie</u>

Energies « propres »
Les énergies propres peuvent être classées en deux groupes :

1. Les énergies électriques non permanentes
2. Les énergies électriques permanentes

1) Les énergies n'ayant pas une capacité de production permanente :

Dans cette catégorie seront classées l'énergie éolienne et l'énergie solaire.

- L'énergie éolienne :

Les éolienne actuelles, ou aérogénérateurs peuvent avoir actuellement en France des puissances allant de quelques kilowatts jusqu'à 3 mégawatts. Celles que nous voyons ont souvent une puissance d'un mégawatt. Comme cette source énergie dépend de la force du vent, elle ne peut être considérée comme constante. Cette centrale pourra être reliée à des batteries pour avoir une prolongation de fourniture. L'installation de cette source d'énergie dans une société, possédant un campus servira à réduire la facture énergétique, mais la société ne pourra se dispenser d'une arrivée fournisseur. S'il y a surplus de production électrique, ce surplus peut être revendu au fournisseur d'électricité, ce qui réduit encore le coût énergétique total.

- L'énergie solaire :

Cette énergie est captée par des cellules photovoltaïques. Ces cellules sont reliées en module et c'est la multiplication des modules qui forme une centrale photovoltaïque. L'énergie solaire n'étant disponible qu'avec un ensoleillement suffisant, cette centrale sera reliée à des batteries pour avoir une prolongation de fourniture. Nous retrouvons ici les mêmes contraintes qu'avec l'énergie éolienne.

2. Les énergies ayant une production permanente :

Dans cette catégorie les principales seront l'énergie géothermique et l'énergie hydroélectrique

- L'énergie géothermique :

Cette énergie est surtout utilisée pour le chauffage. Son gradient thermique dans nos régions est de 3 à 4 degrés pour 100 mètres. Dans les régions volcaniques, des valeurs plus importantes peuvent être atteintes. Néanmoins cette énergie n'est en général pas utilisée pour produire de l'électricité en France.

- L'énergie hydroélectrique :

Les sociétés mitoyennes, avec un cours d'eau possédant un débit permanent tout au long de l'année, peuvent envisager une dérivation permettant une production électrique. Dans ce cas elles peuvent être autosuffisantes et n'avoir recours à un fournisseur qu'en cas de panne de leur production, mais surtout pouvoir leur revendre l'excès de production.

3.1.5.8 Redondance des équipements et des alimentations.

Ce point est traité dans le document CLUSIF « Plan de continuité de l'activité ».

3.1.5.9 Serveurs « lame » et baies

3.1.5.9.1 Serveurs « lame »

La mise en place de serveurs "lame" pose des problèmes de trois ordres :

- Contraintes de poids.
- Contraintes de climatisation.

- Contraintes électriques.

Contraintes de poids
Les serveurs se regroupent dans des armoires "racks" et leur concentration sur quelques mètres carrés (2 ou 3, souvent inférieur à 1) pose des problèmes de poids. Il faut compter pour un "rack" d'environ une cinquantaine de serveurs un poids de près d'une tonne. D'où la nécessité d'adapter éventuellement le faux plancher, soit même de supprimer ce faux plancher. En outre, ne pas oublier de tenir compte de la totalité des poids reposant sur la plate-forme.

Contraintes de climatisation
La circulation de l'air frais dans les racks est totalement différente de celle employée pour les serveurs alignés horizontalement. Un air arrivant à travers des dalles de faux plancher va refroidir les serveurs les plus bas au détriment des serveurs les plus hauts dans l'armoire "rack". D'où la nécessité de réadapter la circulation et la vitesse des flux : Flux par-dessus, par en-dessous ou à défaut laisser des emplacements libres dans le "rack". De plus, il faut toujours mettre en place des caches pour obturer les espaces non occupés par un élément.

Contraintes électriques
Les processeurs de ces nouveaux serveurs sont de plus en plus puissants, cette puissance est concentrée aussi en des points bien précis, d'où la nécessité d'adapter la puissance électrique à cette nouvelle donne. Il est calculé qu'une puissance habituelle d'une baie passe de 2 kW à 20 kW pour une armoire complète de serveurs "lame".

3.1.5.9.2 Baies passives ou actives

Les baies passives sont composées d'équipements qui ne génèrent pratiquement pas de chaleur et faibles consommateurs d'énergie. (Autres termes : baie de brassage, baie cabling, baie de rocade, etc.)

Les baies actives sont composées d'équipement réseaux ou de serveurs, gros consommateurs d'énergie et forts dissipateurs calorifiques.

Baies passives

Les baies passives sont composées d'équipements, généralement assez légers, peu profonds et peu consommateurs d'énergie/dissipateurs de chaleur.

Baies actives

Ces baies reçoivent les équipements réseaux tels que : serveurs, commutateurs, routeurs, répartiteurs…

Les serveurs sont les équipements actifs qui consomment le plus d'énergie et dissipent le plus de chaleur. Leur puissance dissipée peut d'ailleurs être évaluée approximativement en la considérant comme égale à la puissance consommée.

3.1.5.10 Evacuation des personnes.

Ce chapitre concerne l'ensemble du bâtiment et non exclusivement la salle serveur.

Fonctions

Répondre aux pré-requis suivants :

- Effectuer une visite préalable du bâtiment.
- Disposer d'un plan des lieux et en cas de mutualisation y intégrer les consignes d'évacuation communes.
- Avoir une liste du personnel en charge d'organiser l'évacuation. Ce personnel doit connaître les règles de mise en sécurité des personnes.
- Prendre en compte et connaître les lieux occupés par des personnes à mobilité réduite ou disposant d'une perte de l'acuité visuelle ou auditive.
- Attention au déclenchement des systèmes d'extinction d'incendie dans les salles serveurs (panneau, sirène, etc.)

Caractéristiques

Pré-requis

- Repérage.
  - des zones de mise en sécurité,
  - des chemins d'acheminement vers les issues les plus courts possible,
  - des cheminements permettant l'évacuation des personnes handicapées,
  - des goulots d'étranglement possibles, afin de les éviter.
- Balisage menant vers les lieux de regroupement en évitant les contre-courants, que les personnes soient valides ou non.
- Reports des alertes visuelles ou sonores, sous surveillance permanente.

Alerte et évacuation

- Prévenir rapidement les personnes responsables en cas d'évacuation des locaux.
- Déclencher alarme sonore et visuelle.
- Informer les sous-traitants éventuellement présents en salle.
- Aider les personnes handicapées.

Informer et entraîner

- Afficher les consignes donnant la procédure d'alerte et d'évacuation (nom des responsables, numéros de téléphone d'urgence, guides d'évacuation ou équipiers d'étage, lieu de rassemblement, etc.).
- Prévoir des exercices réguliers d'évacuation les plus réalistes possibles avec manipulation des extincteurs.
- Si possible, faire appel aux pompiers pour ces exercices.
- Rappeler les consignes à l'occasion des exercices annuels d'évacuation.

La réglementation (Code du Travail)

- L'article L.230-2 donne les principes généraux de prévention.
- L'article R 232-1 donne des règles sur l'aménagement des lieux de travail.
- L'article R.235-3-18 donne les conditions d'accueil des personnes valides et handicapées.

- L’arrêté du 25 juin 1980 concerne la protection des personnes en cas d’incendie ou de panique.
- L’article GN8 « Admission des handicapés », fixe les règles concernant les personnes à mobilité réduite sur leur déplacement en fauteuil roulant dans différents types d’établissement.

Alternatives possibles
Aucune.

3.1.5.11 Système de contrôles d’accès et de surveillance.

Fonctions
La sécurisation des accès à un site, passe par l'obtention d'un équilibre subtil entre le caractère dissuasif, voire infranchissable, d'une barrière, et la "valeur" des biens à protéger. Un contrôle d'accès ne constitue pas un système de sécurité en soi, mais il y participe en assurant la vérification d'un authentifiant (badge, code d’accès, données biométriques, etc.). Il est, de plus, généralement couplé avec des ensembles mécaniques faisant obstruction au passage libre, et des ensembles électroniques de détection d’ouverture prolongée, d'effraction et/ou de pénétration.

Caractéristiques
La sécurité des accès distingue généralement :

- **La périphérie** : espaces du site extérieurs aux bâtiments renfermant les locaux à protéger.
- **La périmétrie** : partie extérieure du bâtiment (murs, terrasses, ouvertures, etc.) renfermant les locaux à protéger.
- **L'intérieur des locaux** : intérieur du bâtiment, généralement découpé en zones en fonction du besoin de sécurité de chaque zone.

Le choix des systèmes doit notamment prendre en considération :

- L'isolement éventuel du site, et surtout, le mode d'occupation des locaux : permanent 24h/24h ou limité aux heures ouvrées.
- Les éventuels éléments perturbateurs : conditions atmosphériques, présence d'animaux, etc.
- L'emplacement et la nature des issues et des chemins de pénétration.
- La localisation des biens et valeurs à protéger.
- Les flux : personnel, livraison, matériels, médias, etc.

Les systèmes de contrôles d’accès et de surveillance peuvent être de nature mécanique, électronique, électrique, vidéo, acoustique, lumineuse, infrarouge, animale (chiens de garde), ou humaine. Certains de ces systèmes sont soumis à la législation ou à la réglementation (déclaration à la CNIL, au Comité d’Entreprise, Préfecture, etc.)

Le détail de ces systèmes est expliqué dans les documents CLUSIF suivants qu’il est recommandé de consulter :

- « Contrôle d'accès physique et protection intrusion ».
- « Contrôle d'accès par la biométrie ».

Alternatives possibles
Aucune.

3.1.5.12 Installation éventuelle d'une cage de Faraday.

Fonctions
Une cage de Faraday est utile pour les activités demandant un haut niveau de confidentialité (type secret défense). La cage protège également des rayonnements électromagnétiques externes. Ce cas particulier est à prendre en compte au moment de la conception des aménagements intérieurs.

Caractéristiques
Se conformer au manuel d'installation.

3.2 Règles et procédures de sécurité

Les règles et procédures doivent s'appuyer sur la politique de sécurité générale de l'entreprise et dans le cas d'une copropriété respecter son règlement.

Pour que les règles de sécurité soient respectées, vérifiées et améliorées, des procédures d'application des règles de sécurité doivent exister :

- Document d'engagement formel de la direction concernant la sécurité.
- Procédure de gestion des documents.
- Aspects humains
  - description des rôles et responsabilités des employés en matière de sécurité,
  - clauses de sécurité dans les contrats (sous-traitant ou employé), fiche de poste ou règlement intérieur selon l'organisation interne des entreprises,
  - procédure et plan de formation des personnels,
  - procédures comportementales (bureau net, matériels sensibles attachés, etc.),
  - procédures concernant l'organisation et la sécurité des locaux au jour le jour (cartons entreposés, palettes, étagères trop remplies qui gênent l'action des dispositifs mis en place, écrans cathodiques allumés, surcharge des prises de courant, masse combustible à réduire au strict minimum non seulement en salle mais aussi dans les couloirs avoisinants, chasse aux vieux câbles devenus inutiles notamment en cas de réaménagement, propreté des chemins de câbles, référencement des câbles, filtration, etc.).
  - respect de l'affichage légal qui doit être à l'entrée des locaux.
- Contrôle d'accès
  - procédure de gestion des clés,
  - procédure de gestion des accès (port du badge, contrôle des visiteurs, des sous-traitants, des livraisons, etc.),
  - consignes aux gardiens (y compris les aspects malveillance),

- procédure concernant les mesures de sécurité provisoires à prendre lors de travaux,
- procédures d'intervention urgente.

