Bundesministerium
des Innern

Protection d’infrastructures critiques – Concept de base de protection

Recommandations destinées aux entreprises

www.bmi.bund.de

Préface

Les infrastructures occupent dans nos sociétés des fonctions critiques. Nous sommes en effet tributaires du fonctionnement fiable de l'approvisionnement en énergie et en eau, ainsi que de la fluidité des techniques de l'information et, d'une manière générale, de la mobilité garantie des échanges. Si ces systèmes ou d'autres infrastructures importantes sont défaillants à une plus grande échelle, même pour une courte durée, cela peut avoir de lourdes conséquences.

Les attentats à New York et à Washington le 11 septembre 2001, à Madrid le 11 mars 2004 et à Londres les 7 et 21 juillet 2005 ont montré de manière très significative le danger qui menace les sociétés modernes. La lutte contre le terrorisme international et la protection de la population contre cette menace exigent par conséquent une vigilance toute particulière des autorités chargées de sa sécurité.

Outre la défense contre les attentats terroristes, il convient de prendre également en considération d'autres menaces ou dangers Ainsi les catastrophes naturelles telles que les inondations peuvent entraîner des dégâts tout à fait considérables.

Il faut donc aborder de manière globale la notion de protection d'infrastructures dites critiques, c'est-à-dire celle des équipements et des organisations revêtant une importance toute particulière pour la société et dont la défaillance et la perturbation créeraient des blocages durables dans l'approvisionnement, des dysfonctionnements importants en matière de sécurité publique ou d'autres conséquences dramatiques. L'Etat et l'industrie ont donc tout intérêt à renforcer

leur dialogue sur ce sujet et à développer ensemble des solutions visant à plus de sécurité.

Le ministère fédéral de l'Intérieur, l'Office fédéral pour la protection des populations et la gestion des catastrophes et l'Office fédéral de police criminelle (BKA) y ont apporté leur contribution en élaborant un concept de protection de base. Ce projet a bénéficié d'emblée du soutien et de la collaboration active d'experts en économie. Le ministère fédéral de l'Intérieur tient à cet égard à adresser ses remerciements pour leur soutien aux délégués en charge de la sécurité suivants :

- de la société allemande de chemins de fer (Deutsche Bahn AG), Monsieur Jens Puls,
- de la société allemande du contrôle de la circulation aérienne (Deutsche Flugsicherung GmbH), Monsieur Hans-Jürgen Morscheck,
- de la société Deutz AG, Monsieur Werner Becker,
- de la société IBM Deutschland GmbH, Monsieur Klaus Hintz,
- de la société Vattenfall Europe AG (transmission), Monsieur Thomas Schäfer

et leurs collaboratrices et leurs collaborateurs.

Grâce à ce concept de protection de base, des recommandations relatives à la sécurité intérieure sont mises à la disposition des entreprises allemandes. Cette notion de sécurité élevée des infrastructures constitue un authentique label de qualité propre à l'Allemagne. Il est dans l'intérêt élémentaire des entreprises, des citoyennes et des citoyens de notre pays d'assurer son application sur le long terme.

Table des matières

Résumé

Le présent concept de protection de base a pour objectif de **réduire la vulnérabilité des infrastructures critiques** face aux événements et accidents naturels ainsi qu'aux attentats terroristes et aux actes criminels. Dans cet objectif, le concept de protection de base se concentre sur les mesures de protection relatives à la construction, à l'organisation, aux personnes et à la technique.

Point de départ de la gestion du risque

L'exigence d'un concept de protection de base résulte entre autres des dispositions légales et des normes généralement admises[1], mais aussi des principes d'entreprise généralement admis d'une gestion prévisionnelle des risques et d'une planification stratégique tournée vers le succès et la continuité – par exemple dans le cadre dudit plan de continuité d'activités (PCA).

Destinataire : Direction d'entreprise

Les destinataires du développement de **concepts stratégiques** pour les analyses des menaces, les systèmes de gestion du risque et de mesures de minimisation du risque sont avant tout les directions d'entreprise des exploitants d'infrastructures qui, en cas d'infractions, ont à assumer le risque de l'entreprise, voire le cas échéant, les éventuels risques de responsabilité. Les interlocuteurs chargés de l'**application** de ces concepts stratégiques dans l'entreprise sont, en règle générale, les responsables de la sécurité. En fin de compte, la mise en application du concept de protection de base est une mission touchant l'ensemble de l'entreprise qui requiert un soutien à tous les niveaux.