- Gestion technique des alarmes
  - Procédures de traitement des alarmes et des alertes en fonction de leur type.
- Maintenance des équipements
  - Procédure de maintenance des équipements.
  - Consignes concernant le matériel minimum devant être disponible rapidement et facilement en salle (ventouses, bâches, etc.).
  - Procédure d'entrée et de sortie des matériels.
  - Procédure de destruction des médias.
- Procédures liées à l'incendie.
- Etc.

4. Maintenance et évolution

4.1 Maintenance des équipements

La maintenance des équipements recouvre les aspects suivants :

- Assurer l'entretien et le maintien des équipements y compris la maintenance préventive.
- Assurer la continuité d'intervention des équipements.
- Assurer l'entretien des salles informatiques et des locaux annexes.
- Etc.

4.2 Evolutions

L'évolution des salles serveurs doit tenir compte de l'évolution des techniques et des réglementations.

4.2.1 Evolution des techniques

L'évolution des techniques, notamment la virtualisation des serveurs, peut avoir un impact fort sur l'infrastructure des salles serveurs (surface nécessaire, puissance électrique, climatisation, etc.)

En phase d'étude préalable, il est recommandé de prendre en compte les possibilités offertes par les nouvelles techniques, au moment de prendre les décisions d'extension ou de création de nouvelles salles.

Lors de la conception de salles serveurs, il est recommandé de prévoir de la souplesse au niveau des installations pour s'adapter aisément à de nouvelles contraintes.

4.2.2 Evolution des réglementations

L'évolution des réglementations peut impacter la conception ou le réaménagement des salles. Ex.

- Nouveaux standards « sécurité incendie »
- Vidéosurveillance
- Conservation des journaux (logs)
- Lois environnementales
- Lois sur la conservation des archives
- Etc.

ANNEXES

Annexe 1 : Références

Assurance et réglementation

Référentiels APSAD et documents de certification
en vigueur au 26 janvier 2006

DOMAINE 0 : REGLEMENTS GENERAUX DE CERTIFICATION		Date	Observations
Certification			
H0	Règlement général de la marque A2P	04.1999.1 (juin 2001)	
B0	Règlement général de la certification APSAD de service	01.2003.0 (janvier 2003)	

DOMAINE 1 : EXTINCTION AUTOMATIQUE A EAU – TYPE SPRINKLEURS		Date	Observations
Certification			
E1	Règlement - Certification APSAD de service de vérification	02.2003.0 (février 2003)	
I.F1	Règlement - Certification APSAD de service d'installation	07.2004.0 (juillet 2004)	
H1	Agrément des matériels		
	H 1.0 - Conditions d'agrément "Assurance" : Armoires de commande et de contrôle des groupes	11.2002.0 (novembre 2002)	
	H 1.1 - Spécifications et méthodes d'essais - Armoires de commande et de contrôle des groupes moto-pompes à moteur diesel	juin-98	
	H 1.2 - Spécifications et méthodes d'essais - Armoires de commande et de contrôle des groupes de pompage à moteur électrique	juin-98	
	H 1.3 - Spécifications et méthodes d'essais - Dispositif de réception des alarmes	juin-98	
Référentiels techniques			
R1	Règle d'installation	04.2002.1 (octobre 2003)	
N1	Certificat de conformité à la règle APSAD R1	nov-04	
Q1	Compte-rendu de vérification semestrielle d'une installation de sprinkleurs	nov-04	
N100	Avis de mise hors service / remise en service d'une installation de sprinkleurs	avr-05	
S1A / S1B	Entretien des systèmes d'extinction automatique à eau type sprinkleur	oct-05	

DOMAINE 3 : EXTINCTION AUTOMATIQUE A CO2		Date	Observations
Certification			
I 13	Règlement - Certification APSAD de service d'installation de systèmes d'extinction. Certification APSAD de service de recyclage des gaz inhibiteurs.	03.2002.1 (février 2003)	
H 13	Règlement particulier de la marque A2P - Matériels EAG	10.2001.0 (octobre 2001)	
Référentiels techniques			
R3	Règle d'installation	02.1996.2 (février 2003)	en cours de révision
RT3	Spécifications et règles techniques d'essais des composants d'une installation révision prévue d'extinction automatique à CO2	févr-97	Révision prévue (T13 partie 2)
N3	Certificat de conformité à la règle APSAD R3	févr-03	
Q2/3	Compte-rendu de vérification périodique	févr-03	

DOMAINE 4 : EXTINCTEURS MOBILES		Date	Observations
Certification			
I4 - NF 285	Règlement - Certification APSAD et NF Service Service d'installation et de maintenance	07.2003.0 (juillet 2003)	
Référentiels techniques			
R4	Règle d'installation	01.2007.1 (septembre 2007)	
R4	R4 Version Anglaise	09.1994.4 (June 1999)	
N4	Certificat de conformité à la règle APSAD R4	févr-03	
Q4	Compte-rendu de vérification périodique	févr-03	

DOMAINE 5 : ROBINETS D'INCENDIE ARMES		Date	Observations
Certification			
J5/F5	Règlement - Certifications APSAD de service de validation / de maintenance	01.2002.1 (février 2003)	
Référentiels techniques			
R5	Régle d'installation	01.2002.4 (février 2003)	
N5	Certificat de conformité à la règle APSAD R5 et à son annexe 1 (dispositions assurance)	févr-03	
	Déclaration de conformité à la règle APSAD R5	févr-03	
Q5	Compte-rendu de vérification périodique	déc-04	

DOMAINE 6 : SERVICE DE SECURITE INCENDIE		Date	Observations
Référentiels techniques			
R6	Règle d'organisation	04.2002.2 (septembre 2007)	

DOMAINE 7 : DETECTION AUTOMATIQUE D'INCENDIE		Date	Observations
Certification			
F7	Règlement - Certification APSAD de service de maintenance de systèmes de détection d'incendie et de centralisateurs de mise en sécurité incendie	05.2004.0 (mai 2004)	
I7	Règlement - Certification APSAD de service d'installation de systèmes de détection d'incendie et de centralisateurs de mise en sécurité incendie	07.2001.1 (février 2003)	
DAI7	Déclaration d'installation	version février 2003	
Référentiels techniques			
R7	Règle d'installation	07-2006-1 (juin 2007)	

DOMAINE 8 : SURVEILLANCE DES RISQUES D'UNE ENTREPRISE		Date	Observations
Référentiels techniques			
R8	Règle d'organisation	08.1998.2 (décembre 2007)	

DOMAINE 9 : DEFENSE EXTERIEURE CONTRE L'INCENDIE ET RETENTIONS		Date	Observations
Référentiels techniques			
D9	D9 Guide pratique pour le dimensionnement des besoins en eau	09.2001.0 (sept 2001)	FFSA - INESC – CNPP à télécharger sur cnpp.com
D9A	Guide pratique pour le dimensionnement des rétentions des eaux d'extinction	08.2004.0 (août 2004)	

DOMAINE 11 : ABONNEMENT PREVENTION ET CONSEIL INCENDIE		Date	Observations
Certification			
E11 Conditions d'agrément "Assurance" des organismes janv-05 certification prévue fin 2005	Conditions d'agrément "Assurance" des organismes	Janv-05	certification prévue fin 2005
Référentiels techniques			
R11	Règle d'organisation - Réalisation des missions APCI	01.2005.0 (janvier 2005)	

DOMAINE 12 : EXTINCTION AUTOMATIQUE A MOUSSE A HAUT FOISONNEMENT		Date	Observations
Référentiels techniques			
R12	Règle d'installation	05.1999.0 (mai 1999)	
N12	Déclaration de conformité à la règle APSAD R12	mai-99	Modèles à remplir sur papier libre
Q12	Compte-rendu de vérification périodique mai-99 sur papier libre	mai-99	

DOMAINE 13 : EXTINCTION AUTOMATIQUE A GAZ		Date	Observations
Certification			
I13	Règlement – Certification APSAD de service d'installation de systèmes d'extinction Certification APSAD de service de recyclage des gaz inhibiteurs	03.2002.1 (février 2003)	
H13	Règlement particulier de la marque A2P - Matériels EAG	10.2001.0 (octobre 2001)	
Référentiels techniques			
R13	Règle d'installation - Gaz inertes, gaz inhibiteurs	06,2007,0 (juin 2007)	
T13	Règles techniques - Spécifications et méthodes d'essais - 1- Systèmes	03.2002.0 (mars 2002)	
N13	Certificat de conformité à la règle APSAD R13 Déclaration de conformité à la règle APSAD R13	févr-03	
	Déclaration de conformité à la règle APSAD R13	févr-03	
Q13	Compte-rendu de vérification périodique	févr-03	

DOMAINE 14 : CONSTRUCTION - COMPORTEMENT AU FEU		Date	Observations
Référentiels techniques			
D14	Document technique : Ossatures - Murs extérieurs – Couvertures	juil-00	ex DTI4 - PR/f - CB2 - CS1
D14 A	Document technique - Panneaux "Sandwich" - Comportement au feu - Guide pour la mise en œuvre	05.1999.0 (mai 1999)	
T14 A	Règles techniques - Panneaux "Sandwich" - Comportement au feu - Spécifications tech. et méthodes d'essais	06.1999.0 (juin 1999)	

DOMAINE 15 : OUVRAGES SEPARATIFS COUPE-FEU		Date	Observations
Référentiels Techniques			
R15	Règle de construction	07.1985.2 (janvier 2000)	en cours de révision

DOMAINE 16 : FERMETURES COUPE-FEU Date		Date	Observations
Certification			
X16 / Y16	Conditions d'agrément "Assurance" : portes coupe-feu et installation de portes coupe-feu	04.2002.0 (avril 2002)	I16 à paraître
Référentiels Techniques			
R16	Règle d'installation	07.2005.1 (août 2007)	
N16	Certificat de conformité à la règle APSAD R16	mars-01	
Q16	Compte-rendu de vérification périodique	mars-01	

DOMAINE 17 : DESENFUMAGE		Date	Observations
Certification			
I17	Règlement - Certification APSAD de service d'installation de systèmes de désenfumage naturel	06.2002.1 (février 2003)	
F17	Règlement - Certification APSAD de service de maintenance de systèmes de désenfumage naturel	06.2002.1 (février 2003)	
SDN17	Déclaration d'installation	Version mars 2004	
Référentiels Techniques			
R17	Règle d'installation des exutoires de fumées et de chaleur	07.2006.0 (juillet 2006)	
N17	Certificat de conformité à la règle APSAD R17	août-00	Modèle à remplir sur papier libre

DOMAINE 18 : INSTALLATIONS ELECTRIQUES		Date	Observations
Certification			
Y18	Conditions d'agrément "Assurance" des organismes de vérification	11.2004.1 (février 2005)	
Référentiels Techniques			
Q18	Compte rendu de vérification périodique	nov-04	

DOMAINE 19 : THERMOGRAPHIE INFRAROUGE		Date	Observations
Référentiels Techniques			
D19	Document technique – Contrôle d'installations électriques	05.2007.0 (mai 2007)	
Q19	Déclaration de contrôle d'une installation électrique par thermographie infrarouge	mars-99	Modèle à remplir sur papier libre

DOMAINE 31 : TELESURVEILLANCE		Date	Observations
Certification			
I31	Règlement – Certification APSAD de service de télésurveillance	10.2003.0 (octobre 2003)	
Référentiels Techniques			
R31	Règle de prescription	07.2007.0 (juillet 2007)	
N31	Certificat de conformité à la règle APSAD R31 et à son annexe 1 (dispositions assurance)	oct-02	

DOMAINE 41 : TELESECURITE		Date	Observations
Référentiels Techniques			
R41	Règle de prescription - Habitations - Risques "Standard"	12.2000.0 (déc 2000)	

DOMAINE 50 : DETECTION D'INTRUSION – Risques habitations		Date	Observations
Certification			
I50	Règlement – Certification APSAD de service d'installation	06.2000.1 (février 2003)	
Référentiels Techniques			
R50	Règle d'installation – Risques habitations	05.1999.2 (février 2003)	en cours de révision
N50	Certificat de conformité à la règle APSAD R50 et à son annexe 1 (dispositions assurance)	févr-03	
	Déclaration de conformité à la règle APSAD R50	févr-03	

DOMAINE 55 : DETECTION D'INTRUSION - Risques professionnels		Date	Observations
Certification			
I55	Règlement – Certification APSAD de service d'installation	07.2000.3 (février 2003)	
Référentiels Techniques			
R55	Règle d'installation – Risques professionnels	06.2000.2 (février 2003)	en cours de révision
N55 niveau 1	Certificat de conformité aux prescriptions de l'assurance (risques [600 m²)	févr-03	
	Déclaration de conformité (risques [600 m2)	févr-03	
N55 niveau 2	Certificat de conformité aux prescriptions de l'assurance (risques > 600 m2)	févr-03	
	Déclaration de conformité (risques > 600 m2)	févr-03	
Q55	Compte-rendu de vérifications	févr-03	

DOMAINE 58 : DETECTION D'INTRUSION - Matériels de sécurité électroniques		Date	Observations
Certification			
H58 - NF 324	Règlement unique des certifications NF et A2P	oct-02	

DOMAINE 59 : DETECTION D'INTRUSION – Systèmes d'alarme à liaison hertziennes		Date	Observations
H59	Règlement particulier de la marque A2P - Matériel Radio	04.1999.0 (avril 1999)	Agrément "Assurance" (validité : sept.2005)
T59	Règles techniques - Spécifications et méthodes d'essais	04.1999.0 (avril 1999)	

DOMAINE 60 : PROTECTION MECANIQUE CONTRE LA MALVEILLANCE		Date	Observations
C60	Règlement - Certification A2P Service de pose et d'après-vente d'équipements	07.2005.0 (Janvier 2006)	

DOMAINE 61 : SERRURES DE BATIMENTS		Date	Observations
Certification			
H61	Règlement particulier de la marque A2P	10.2000.0 (octobre 2000)	
T61	Règles techniques - Spécifications et méthodes d'essais	10.2000.0 (octobre 2000)	

DOMAINE 62 : FENETRES ET FERMETURES DES BATIMENTS		Date	Observations
Certification			
H62	Règlement particulier de la marque A2P	09.2001.0 (sept 2001)	
T62	Règles techniques - Spécifications et méthodes d'essais	09.2001.0 (sept 2001)	

DOMAINE 63 : DEVANTURES DE MAGASINS		Date	Observations
Référentiels Techniques			
D63	Document technique - Guide de protection	05.1998.1 (juillet 2000)	

DOMAINE 64 : BLOCS-PORTES DE BATIMENT		Date	Observations
Certification			
H64	Règlement particulier de la marque A2P	01.2003.0 (janvier 2003)	
T64	Règles techniques - Spécifications et méthodes d'essais	01.2003.0 (janvier 2003)	

DOMAINE 71 : COFFRES-FORTS		Date	Observations
Certification			
H71	Règlement particulier de la marque A2P	09.2002.0 (septembre 2002)	
Référentiels Techniques			
T71-1	Spécifications et méthodes d'essais - 1 : Coffre-forts, portes fortes et chambres fortes préfabriquées	09.2002.0 (septembre 2002)	
T71-2	Spécifications et méthodes d'essais - 2 : Serrures de coffre-forts	09.2002.0 (septembre 2002)	
T71-3	Spécifications et méthodes d'essais - 3 : Coffres pour automates bancaires	09.2002.0 (septembre 2002)	
T71-4	Spécifications et méthodes d'essais - 4 : Coffres domestiques	09.2002.0 (septembre 2002)	
T71-5	Spécifications et méthodes d'essais - 5 : Systèmes de neutralisation de billets intégrés aux automates bancaires	12.2003.1 (avril 2005)	

DOMAINE 81 : DETECTION D'INTRUSION		Date	Observations
Référentiels Techniques			
R81	Règle d'installation	12.2005.0 (décembre 2005)	Remplace R50 et R55

DOMAINE 201 : MARQUAGE CE		Date	Observations
Certification			
A201	Procédure Directive Produits de Construction 89/106/CEE - Attestation de conformité (système 1) Systèmes fixes de lutte contre l'incendie : systèmes fixes d'extinction à gaz, systèmes fixes d'extinction à poudre, systèmes fixes d'extinction type sprinkleur et à pulvérisation d'eau	07.2002.0 (juillet 2002)	CNPP organisme notifié
A201	Version anglaise	07.2002.0 (July 2002)	

DOMAINE 301 : SYSTEMES DE MANAGEMENT DE LA QUALITE (SMQ)		Date	Observations
Certification			
K301	Règlement – Certification " CNPP - Qualité certifiée ISO 9001 : 2000 "	06.2003.0 (juin 2003)	

Décret

88-1056 **14/11/1988** version consolidée au 22 juin 2001	Décret n°88-1056 du 14 novembre 1988 pris pour l'exécution des dispositions du livre ii du code du travail (titre iii: hygiène, sécurité et conditions du travail) en ce qui concerne la protection des travailleurs dans les établissements qui mettent en œuvre des courants électriques nor: teft8804060d
Nouvelle parution **2008-2009**	Pour information : Un nouveau décret est en étude pour être publié fin 2008, début 2009.

Normes d'installation UTE, NFC et NFEN.

NFEN 1047-2 Mar 2000	Classification et méthodes d'essai de résistance au feu. Partie 2 : conteneurs et chambres réfractaires Indice de classement : K20-006-2 Statut : norme homologuée
NFEN 60529 juin 2000 (2ème tirage – novembre 2007)	Degrés de protection procurés par les enveloppes (Code IP). Statut : norme homologuée (2ème tirage - novembre 2007) Est composé de : NFEN 60529 (01/10/1992) NFEN 60529/A1 (01/06/2000) Corrigendum de la NFEN 60529 - 1992.
NFC15-100 E02 01/12/2002	Installations électriques à basse tension (CEI série 60364 et HD de la série 384). Est destinée à remplacer la NF C 15-100 - 1991 + A1 - 1994 + A2 - 1995. La mise à jour de juin 2005 est intégrée.
NFC 17 100	Concernant la protection contre la foudre et les installations de paratonnerre.
NFC 53-040-1-1 NF EN 62040-1-1 01/12/2004	Alimentations sans interruption (ASI) Partie 1-1: Prescriptions générales et règles de sécurité pour les ASI utilisées dans des locaux accessibles aux opérateurs. (Remplace la norme homologuée NF EN 50091-1 (C 42-810-1) de septembre 1993)
UTEC00-105-1 01/06/2006	Avis relatif à l'application du décret 95-1081 – listes des normes utilisées dans le cadre de la directive "basse tension"
UTEC15-103 01/04/2004	Installations électriques à basse tension - Guide pratique - Choix des matériels électriques (y compris les canalisations) en fonction des influences externes.
UTEC15-105 01/07/2003	Guide pratique - Détermination des sections de conducteurs et choix des dispositifs de protection - Méthodes pratiques
UTEC15-106 01/12/2003	Installations électriques à basse tension et à haute tension - Guide pratique - Sections des conducteurs de protection, des conducteurs de terre et des conducteurs de liaison équipotentielle.

UTEC15-401 01/01/2004	Guide pratique - Groupes électrogènes - Règles d'installation.
UTEC15-402 01/11/2004	Guide pratique - Alimentation sans interruption (ASI) de type statique et système de transfert statique (STS) - Règles d'installation.
UTEC15-520 01/07/1998	Installations électriques à basse tension - Guide pratique: Canalisations - Modes de pose - Connexions. (Remplace la UTE C 15-520 - 1992).
UTEC15-559 01/09/2002	Installations électriques à basse tension - Guide pratique - Installation d'éclairage en très basse tension.
UTEC15-900 01/10/2000	Guide pratique - Mise en œuvre et cohabitation des réseaux de puissance et des réseaux de communication dans les installations des locaux d'habitation, du tertiaire et analogues. (Remplace la UTE C 15-900 - 1999).

Foudre

NFC17-100 01/12/1997	Protection contre la foudre - Protection des structures contre la foudre - installation de paratonnerres
NFC17-100-2 01/11/2006	Protection contre la foudre Partie 2: Evaluation du risque.
UTEC15-443 01/08/2004	Guide pratique - Protection des installations électriques basse tension contre les surtensions d'origine atmosphérique ou dues à des manœuvres. Choix et installation des parafoudres.

Groupes électrogènes

UTEC15-401 01/01/2004	Guide pratique - Groupes électrogènes - Règles d'installation.

Alimentation sans interruption

UTEC15-402 01/11/2004	Guide pratique - Alimentation sans interruption (ASI) de type statique et système de transfert statique (STS) - Règles d'installation.
NFC53-040-1-1 NFEN 62040-1-1 01/12/2004	Alimentations sans interruption (ASI) - Partie 1-1: Prescriptions générales et règles de sécurité pour les ASI utilisées dans des locaux accessibles aux opérateurs. (Remplace la norme homologuée NF EN 50091-1 (C 42-810-1) de septembre 1993)
NFC53-040-1-2 NFEN 62040-1-2 01/12/2004	Alimentations sans interruption (ASI) Partie 1-2: Prescriptions générales et règles de sécurité pour les ASI utilisées dans des locaux d'accès restreint. (Est destinée à remplacer la NF C 42-810-1-2 - 1999)
NFC53-204-3 01/07/2001	Alimentations basse tension, sortie continue - Partie 3: Compatibilité électromagnétique (CEM) (CEI 61204-3 - 2000).
NFC53-240-3 A11 01/08/2001	Amendement à la NF C 53-240-3 - 1997.
NFC71-815-1 01/09/2001	Systèmes d'alimentation à source centrale. (Est destinée à remplacer la NF C 71-815 - 1987 ainsi que l'amdt.1 - 1988).
NFC53-040-2	Alimentations sans interruption (ASI) - Partie 2: Exigences pour la

01/06/2006	compatibilité électromagnétique (CEM). (est destinée à remplacer la NFEN 50091-2 - 1995)
NFC53-040-3 01/12/2001	Alimentations sans interruption (ASI) Partie 3 : Méthode de spécification des performances et procédures d'essai
UTEC15-400 01/07/2005	Installations électriques à basse tension Guide pratique - Raccordement des générateurs d'énergie électrique dans les installations alimentées par un réseau public de distribution
NFC58-272-2 01/12/2005	Règles de sécurité pour les batteries et les installations de batteries - Partie 2 : Batteries stationnaires

Compatibilité électromagnétique

NFC91-002-4 01/01/2003	Compatibilité électromagnétique (CEM) Partie 2-4: Environnement - Niveaux de compatibilité dans les installations industrielles pour les perturbations conduites à basse fréquence.
NFC91-003-2 E2 01/08/2006	Compatibilité électromagnétique (CEM) Partie 3-2 : Limites - Limites pour les émissions de courant harmonique de courant appelé par les appareils 16 A par phase. (2ème édition) (est destinée à remplacer la NFEN 61000-3-2 - 2001 et son amdt 2 - 2006)
NFC91-004-13 01/09/2002	Compatibilité électromagnétique (CEM) Partie 4-13 : Techniques d'essai et de mesure - Essais d'immunité basse fréquence aux harmoniques et inter-harmoniques incluant les signaux transmis sur le réseau électrique alternatif.