La condition sine qua non pour concrétiser les mesures de protection de grande envergure est la **collaboration** basée sur la confiance **entre Etat et exploitants d'infrastructures**. Les exploitants sont ceux qui disposent des connaissances détaillées suffisantes sur leurs infrastructures et peuvent appliquer efficacement les mesures concrètes de protection. Il est donc

[1] Par exemple : les normes de l'article 91 de la loi sur les sociétés anonymes (mise en place des systèmes de gestion du risque et de surveillance), de l'ordonnance sur les accidents majeurs, des obligations générales et particulières supplémentaires des exploitants et des réglementations légales spécialisées ou bien également du nouvel accord sur les fonds propres « Bâle II ».

d’abord indispensable de s’entendre sur le **niveau de protection** qui est visé ou acceptable.

Processus d’analyse et de planification

Le point de départ est un processus d’analyse et de planification multiétagé qui comprend une évaluation des risques, suivi d’un contrôle ainsi qu’une adaptation des mesures de protection. Il peut être divisé comme suit :

I. La formation des catégories de risques, classées selon les différents domaines : catastrophes naturelles, accidents, terrorisme et criminalité,

II. la fixation du niveau respectif de protection basée sur ces catégories,

III. la conception de scénarios de sinistre et de menace,

IV. l’analyse des points faibles,

V. la formulation des objectifs de protection et la fixation des mesures de protection et contre-mesures qui en découlent,

VI. la formulation de l’urgence respective (coordination entre mesures publiques et privées),

VII. la mise en application du besoin d’action formulé et

VIII. le contrôle régulier de ce processus d’analyse et de planification dans le cadre de la gestion de la qualité.

Les dangers éventuels pour les infrastructures critiques seront présentés comme premier point de repère. Il comprend essentiellement les risques liés aux événements naturels, à une erreur humaine ou défaillance technique, au terrorisme ou aux actes criminels. Ces risques permettent d’identifier les zones particulièrement menacées dans l’entreprise et d’en déduire les recommandations de protection de base généralisées.

Là où ce processus est ressenti comme étant trop fastidieux ou difficilement applicable en raison du manque de ressources, par exemple dans **les petites et moyennes entreprises (PME)**, il peut s’avérer être tout à fait pertinent d’approcher le sujet par petites étapes et d’attaquer d’abord les aspects individuels, ressentis comme étant particulièrement urgents du concept de base de protection.

Catalogue de questions/liste de contrôle

Un catalogue de questions et une liste de contrôle (annexe 1) avec lesquelles travaillent les exploitants des équipements d'infrastructure ont été conçus comme une aide pour l'application du concept de protection de base. Comme instruments interdisciplinaires, les catalogues de questions et la liste de contrôle doivent contribuer avant tout à initier **un processus de discussion interne à l'entreprise** concernant le renforcement de la sécurité et à le diriger de façon ciblée. Le catalogue de questions et la liste de contrôle ne sont pas **des listes finales**, il s'agit uniquement de modèles; il s'ensuit que les points manquants devront être complétés dans le cadre de ce processus ou que, le cas échéant, les questions non pertinentes pourront être modifiées ou rayées.

L'objectif de cette étape de conception est d'établir communément des priorités dans la perspective de la sécurité intérieure et dans une discussion étroite avec les exploitants d'équipements d'infrastructure et d'opérationnaliser les mesures de protection d'infrastructures critiques.

Interlocuteurs du concept de protection de base:

Office fédéral pour la protection des populations et la gestion des catastrophes
(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)
Centre Protection d'infrastructures critiques
(Zentrum Schutz Kritischer Infrastrukturen)
Deutschherrenstrasse 93-95
53177 Bonn
BBK-Zentrum-I@bbk.bund.de

http://www.bbk.bund.de

Office fédéral de police criminelle
(Bundeskriminalamt)
65173 Wiesbaden
http://www.bka.de oder http://www.bundeskriminalamt.de

1.

Objectif et bases méthodiques

Définition KRITIS

Face aux dangers potentiels liés aux catastrophes naturelles, à des événements techniques ou à une erreur humaine, au terrorisme ou aux actes criminels, des mesures pour protéger nos infrastructures économiques et sociales extrêmement complexes semblent impératives, en particulier lorsqu'il s'agit d'infrastructures revêtant « une **importance particulière** pour la communauté et dont la défaillance et la perturbation créeraient **des blocages durables dans l'approvisionnement**, des dysfonctionnements importants de la sécurité publique ou d'**autres conséquences dramatiques** ».[2] Il s'agit de prévoir et de concevoir pour ces infrastructures dites critiques des mesures visant à limiter et à maîtriser les dommages, mais aussi et surtout des **mesures préventives** permettant d'éviter d'emblée la survenance de défaillances considérables ou en tout cas de minimiser autant que possible leurs conséquences.

Base : coopération entre l'Etat et les entreprises

La condition sine qua non pour concrétiser et formuler les mesures de protection indispensables est une collaboration basée sur la confiance entre l'Etat et les exploitants d'équipements d'infrastructure: Tandis que l'Etat reste le garant de la sécurité intérieure et qu'il présente également les processus d'information et de communication, les exploitants disposent des connaissances détaillées suffisantes sur leurs infrastructures, si bien qu'ils sont les seuls à pouvoir appliquer efficacement les mesures concrètes de protection.