Habilitation et sécurité des personnels

UTEC18-510 MAJ 2004 01/11/1988	Recueil d'instructions générales de sécurité d'ordre électrique (MAJ 2004).
UTEC18-510 M Découverte	Fascicule Découverte: Employeurs: à la découverte de l'Habilitation Electrique.
UTEC18-530	Carnet de prescriptions de sécurité électrique destiné au personnel habilité - non électricien (BO, HO), exécutant (B1, H1), chargé d'interventions (BR).
UTEC18-511	Consignes relatives aux premiers secours à donner aux victimes d'accidents électriques.

Documents CLUSIF à consulter utilement

Plan de continuité d'activité – stratégie et solutions de secours du Système d'Information (09/2003) [http://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf]

Sécurité physique des éléments d'un réseau local (1999)
[http://www.clusif.asso.fr/fr/production/ouvrages/pdf/SecPhysReseauLocal.pdf]

Problématique des risques liés à l'eau (2004)
[http://www.clusif.asso.fr/fr/production/ouvrages/pdf/Risques_lies_eau.pdf]

Sécurité des installations électriques (1996)

Sécurité incendie des équipements techniques (2002)
[http://www.clusif.asso.fr/fr/production/ouvrages/pdf/SecuriteIncendie2002.pdf]

Contrôle d'accès physique : biométrie (2002)
[http://www.clusif.asso.fr/fr/production/ouvrages/pdf/ControlesAccesBiometrie.pdf]

Sécurité Physique, Equipements électriques (2005)

Les dossiers techniques : la sécurité des installations électriques des équipements informatiques (1998)

Dossiers techniques : l'alimentation électrique des systèmes informatiques (1996)
[http://www.clusif.asso.fr/fr/production/ouvrages/pdf/AlimentationElectriqueSI.pdf]

Annexe 2 : Glossaire

Extraits de la loi MOP (Loi n° 85-704 du 12/07/85) concernant le maître de l'ouvrage et le maître d'œuvre :

Maître de l'ouvrage

Le maître de l'ouvrage est la personne morale, mentionnée à l'article premier, pour laquelle l'ouvrage est construit. Responsable principal de l'ouvrage, il remplit dans ce rôle une fonction d'intérêt général dont il ne peut se démettre.

Il lui appartient, après s'être assuré de la faisabilité et de l'opportunité de l'opération envisagée, d'en déterminer la localisation, d'en définir le programme, d'en arrêter l'enveloppe financière prévisionnelle, d'en assurer le financement, de choisir le processus selon lequel l'ouvrage sera réalisé et de conclure, avec les maîtres d'œuvre et entrepreneurs qu'il choisit, les contrats ayant pour objet les études et l'exécution des travaux.

Lorsqu'une telle procédure n'est pas déjà prévue par d'autres dispositions législatives ou réglementaires, il appartient au maître de l'ouvrage de déterminer, eu égard à la nature de l'ouvrage et aux personnes concernées, les modalités de consultation qui lui paraissent nécessaires. Le maître de l'ouvrage définit dans le programme les objectifs de l'opération et les besoins qu'elle doit satisfaire ainsi que les contraintes et exigences de qualité sociale, urbanistique, architecturale, fonctionnelle, technique et économique, d'insertion dans le paysage et de protection de l'environnement, relatives à la réalisation et à l'utilisation de l'ouvrage.

Le programme et l'enveloppe financière prévisionnelle, définis avant tout commencement des avant-projets, pourront toutefois être précisés par le maître de l'ouvrage avant tout commencement des études de projet. Lorsque le maître de l'ouvrage décide de réutiliser ou de réhabiliter un ouvrage existant, l'élaboration du programme et la détermination de l'enveloppe financière prévisionnelle peuvent se poursuivre pendant les études d'avant-projets ; il en est de même pour les ouvrages complexes d'infrastructure définis par un décret en conseil d'Etat.
Le maître de l'ouvrage peut confier les études nécessaires à l'élaboration du programme et à la détermination de l'enveloppe financière prévisionnelle à une personne publique ou privée.

Maîtrise d'œuvre

La mission de maîtrise d'œuvre que le maître de l'ouvrage peut confier à une personne de droit privé ou à un groupement de personnes de droit privé doit permettre d'apporter une réponse architecturale, technique et économique au programme mentionné à l'article 2.
Pour la réalisation d'un ouvrage, la mission de maîtrise d'œuvre est distincte de celle d'entrepreneur.

Le maître de l'ouvrage peut confier au maître d'œuvre tout ou partie des éléments de conception et d'assistance suivants :
1° Les études d'esquisse ;
2° Les études d'avant-projets ;
3° Les études de projet ;
4° L'assistance apportée au maître de l'ouvrage pour la passation du contrat de travaux ;
5° Les études d'exécution ou l'examen de la conformité au projet et le visa de celles qui ont été faites par l'entrepreneur ;
6° La direction de l'exécution du contrat de travaux ;
7° L'ordonnancement, le pilotage et la coordination du chantier ;
8° L'assistance apportée au maître de l'ouvrage lors des opérations de réception et pendant la période de garantie de parfait achèvement.
Toutefois, pour les ouvrages de bâtiment, une mission de base fait l'objet d'un contrat unique. Le contenu de cette mission de base, fixé par catégories d'ouvrages conformément à l'article 10 ci-après, doit permettre :
- au maître d'œuvre, de réaliser la synthèse architecturale des objectifs et des contraintes du programme, et de s'assurer du respect, lors de l'exécution de l'ouvrage, des études qu'il a effectuées ;
- au maître de l'ouvrage, de s'assurer de la qualité de l'ouvrage et du respect du programme et de procéder à la consultation des entrepreneurs, notamment par lots séparés, et à la désignation du titulaire du contrat de travaux.

Les locaux informatiques doivent répondre aux spécifications de la classe ISO 8 de la Norme NF EN ISO 14644-1 relative aux salles propres, cette norme est disponible auprès des bureaux normalisation.

Niveau Kéraunique : Nombre de jours où le tonnerre est entendu pendant une période donnée. Les calculs associés sont définis dans l'annexe B des normes NFC 17-100 et NFC 17-102.

Sigles

UTE : **U**nion **T**echnique de l'**E**lectricité

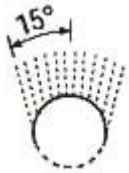
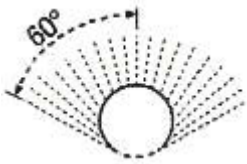
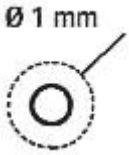
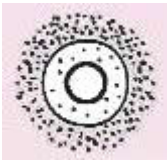
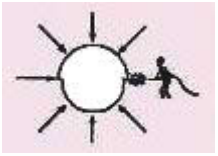
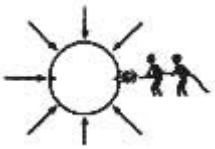
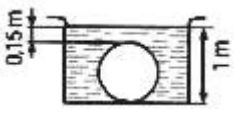
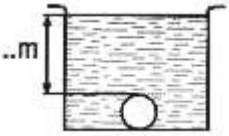
NFC : **N**orme **F**rançaises Classe **C** "Electrique",

NFEN : **N**orme **F**rançaise d'origine **E**uropéenne,

IEC : **N**orme de la Commission **E**lectrotechnique **I**nternationale

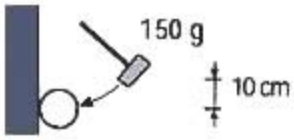
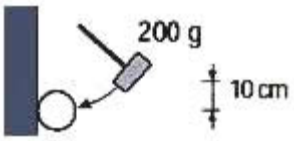
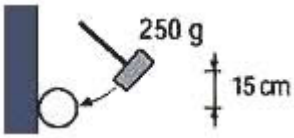
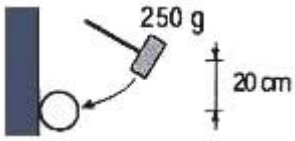
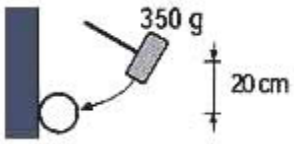
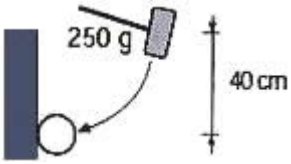
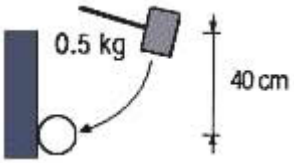
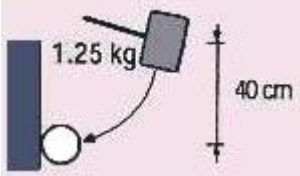
Tableau des indices de protection

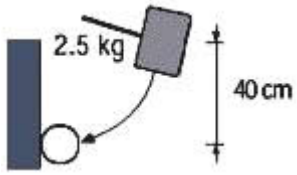
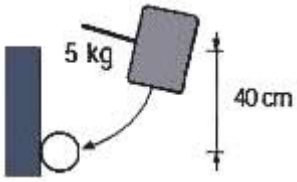
Indice de protection IP

	1er chiffre : Protection contre les corps solides			***2ème chiffre : Protection contre les liquides***	
IP	Tests	Définition	IP	Tests	Définitions
0		Pas de protection.	0		Pas de protection.
1		Protégé contre les corps solides supérieurs à 50mm. *Exemple :* contact involontaire de la main.	1		Protégé contre les chutes verticales de gouttes d'eau. *Exemple :* condensation.
2		Protégé contre les corps solides supérieurs à 12mm. *Exemple :* doigt de la main.	2		Protégé contre les chutes de gouttes d'eau jusqu'à 15° par rapport à la verticale.
3		Protégé contre les corps solides supérieurs à 2,5mm. *Exemple :* outils, fils.	3		Protégé contre les chutes de gouttes d'eau jusqu'à 60 ° par rapport à la verticale.
4		Protégé contre les corps solides supérieurs à 1mm. *Exemple :* outils fins, petits fils.	4		Protégé contre les projections d'eau de toutes les directions.
5		Protégé contre les poussières. Pas de dépôt nuisible.	5		Protégé contre les jets d'eau à la lance de toutes direction.
			6		Protégé contre les projections d'eau assimilables aux paquets de mer.
			7		Protégé contre les effets de l'immersion entre 0,15 et 1m.
			8		Protégé contre les effets de l'immersion prolongée sous pression.