[2] Définition d'infrastructures critiques du groupe de travail K KRITIS du ministère de l'Intérieur (Bundesministerium des Innern – BMI) du 17.11.2003

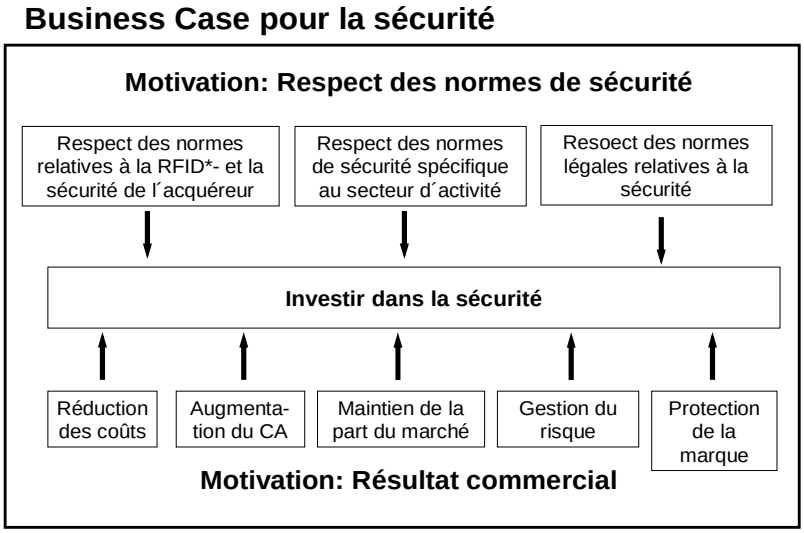
Les points de départ pour le concept de protection de base résultent d'une part des **dispositions légales**, d'autre part des **principes d'entreprise** généralement admis de la gestion prévisionnelle des risques et de la planification stratégique, adaptée au succès et à la continuité (par exemple dans le cadre dudit plan de continuité d'activités (PCA).

Gestion des risques, devoirs des exploitants, lois spécifiques

l'article 91, alinéa 2 de la loi sur les sociétés anonymes (AktG) oblige le conseil de direction d'un certain nombre d'exploitants à prendre les mesures appropriées et mettre en place les systèmes de surveillance – par exemple un système de gestion des risques – pour identifier très tôt les évolutions qui mettent en danger l'existence continue de la société. De telles évolutions comprennent, outre les activités à risques et les infractions aux dispositions légales, également les risques liés aux événements naturels ou aux actes terroristes, susceptibles d'affecter considérablement l'existence continue de l'entreprise. Les questions de l'estimation et l'évaluation des risques de l'entreprise sont mises très en avant, notamment avec le nouvel accord sur les fonds propres « Bâle II » et les normes adoptées relatives à l'attribution de crédits.

Un autre point de départ des mesures destinées à protéger les infrastructures découle de la responsabilité des exploitants à assurer la sécurité de leurs installations face aux éventuels dangers et de prendre les dispositions nécessaires. Les **devoirs de l'exploitant** sont fixés en partie par la loi (devoirs généraux de l'exploitant ou obligations spécifiques, par exemple conformément à la loi sur les télécommunications, à l'ordonnance régissant le transport des matières dangereuses ou concernant les entreprises soumises à l'ordonnance sur les accidents majeurs). Ces devoirs constituent aussi en partie un élément essentiel des principes d'entreprise généralement admis tout comme ils représentent, par exemple, les **principes de gestion et de direction en bonne et due forme des entreprises.** S'y ajoutent les réglementations légales générales et spécifiques comprenant, par exemple, les lois sur la protection contre le feu et l'incendie, le code de la construction et le droit de l'urbanisme et de l'aménagement du territoire, mais aussi le droit de l'environnement et de l'énergie.

Figure 1 : Motivation pour la sécurité dans l'entreprise



*) Les technologies telles que RFID (Radio Frequency Identification), capteurs, conteneurs intelligents et solutions logicielles destinées à la gestion de la chaîne de reporting et logistique, peuvent être combinées avec des procédés et déroulements optimisés qui font ressortir bien plus clairement la chaîne d'approvisionnement.

Illustration et explication de : Deloitte, Réussir dans une économie sécurisée – Croissance et aisance dans une économie sécurisée. Executive Summary, 2004, p. 4 f.

Mesures contre toute intervention de personnes non autorisées

Du point de vue de la sécurité, les mesures contre toute **intervention de personnes non autorisées** constituent une importante contribution à la protection des infrastructures critiques. Les équipements doivent être protégés contre toute panne causée intentionnellement ou due à des événements naturels ou accidents de manière à pouvoir exclure le plus possible