Indice de protection IK

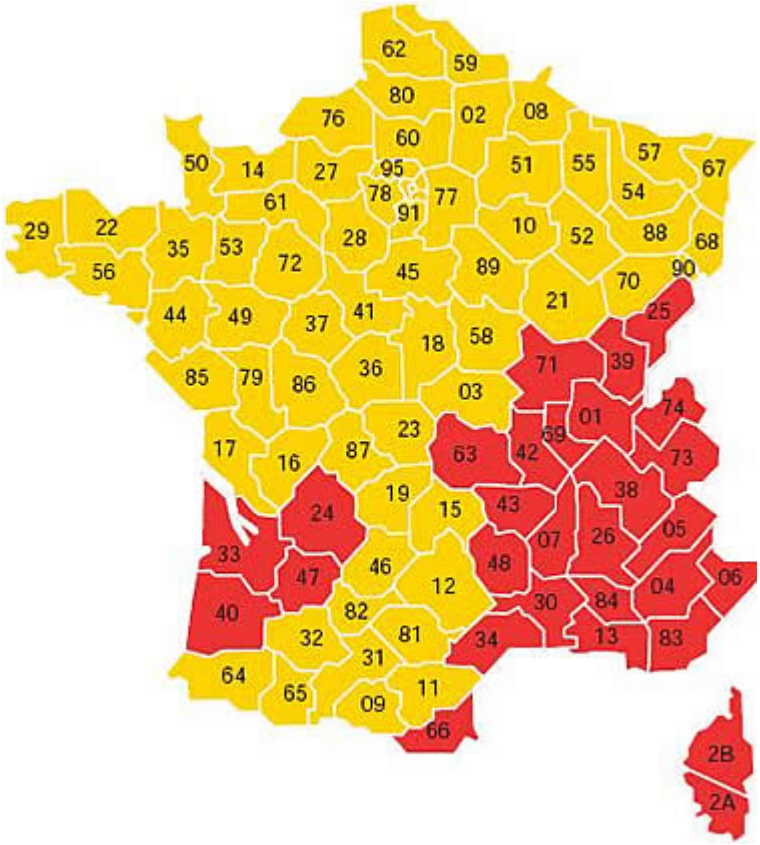
Protection mécanique

IK	Tests	Définition
00		Pas de protection.
01		Energie de choc 0,15J.
02		Energie de choc 0,20J.
03		Energie de choc 0,37J.
04		Energie de choc 0,50J.
05		Energie de choc 0,70J.
06		Energie de choc 1J.
07		Energie de choc 2J.
08		Energie de choc 5J.

09		Energie de choc 10J.
10		Energie de choc 20J.

Niveau kéraunique

Voici une carte montrant les différents niveaux kérauniques (nombre de jour par an où l'on entend le tonnerre) en France.



Niveau kéraunique ≤ 25

Niveau kéraunique > 25

DOM-TOM :
Guyane, Martinique, Guadeloupe : Nk = 40
Réunion :Nk = 20
St-Pierre et Miquelon : Nk = 1

Moyenne française = 20

Rappel : quand le niveau kéraunique est > 25 pour une alimentation BT par une ligne complètement ou partiellement aérienne, le parafoudre est obligatoire.

Il est obligatoire dans tous les cas si le bâtiment est équipé de paratonnerre.

Annexe 3 : Fiches pratiques

Ces fiches ont pour objectif de passer en revue les différents risques pouvant peser sur une salle ou des bâtiments abritant un ou plusieurs serveurs et des équipements techniques.

Les causes et les conséquences de chaque risque seront identifiées et les parades associées proposées dès les phases initiales du projet d'aménagement (ou de réaménagement) de ces salles ou de ce centre.

En outre, un lien sera effectué avec le document "Plan de continuité de l'activité" pour la prise en compte de dispositifs d'actions immédiates en cas de survenance de l'événement redouté.

Les risques passés en revue dans ce document sont :

Fiche 1 - Risques et parades liés à l'eau
Fiche 2 - Risques et parades liés à l'incendie et aux explosions
Fiche 3 - Risques et parades liés à l'électricité
Fiche 4 - Risques et parades liés à l'électricité statique et au phénomène d'électromagnétisme
Fiche 5 - Risques et parades liés à l'installation de la climatisation
Fiche 6 - Risques et parades liés aux télécommunications
Fiche 7 - Risques et parades liés à la foudre
Fiche 8 - Risques et parades liés à l'intrusion et à la malveillance interne
Fiche 9 - Risques et parades liés à la pollution et à la contamination
Fiche 10 - Risques et parades liés à l'organisation et aux procédures
Fiche 11 -Risques et parades liés à l'inaccessibilité du site

Les parades énumérées dans les pages suivantes n'ont en aucun cas l'ambition d'être obligatoires (puisque les parades doivent, par principe, être sélectionnées essentiellement en rapport direct avec la potentialité des menaces et l'ampleur des enjeux), ni exhaustives, ni suffisamment détaillées pour permettre une sélection en l'état. Il sera donc essentiel, au moment de la définition détaillée des parades à mettre effectivement en place sur un site donné, de procéder à une analyse réaliste des menaces, puis de se référer à une ou plusieurs des sources ou entités qualifiées dans les domaines considérés (expertise interne, professionnels des métiers concernés, cabinets de conseil spécialisés, organismes professionnels tels que le CLUSIF ou le CNPP, etc.).

Note : Pour pallier les risques majeurs il est fortement recommandé d'avoir un plan de continuité de l'activité. Les détails de ce plan sont décrits dans le document CLUSIF "Plan de continuité de l'activité – stratégie et solution de secours du Système d'Information".

Les parades ne seront vraiment efficaces que dans le cadre d'une approche organisationnelle adéquate, notamment en ce qui concerne la cohérence de la chaîne "détection-alarme-intervention".

Leur efficacité est liée à une formation adéquate du personnel : il est, en effet, parfaitement illusoire de mettre en place un système de détection sophistiqué, si personne ne sait interpréter les alarmes et/ou ne sait comment intervenir.

Fiche 1. Risques et parades liés à l'eau

Les risques liés à l'eau sont traités en détail dans le document "Problématique des risques liés à l'eau". Il pourra être utile de s'y reporter. Ce chapitre analyse les causes, les conséquences et les impacts d'un risque lié à l'eau.

Les causes

Les incidents pouvant conduire à un dégât des eaux peuvent être d'origines diverses, comme par exemple :

- Orages.
- Crues.
- Mauvaise maintenance (conduites, climatisation, installation de sprinkler, etc.).
- Mauvais entretien du bâtiment.
- Défaut d'étanchéité (façades, toitures).
- Extinction d'incendie.
- Etc.

Les conséquences

Les conséquences de ce type d'incident peuvent être par exemple :

- Inondations (débordement de rivières, fuites, etc.).
- Inaccessibilité ou indisponibilité du site ou des bâtiments.
- Infiltrations.
- Débordement ou panne des systèmes d'évacuation.
- Rupture de conduites.
- Fuite de condensateurs de climatisations.
- Déclenchement intempestif de sprinklers.
- Détérioration du matériel et des fournitures.
- Dégradation du faux-plancher ou du faux plafond.
- Courts-circuits électriques.
- Corrosion progressive.
- Risques d'électrocution.
- Inhibition de certaines alarmes.
- Etc.

Parades

Un certain nombre de mesures (dites "de prévention" ou de "protection") permet d'éviter que des incidents tels que ceux listés ci-dessus surviennent :

- Choix de l'implantation des salles les plus critiques ou de l'implantation du nouveau site en prenant en compte ce risque. Il faut éviter :
  - les sous-sols et rez-de-chaussée pour les risques d'inondations,
  - les derniers étages pour les risques d'infiltration par les toits,

    - les façades extérieures, surtout au vent dominant, pour éviter les ruissellements par les façades, etc.).
- Surélévation des équipements informatiques critiques.
- Surdimensionnement et doublement des équipements d'évacuation critiques. (drainage et pompes de relevage, etc.).
- Maintenance préventive des installations et du (ou des) bâtiment(s).
- Limitation des apports d'eau en salle ou dans les locaux attenants (climatisations hors salle ou, pour le moins, traitées spécifiquement, choix judicieux de l'emplacement des sanitaires, etc.).
- Choix des cheminements de toutes les conduites (sous pression ou non) à moindre risque, et toutes conduites apparentes, dans la mesure du possible.
- Conception d'un drainage efficace du bâtiment ou mise en place d'un cuvelage.
- Mise en place de bacs de rétention (avec détecteur de fluide ou évacuation par gravité en respectant les contraintes environnementales) sous tous les équipements ou conduites susceptibles de fuir.
- Disponibilité de plans des circuits, avec identification claire des systèmes de coupure.
- Existence de systèmes de détection d'humidité placés au point bas des salles.
- Existence de systèmes de détection et de localisation des fuites.
- Mécanismes de coupure automatique en cas de fuites.
- Prise en compte des contraintes logistiques nécessaires au basculement sur les installations informatiques de secours. (cf. Plan de continuité d'Activité – Stratégie et solutions de secours du système d'information CLUSIF-Sept. 2003).
- Construction d'une salle informatique étanche :
    - étanchéité à l'eau d'extinction : IP56 selon NFEN 60529,
    - étanchéité aux eaux stagnantes (Ex. : étanchéité 72h avec 40cm de hauteur d'eau à l'extérieur de la salle).
- Toutes les alarmes doivent être reportées et faire l'objet d'une procédure de traitement.
- Etc.

Avant la mise en œuvre des parades, une analyse de risques doit être menée pour les adapter à la réalité du risque.

De plus, ces parades ne seront vraiment efficaces que dans le cadre d'une approche organisationnelle adéquate. Un ensemble de préconisations doit être écrit, connu et appliqué, en particulier celles concernant le traitement des alarmes.

L'ensemble des aspects dégâts des eaux est traité de façon détaillée dans le document CLUSIF "Problématique des risques liés à l'eau".

Fiche 2. Risques et parades liés à l'incendie et aux explosions

Les incidents liés à l'incendie ou aux explosions pouvant conduire à une destruction totale ou partielle peuvent être d'origine accidentelle ou malveillante, interne ou externe.

Les causes

Les incidents pouvant conduire à un incendie ou à une explosion peuvent être d'origines diverses :

- Environnement (dépôt d'essence, stockage de forte masse combustible, zones sensibles ou à risques, environnement naturel, aéroport civil ou militaire, etc.).
- Voisinage direct de parking ou d'une voie publique.
- Court-circuit, échauffements ou mauvaise maintenance, surcharge des prises multiples, mauvais dimensionnement des installations, suite à un dégât des eaux, vétusté des installations, erreur humaine, malveillance. Les aspects électriques sont détaillés dans le chapitre "Risques liés à l'électricité".
- Négligence humaine (mégot, travaux sans ou avec mauvaise application du permis de feu, etc.).
- Mauvais stockage de matières inflammables ou de masse combustible.
- Explosion due au gaz (exemple : dans le local batterie).
- Foudre.
- Mauvaise maintenance des systèmes d'éclairage.
- Malveillance humaine.
- Etc.

Les conséquences

Les conséquences de ce type d'incident sont en général très graves, et peuvent être fatales à l'entreprise, car les moyens informatiques peuvent être rendus hors service pour une durée très longue.

- Une destruction partielle ou totale du site.
- Dommages au câblage et vieillissement prématuré.
- Dégagement de fumées (ex. : gaz corrosifs) : une contamination par les fumées, aux effets pervers durables.
- Des risques humains importants.
- Incendie.
- Dégâts des eaux suite à l'extinction d'un incendie (lances d'extinction ou évaporation de l'eau contenue dans les matériaux de construction de la salle).
- Déclenchement inopiné du système d'extinction qui peut conduire à la destruction partielle des structures de la salle et à la pollution des éléments actifs de la salle.
- La mise hors service des équipements de traitement, même en cas de sinistre limité (périmètre de sécurité inaccessible, contamination, dégâts des eaux successifs à l'extinction de l'incendie, mise hors service des équipements de sécurité...).

- Etc.

Parades

Pour la conception ou le réaménagement d'un site, les mesures de "prévention" et de "protection" permettent d'éviter que de tels désastres surviennent ou s'étendent.

- Plan d'évacuation des personnes.
- Education des personnes.
- La prise en compte des risques extérieurs (éviter le voisinage d'entités à risque).
- Une conception et une maintenance rigoureuses des installations électriques.
- Un compartimentage efficace des locaux en fonction des risques et enjeux (murs et portes coupe-feu, matériaux de construction "secs" selon ECB-S).
- Mise en place et maintenance de systèmes de détection et d'extinction incendie.
- L'absence de stockage de matières inflammables et de matériaux à forte masse combustible sans contrôle (cartons, palettes, etc.).
- Une bonne gestion des stocks et déchets d'emballage et de façonnage (localisation, évacuation).
- La réduction des risques de courts-circuits (séparation courants forts et courants faibles).
- La gestion de tous les chemins de propagation de feu (limitation des cloisons vitrées, choix judicieux des huisseries, confection soignée des passages de câbles et conduites, existence de clapets automatiques dans les gaines de climatisation, asservissement des climatisations et prises d'air...).
- Contrôler les accès et mettre en place des systèmes de détection intrusion pour limiter les actions malveillantes.
- Contrôler la sécurité des bureaux utilisateurs.
- Recours à une salle informatique étanche à l'eau (IP56 selon NFEN 60529) et aux gaz corrosifs (selon DIN 18095).
- Utilisation de matériaux secs pour la construction pour éviter l'augmentation du taux d'hygrométrie dans la salle soumise à un incendie à l'extérieur (voir norme ECB-S).
- Etc.

Le document CLUSIF "la sécurité incendie des équipements techniques" décrit tout ce qui concerne la détection et l'extinction incendie pour les équipements techniques, l'asservissement des moyens de climatisation et des alimentations électriques, etc.

Les règles APSAD définissent les recommandations en ce qui concerne les installations, elles sont actuellement conçues et diffusées par le CNPP (liste jointe en annexe).
Il est recommandé d'utiliser des produits certifiés et de les faire installer par des entreprises également certifiées.

En outre, un certain nombre de mesures organisationnelles (non liées directement à la conception du site, mais plutôt à sa prise en charge) seront décisives :

- Rédaction de règles de sécurité spécifiques pour les locaux sensibles (interdiction de fumer, de stocker des matières combustibles, etc.).

- Rédaction de procédures de réactions internes et externes vis-à-vis de l'incendie, rigoureuses et régulièrement testées, (Ex: procédure et plan d'évacuation d'urgence, et tests).
- Politique du bureau net.
- Conduite des actions de formation correspondantes, avant même la fin de l'emménagement sur le site.
- Surveillance des interventions extérieures (permis de feu, plan de prévention, rondes avant et après les interventions, etc.).
- Dépoussiérage régulier des plénums, des faux-planchers et de faux-plafonds par une société spécialisée.
- Choix judicieux des issues de secours et des moyens correspondants à mettre en place (sans compromettre les impératifs de contrôle des accès).
- Etc.

Fiche 3. Risques et parades liés à l'électricité

L'ensemble des équipements est sensible à la qualité et aux coupures intempestives d'électricité. Une interruption prolongée peut entraîner une cessation temporaire d'activité.

Causes

Les incidents qui peuvent aboutir à une interruption totale ou partielle de l'alimentation électrique ou à une altération de sa qualité peuvent être d'origine interne (par exemple court-circuit ou surcharge) ou externe (perturbations dues au fournisseur d'électricité) ; ils peuvent être aussi bien accidentels (erreur de manipulation lors d'interventions sur les installations électriques ou lors du branchement d'un nouvel équipement) que malveillants (sabotage d'un poste de transformation Basse-Tension).

Quelques exemples :

- Surcharge des prises multiples.
- Mauvais dimensionnement de la puissance installée par rapport à la puissance utile.
- Coupure et perturbation électrique d'origine interne (erreurs, proximité d'équipements perturbateurs, etc.).
- Défaillance du fournisseur d'énergie électrique (coupures, qualité).
- Mauvais emplacement ou protection insuffisante des dispositifs d'arrêt d'urgence (coup de poing, etc.).
- Intempéries (destruction de pylône, foudre, etc.).
- Sabotage des sources d'alimentation (transformateurs, groupes électrogènes, câbles, etc.).
- Câbles sectionnés accidentellement ou volontairement.
- Mise à la terre défectueuse (les supports de faux planchers, etc.).
- Défaillance mécanique de la connectique (par exemple suite à des vibrations).
- Incohérence des réseaux.
- Etc.

Conséquences

Les conséquences de ces types d'incident peuvent aboutir à un arrêt complet ou à un dysfonctionnement des équipements sensibles. Les mécanismes de sécurité ne doivent pas être affectés par une coupure électrique.

En outre, la brutalité de l'arrêt peut avoir des conséquences sur l'intégrité des données et sur le redémarrage des machines.

Quelques exemples :

- Perturbations électriques transmises.
- Perturbations électriques rayonnées.
- Références de potentiel multiple.
- Electricité statique.
- Foudre (voir le chapitre "Risques et parades liés à la foudre").

- Interruption de l'activité.
- Incendie.
- Humains.
- Etc.

Parades

Le document CLUSIF "L'alimentation électrique des systèmes informatiques" de 1996 constitue un document de référence.

Les parades élémentaires concernent :

- La structure et la source de l'installation.
- La conception et le dimensionnement des installations qui doivent être conformes aux normes et aux préconisations des professionnels du métier et des constructeurs informatiques, incluant notamment la mise en place de protections sélectives par équipement.
- L'homogénéité des installations.
- Les dispositifs de sécurité et de remplacement (redondance équilibrée des moyens de secours et des sources d'alimentation – onduleurs, batteries, groupes électrogènes, etc.).
- La protection contre la malveillance :
    - veiller à ce qu'aucun équipement sensible ne soit accessible de l'extérieur, par exemple inclusion des Tableaux Généraux Basse Tension (TGBT) dans le périmètre à accès et circulation contrôlés.
    - Contrôler les accès (cf. Chapitre "contrôles d'accès").
- Le choix de moyens d'éclairage étudiés (éclairages luminescents à starters antiparasités).
- La qualité des réseaux de protection et de terre (raccordement correct à la terre de tous les matériels (évacuation des charges électrostatiques) y compris les structures des faux-planchers, etc.).
- La qualité des câblages et des connexions (le blindage adéquat de tous les conducteurs véhiculant des intensités élevées, etc.).
- Outil de contrôle : thermographie infrarouge suivie d'une analyse identifiant les points anormalement chauds (voir le domaine 19 dans le référentiel en annexe).
- Suivi des consommations au niveau des armoires divisionnaires (les disjoncteurs sont calibrés pour un certain nombre de prises qui sont souvent multipliés par les utilisateurs (Prises multiples en cascade).
- La foudre (voir le chapitre "Risques et parades liés à la foudre").
- Recours à des condensateurs de compensation d’énergie réactive.
- Recours au filtrage actif.
- Etc.

Fiche 4. Risques et parades liés aux phénomènes électromagnétiques et électrostatiques

Les incidents liés aux phénomènes électromagnétiques et électrostatiques, souvent méconnus, parfois difficiles à diagnostiquer, peuvent entraîner une détérioration des équipements et nuire à l'intégrité des données. Il faut tenir compte également des niveaux d'émission électromagnétique des équipements réseau dans le cadre de l'hygiène et la sécurité des travailleurs. Les champs magnétiques intenses sont également la cause de troubles pour les matériels et pour les travailleurs.

Causes

Les causes sont d'origines diverses, par exemple :

- Des situations où le Centre est affecté par des rayonnements ou des accumulations de charges parasites d'origine externe (phénomènes atmosphériques, émissions radios ou radars, proximité de machines tournantes puissantes, appareils électriques à décharges tels que des éclairages luminescents comme les néons, ...).
- Des situations inverses où les rayonnements sont générés par le site et peuvent avoir une influence sur l'environnement.
- Bien que ces deux types de risque ne soient théoriquement pas nuls, ils sont très improbables, en particulier du fait que les fabricants de matériels doivent se conformer aux normes de compatibilité électromagnétique (Immunité des équipements 10V/m ou 3V/m selon les applications). Les équipements de transmission hertziens peuvent par contre susciter de l'inquiétude chez les travailleurs et les riverains. Les niveaux d'émission des répéteurs Wifi à proximité des postes de travail permanents doivent être gardés au-dessous d'un seuil réglementaire (100 mW puissance rayonnée max., 3V/m mesuré au poste de travail, limite qui pourrait être abaissée à 0,6 V/m par un projet de loi en discussion – projet de loi 2491).
- Des situations de type malveillant, où les rayonnements électromagnétiques émis par les matériels de traitement du site sont captés par des parties tierces, dans le cadre de tentatives d'atteinte à la confidentialité. Bien que ce risque soit limité, il est bien réel.
- Proximité de transformateurs de puissances ou de lignes d'alimentation à fort courant générant des champs magnétiques intenses.
- Revêtements muraux et des sols mal adaptés et générant de l'électricité statique.
- Hygrométrie mal gérée.
- Téléphones mobiles.

Conséquences

Les conséquences peuvent être :

- Des dysfonctionnements (souvent apparemment aléatoires) des matériels de traitement ou une perte d'intégrité des informations stockées sur des supports magnétiques.
- Le déménagement du site en raison des rayonnements émis.
- La divulgation d'informations confidentielles (captation de données à distance, etc.).
- Des perturbations des communications.
- Inconfort au poste de travail (migraines, flicker sur les écrans).

- Effets à long termes mal connus mais probablement négatifs (altérations cellulaires, problèmes cardiaques, effets sur le système nerveux, reproducteur,…).
- Etc.

Parades

Les parades peuvent être :

- Le choix judicieux du site du Centre (éloignement d'émetteur radio ou radar puissants).
- Le bannissement dans les endroits les plus critiques des matériaux et éléments générateurs de charges (les corbeilles en plastique, et même les fauteuils à roulettes aux postes les plus critiques, tels que dans "l'atelier" de préparation/réparation des micros, etc.).
- Un choix judicieux des revêtements (non-accumulation des charges).
- Le maintien du degré hygrométrique.
- La suppression de tous les moyens de fixation de nature magnétique (aimants, tableaux...) à proximité immédiate des équipements.
- Le choix de l'emplacement des matériels et supports les plus critiques (loin de blocs tournants puissants tels que des machineries d'ascenseurs ou des machines industrielles pour les problèmes d'induction, loin des conducteurs aériens ou souterrains à haute tension, loin des parois et voies d'accès...).
- L'installation de cages de Faraday (enceinte métallique fermée, salle munie de tapisserie métallisée, salle revêtue de feuillard de cuivre ou d'acier soudé en continu). et ou de matériel "Tempest" (utilisation de filtres sur les câbles).
- Le respect des réglementations en matière de niveaux d'émission de radiations électromagnétiques et des directives européennes de compatibilité électromagnétique (CEM : Directive Européenne 89/339, 2004/108). Se méfier en particulier de l'installation de routeurs ou répéteurs amplificateurs, antennes directives de manière anarchique.
- Le respect des réglementations en matière de niveau de champs magnétiques : (EN61000-4-8 : immunité des équipements électroniques 3,75 µT [micro-Tesla], EN55024 : immunité des équipements informatiques 1µT, niveau recommandé pour les êtres humains : < 1 µT – US National Council on Radiation Protection – WG 89-3).
- Eloigner les équipements et les postes de travail des sources de champs magnétiques intenses et si c'est impossible, utiliser des protections à base de plaques de matériaux ferro-magnétiques qui annulent ces champs ou les réduisent dans des limites acceptables.
- L'interdiction ou la réglementation des téléphones mobiles à proximité des équipements techniques.
- La mise à la terre de tous les équipements sans oublier le faux-plancher.
- Etc.

Fiche 5. Risques et parades liés à l'installation de la climatisation

La climatisation dans une salle serveurs joue généralement deux rôles : le maintien de la température et celui de l'hygrométrie nécessaires au bon fonctionnement des appareils.

Causes

Les incidents, pouvant être à l'origine d'un dysfonctionnement ou d'une interruption des fonctions de climatisation, sont par exemple :

- Une défaillance du fournisseur d'alimentation électrique.
- Une coupure de l'alimentation d'eau (pour les climatisations à eau perdue).
- Une défaillance du fournisseur d'eau glacée.
- Une panne ou un dysfonctionnement des installations de climatisation.
- Une fuite du fluide frigoporteur.
- Un sabotage des installations, particulièrement en ce qui concerne les mécanismes d'évacuation des calories (aérothermes par exemple).
- Les effets du rayonnement solaire direct.
- Filtres encrassés en raison d'une eau trop calcaire.
- Capacité insuffisante en cas de conditions climatiques exceptionnelles.
- Configuration inadaptée en cas de modification (ajout, remplacement, déplacement, suppression, etc.) de matériels en trop grand nombre.
- Déclenchement des détecteurs d'incendie au moment du rechargement en gaz de la climatisation.
- Déclenchement inopiné des détecteurs d'incendie suite à diffusion de fumées en provenance de l'extérieur par les conduites de climatisation.
- Etc.

Conséquences

Les conséquences de ce type d'incident peuvent être par exemple :

- Une hausse de température, localisée ou généralisée, dommageable aux équipements (dilatations, chocs thermiques...).
- Un vieillissement prématuré des composants.
- Fréquemment, la nécessité de l'arrêt des matériels informatiques en attendant la remise en route des installations.
- Une détérioration des batteries de secours.
- Détérioration du degré hygrométrique.
- Etc.

Parades

La sécurité de la climatisation des équipements prend en compte les points suivants :

- Etude du système de climatisation en fonction de l'ensemble du site.
- Circulation de l'air adéquate axée sur les parties produisant de la chaleur.
- Mise en place impérative d'une redondance sur toute la chaîne climatique.
- Etude soigneuse de l'alimentation électrique des équipements frigorifiques, avec onduleurs.
- Mise en place de protections contre les rayonnements solaires directs.
- Bonne répartition des dalles perforées.
- Bonne hauteur de faux-plancher.
- Alternance allées chaudes, allées froides.
- Maintenance régulière des systèmes.
- Redondance des systèmes.
- Remontée des alarmes au poste centralisé.
- Etc.

En outre, il pourra être nécessaire de considérer :

- La mise en place de processus cohérents de détection des défauts.
- La définition et la construction d'asservissements permettant de limiter la détérioration des équipements (mise hors tension automatique des unités de traitement).
- L'inclusion de tous les éléments critiques (vannes, aérothermes, bâches de réserve...) dans le périmètre à accès et circulation contrôlés.
- La disponibilité permanente d'un stock de secours des composants essentiels.
- Etc.

Fiche 6. Risques et parades liés aux télécommunications

Une interruption des télécommunications peut entraîner des conséquences graves sur l'ensemble de l'entreprise.

L'accès aux équipements réseaux et au câblage peut favoriser les atteintes aux informations confidentielles, leur divulgation voire leur intégrité.

Causes

Quelques-unes des situations pouvant se produire sont par exemple :

- Rupture de liaisons de télécommunication (internes ou externes).
- Problèmes des "coups de pelleteuse".
- Interruption momentanée du service des fournisseurs (accident, qualité, grève, etc.).
- Malveillance.
- Mauvaise conception du câblage.
- Dysfonctionnement des télécommunications.
- Perturbations.
    - électriques (cf. chapitre ad hoc),
    - dues à la foudre (cf. chapitre ad hoc),
    - environnementales (de ou vers les autres).
- Panne ou destruction involontaire ou volontaire d'un équipement.
- Suite d'un incendie localisé.
- Mauvais positionnement d'une borne WIFI.
- Incompatibilité du WIFI avec les matériaux de construction.
- Accès non contrôlé aux équipements réseaux.
- Rongeurs et divers nuisibles.
- Etc.

Conséquences

Les conséquences de ce type d'incident peuvent être par exemple :

- Des interruptions ou des dégradations de service.
- Désactivation de dispositifs de sécurité (télésurveillance), pouvant entraîner une interdiction d'accès ou libérer tous les accès.
- Isolement total ou partiel du centre (service de messagerie, téléphonie, etc.).
- Perturbations entre des câbles de différentes catégories.
- Possibilité de vols de matériel.
- Etc.

Parades

Les mesures de prévention/protection permettant d'éviter que de tels incidents se produisent sont par exemple les suivantes :

- La protection efficace des têtes de lignes et locaux de télécommunication.
- La protection des liaisons extérieures (gainages, grillages, avertisseurs...).
- Le choix soigneux du type de câbles utilisés (blindage).
- La pose enterrée des liaisons extérieures.
- La séparation des cheminements courant forts / faibles.
- Etiquetage des câbles.
- Choix des matériaux (notamment si WIFI installé).
- Protection contre l'intrusion physique permettant une prise de contrôle sur les équipements (cf. chapitre intrusion physique).
- La mise en place d'un plan de continuité des opérations en cas d'incidents graves.
- Le doublement des liaisons de télécommunication sur deux centraux distincts (si possible) ou, au moins, si les liaisons sont critiques, la souscription d'un abonnement avec chemins d'accès distincts. Limiter toutefois la multiplication des points de pénétration dans la salle.
- Le doublement de tous les équipements critiques. (rocade, câbles, matériels, etc.).
- Le recours à des liaisons d'autres types de technologie (sans fil, mobile, voix sur IP etc.).
- Le recours à des opérateurs redondants.
- La vérification de l'accessibilité des chemins de câbles (et la disponibilité de la documentation correspondante).
- La protection contre la foudre de toutes les installations de télécommunication (Cf. chapitre foudre).
- La mise en place de moyens de détection des écoutes en ligne.
- Installer les points d'accès WI-FI dans les salles fermées à clé et près du plafond.
- Etc.

Il pourra être utile de se référer au document CLUSIF " Sécurité physique des éléments d'un réseau local".

Fiche 7. Risques et parades liés à la foudre

Les incidents liés à la foudre pouvant conduire à une surtension brutale, voire à un incendie sont toujours d'origine naturelle.

Causes

Les situations résultant de foudre "directe", celles où la foudre tombe sur un ou des éléments des installations, sont à séparer des situations de foudre "indirecte", celles où la foudre est tombée en un point pouvant être assez éloigné des installations, mais "remonte" ou rayonne jusque dans les bâtiments (terres électriques, alimentation électrique, circuits de télécommunications, réseaux de télécommande ou de télésurveillance internes, câblage terminaux, etc.). Dans tous les cas, le résultat aboutit à des surtensions violentes et/ou à l'émission de champs électriques intenses.
L'onduleur-chargeur étant protégé par des filtres d'alimentation, les équipements informatiques branchés en aval ne nécessitent pas de protection au niveau alimentation électrique, en revanche, ils restent sensibles du point de vue du réseau de télécommunication.

Conséquences

Les conséquences de ce type d'incident peuvent être par exemple :

- Une perturbation des traitements des données informatiques, consécutive aux perturbations des champs électriques.
- La destruction des circuits électriques et/ou électroniques.
- La mise hors service de dispositifs de sécurité.
- L'électrocution de personnels.
- Incendie.
- Etc.

Parades

Les mesures de prévention permettant d'éviter que de tels incidents ne se produisent sont par exemple les suivantes.
Voir en fonction de l'indice kéraunique :

- Le choix de l'implantation des installations en dehors de zones à risque.
- L'absence de dispositions constructives susceptibles d'attirer la foudre.
- La mise en place, dans les zones exposées, de câbles ne permettant pas la remontée de la foudre (fibres optiques), en particulier pour les liaisons inter-bâtiments.
- Dans le même esprit, la segmentation des installations (raccordement des équipements par modems à isolement galvanique).
- Construction d'une "cage maillée" autour des installations critiques (les termes de "Cage de Faraday" sont souvent, improprement employés ; ces dernières sont effectivement efficaces contre la foudre directe, mais elles sont plutôt destinées à protéger des champs électromagnétiques, et leur prix est beaucoup plus élevé que la cage maillée).
- Mise en place de paratonnerres (dans le cadre d'études bien spécifiques).

- Installation de para-surtenseurs de puissance adaptée.
- Installation de parafoudres, cependant il y a deux approches possibles : mettre un paratonnerre et alors augmenter le risque de chute de foudre sur le bâtiment et donc de remontée par la terre et ne pas en mettre et devoir alors protéger chaque départ et liaison externe ; le choix dépend en fait du degré d'exposition du site (ou indice kéraunique), donnée qu'il est possible de procurer auprès des services départementaux de l'environnement (cf. la carte de France en annexe).
- Vérifier la protection au niveau électrique de l'ensemble des équipements interconnectés.
- Forage d'un puits pour mise à la terre.
- Etc.

Fiche 8. Risques et parades liés à l'intrusion et à la malveillance interne

Les incidents liés à l'intrusion et à la malveillance interne pouvant conduire jusqu'à une destruction totale ou partielle sont toujours d'origine humaine malveillante, interne ou externe.

Causes

Les risques liés à l'intrusion et à la malveillance interne peuvent provenir de :

- Intrusion et circulation de personnes non autorisées.
  - individu externe,
  - ancien salarié,
  - individu interne mais non autorisé pour une zone donnée.
- Action de malveillance de personnel interne (salarié, sous-traitant, etc.).
  - frustration,
  - sabotage,
  - vengeance,
  - personne devenue incontrôlable,
  - etc.
- Action de groupes (occupations de locaux, saccage, blocage du site).
- Action d'intelligence économique active.
- Terrorisme.

Conséquences

Les conséquences sont nombreuses à partir du moment où un intrus malveillant a pu pénétrer dans les locaux, par exemple :

- Vols de matériels (critiques ou non).
- Pertes de confidentialité (vol ou copie de documents ou sauvegardes, vol d'équipements, mise en place de bretelles d'écoute).
- Pertes d'intégrité.
- Sabotages (avec éventuellement mise hors service des mécanismes de sécurité).
- Indisponibilité des installations.
- Atteinte aux personnes (prise d'otage, coups et blessures, menaces, etc.).

Parades

Les parades sont divisées en deux parties, la partie physique et la partie organisationnelle. La partie organisationnelle est traitée dans le chapitre "Risques liés à l'organisation et aux procédures"

Les principales parades périphériques et périmétriques sont :

- Protection périphérique par :
  - Clôtures (grillage, concertinas, double clôture, etc.).

- Détection anti-intrusion (caméras, barrière infrarouge, alarme, détecteur d'approche, détection de coupure de circuit, détection de vibrations, détection des chocs).
- Contrôle d'accès évolué et rigoureux à la périphérie sous contrôle ou non du poste de gardiennage.
- Plots, herses anti-véhicules.
- Rondes.
- Chiens.
- Phares anti-intrusion.
- Etc.

- Protection périmétrique par :
  - La mise en place de protections passives par une ou des enceintes étudiées en fonction des risques (solidité des murs, mise en place de blindages, conceptions de type "bunker"...).
  - La limitation du nombre de baies ouvrant sur l'extérieur, et leur renforcement (produit verrier, barreau, volet, etc.).
  - La solidité des portes et des huisseries et la limitation du nombre de portes.
  - Homogénéité des mesures de protection de l'ensemble : murs, portes, serrures, groom…
  - Mesures particulières pour le quai de livraisons (sas, contrôle d'accès spécifique, etc.).
  - Le choix judicieux de l'implantation, du type et de la surveillance des issues de secours.
  - Détecteur d'ouverture ou de chocs (porte, fenêtres, etc.).
  - Caméras installées dans le respect de la législation en vigueur.
  - Radars (volumétrique, hyperfréquence, mixte, etc.).
  - Agents de prévention et de sécurité (dispositif d'alerte, etc.).
  - Contrôle d'accès adapté aux risques (badges, biométrie, digicodes, accompagnement des visiteurs, etc.).
  - Mettre en place un système d'identification des visiteurs (une banque d'accueil adéquate).
- Protection des locaux ou équipements sensibles.
  - Sirènes.
  - Local rendu opaque par des fumées.
  - Contrôles d'accès évolué et rigoureux pour les locaux ou équipements sensibles.
  - Certains des contrôles périmétriques peuvent également être utilisés pour la protection des locaux internes.
  - Portiques sécurisés (en entrée ou sortie) et puces sur les matériels.
- Dans tous les cas, une protection active par détection de présence, avec un report des alarmes vers un PC de surveillance 24h/24h.
- Ne pas laisser à la vue des visiteurs non concernés les matériels les plus critiques.

Fiche 9. Risques et parades liées à la pollution ou à la contamination

Les incidents liés à la pollution ou à la contamination pouvant conduire à la détérioration des équipements et pouvant aller jusqu'à nuire à la sécurité des personnes, peuvent être d'origine accidentelle ou malveillante, interne ou externe.

Causes

Les incidents pouvant conduire à une pollution ou à une contamination d'une salle serveur sont, par exemple :

- L'existence de vapeurs corrosives.
- La présence de poussières (environnement, travaux, éditions massives, etc.).
- Les conséquences induites d'un incendie (fumées, vapeur d'eau, brouillards d'eau, etc.).
- Les suites d'un accident ou d'une erreur (ex. déclenchement intempestif du système d'extinction à gaz).
- Le risque chimique.
- Le risque bactériologique (légionellose, etc.).
- La radioactivité.
- La négligence (défaut de maintenance et d'entretien).
- Climatisation défaillante.
- La malveillance.
- Acidité de l'eau.
- Présence d'équipements polluants (imprimantes, frottement de câbles, etc.).
- Stockage des produits d'entretien mal adapté (ménage, etc.).
- Travaux (une des causes importantes de pollution si des protections ne sont pas utilisées).
- Présence de matériaux interdits en cas réutilisation de locaux existants (amiante, plomb, etc.).
- Etc.

Conséquences

Les conséquences de ce type de situation peuvent par exemple être :

- Les conséquences sur la santé des personnes (indisponibilité, maladie, etc.).
- L'indisponibilité des systèmes (par manque de personnel ou impossibilité d'entrer dans la salle).
- La responsabilité civile ou pénale de l'entreprise et de ses dirigeants.
- Une altération ou destruction plus ou moins progressive des circuits internes des équipements informatiques.
- Masquage de têtes de lecture des unités disques.
- Altération des contacts.
- La contamination et la détérioration des isolants électriques.

- La perte d'isolement entre les conducteurs.
- La détérioration des propriétés diélectriques.
- La réduction de la conductivité thermique.
- L'encrassement des filtres à air (climatisation, équipements "air neuf", etc.).
- Détérioration des parties mécaniques en mouvement.
- Des dysfonctionnements consécutifs à un taux (ou des caractéristiques) de poussières supérieur aux spécifications des constructeurs.
- Un échauffement anormal des équipements dû à la baisse d'efficacité de la climatisation.
- Un échauffement anormal des équipements dû à l'encrassement de leurs filtres.
- Un déclenchement intempestif du système d'extinction incendie.
- Des risques de court-circuit.
- Un dérèglement des systèmes de régulation d'hygrométrie.
- Etc.

Parades

Les mesures de prévention/protection permettant d'éviter que de tels incidents se produisent sont par exemple les suivantes :

- Un choix approprié du site (absence de voisinages générateurs de vapeurs corrosives ou poussiéreuses).
- Un cloisonnement des circulations d'air en cas d'incendie (portes coupe-feu, clapets automatiques dans les gaines de climatisation...).
- Surveillance de l'étanchéité des cloisons et des huisseries.
- Un choix pertinent de tous matériaux de construction et revêtements (ne générant ni ne retenant de poussières, peintures, revêtements muraux, revêtements de sol, etc.).
- Eviter les faux-plafonds à dalles minérales qui ont tendance à s'effriter.
- La peinture anti-poussières des surfaces sous faux-plancher.
- Système d'évacuation des eaux dans le faux-plancher pour pallier les fuites et les conséquences de l'extinction d'un incendie.
- Protection et contrôles efficaces des arrivées d'air (sas, etc.) extérieures.
- Un filtrage approprié des apports d'air neuf.
- Une limitation des apports d'air neuf au strict nécessaire.
- Des dispositifs de nettoyage adaptés (aspiration centralisée).
- Un fonctionnement sous atmosphère neutre et en surpression.
- Un isolement (y compris pour les plénums) des zones génératrices de poussières (locaux d'impression et de façonnage).
- Dépoussiérage et nettoyage réguliers : opérer un dépoussiérage complet des salles serveurs au moins une fois par an (entreprises spécialisées).
- Système d'aspiration de l'air efficace (désenfumage).
- Protection des équipements en cas de travaux en salle.
- Professionnalisme des intervenants de nettoyage (entreprise spécialisée).
- Moyens utilisés (pour éviter le recyclage des poussières).

- Cohérence de ces nettoyages (plénums sous faux-planchers et faux-plafonds), et fréquences (au moins annuel).
- Le respect des interdictions de fumer.
- Contrôles réguliers du niveau bactériologique des équipements de climatisation.
- Etc.

Fiche 10. Risques liés à l'organisation et aux procédures

Les différents risques ont souvent pour origine le facteur humain, ce qui nécessite une organisation et des procédures efficaces.

Causes

Les principales causes de dysfonctionnement liées à l'organisation et aux procédures sont :

- Non-engagement formel de la direction.
- Organisation inadaptée.
- Laxisme du management.
- Absence de gestion efficace suite aux incidents.
- Formation insuffisante.
- Gestion des ressources humaines incomplète.
- Définition des responsabilités peu claire (en particulier en ce qui concerne les aspects sécurité).
- Personnes "clés", dont l'absence peut provoquer un dysfonctionnement.
- Procédures inadaptées, incomplètes, peu claires, non régulièrement testées, non écrites.
- Réactions en cas d'alarme, inexistantes ou inappropriées (consignes, formation, etc.).
- Etc.

Conséquences

Les principales conséquences sont :

- Interruption de l'activité.
- Non-conformité par rapport aux exigences du marché (clients, réglementation, assurance, etc.).
- Dégradation rapide du niveau de sécurité dans les salles.
- Laxisme du personnel.
- Difficultés dans la prise de décision en cas de crise ou d'incidents.
- Actions inappropriées.
- Personnel non adapté au poste occupé.
- Alarmes non traitées : un incident mineur peut prendre de l'ampleur sans contrôle.
- Pertes financières ou d'image de marque.
- Etc.

Parades

Les différentes parades reposant sur le facteur humain, une organisation doit être mise en place, basée sur un ensemble de procédures.

- Un engagement formel de la direction (document écrit largement diffusé).

- Entretiens d'embauche prenant en compte la motivation des candidats vis-à-vis de la sécurité.
- Enquêtes préalables, dans le respect de la législation en vigueur, en fonction de la spécificité de certains postes.
- Le contrat d'embauche doit inclure des clauses précises concernant la sécurité.
- Les contrats des sous-traitants doivent comprendre des clauses de sécurité adaptées aux missions confiées.
- La formation à la sécurité doit être régulière.
- Des procédures doivent prendre en compte l'ensemble des aspects sécurité. (hiérarchisation et gestion des contrôles d'accès, gestion des clés, gardiennage, etc.).
- Procédure de traitement des alarmes.
- Mettre en œuvre des procédures généralisées d'interception des visiteurs non identifiés.
- La mise en place de dispositifs antivol sur les matériels les plus tentants ou les plus critiques.
- Un certain nombre de mesures possibles est abordé dans les ouvrages "Contrôle d'accès et détection intrusion physique" et "Contrôles d'accès par la biométrie" du CLUSIF.
- Audits réguliers en interne ou par un organisme extérieur agréé.

Enfin, il faudra prendre en compte tous les aspects organisationnels, non directement liés aux dispositions constructives des salles serveurs, mais plutôt à leur prise en charge :

- Disponibilité permanente de documentations adaptées.
- Souscription d'un contrat de maintenance (préventif et curatif) efficace avec ou sans astreinte.
- Rédaction et test des procédures d'intervention.
- Etc.

Fiche 11. Risques et parades liés à l'inaccessibilité du site

Les risques liés à l'inaccessibilité du site sont souvent la conséquence de la réalisation d'un des événements décrits dans ce chapitre.

Causes

Cette situation peut résulter de circonstances d'ordre accidentel ou malveillant :

- Catastrophe naturelle.
- Accidents dans le voisinage.
- Moyens de transport hors service.
- Mouvements sociaux internes et externes.
- Manifestations ou émeutes.
- Attentats.
- Mise en place de cordons de sécurité par les autorités.
- Risques décrits précédemment.
- Etc.

Conséquences

Les conséquences de ce type d'incident peuvent être par exemple :

- Arrêt du système d'information du fait de l'impossibilité des personnels d'exploitation d'y accéder.
- Destruction ou mise hors service d'équipements sensibles.
- Impossibilité de faire fonctionner le site par occupation des locaux.
- Déclenchement éventuel du plan de continuité des activités.
- Etc.

Parades

Les mesures de prévention/protection permettant d'éviter la survenance de telles situations sont par exemple :

- Le choix approprié du site (hors zone inondable ou susceptible d'être l'objet de séismes ou glissements de terrains, multiplicité des chemins d'accès, identification des barrières de dégel possibles, choix de régions et/ou de voisins réputés peu susceptibles d'être l'objet de mouvements sociaux et/ou d'actes de terrorisme,...).
- Limitation à l'essentiel des accès au site (ce qui exclut les visites de prestige, et encourage la spécialisation du site aux seuls usages du site).
- Absence d'affichage ostensible de l'identité et des missions du Site.
- La protection du site contre l'intrusion (méthodes actives et passives).
- La protection au moins aussi évoluée de tous les éléments essentiels au fonctionnement du site (TGBT et groupes électrogènes, condenseurs, entrées d'apport d'air...).
- Gestion des infrastructures à distance.
- Etc.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr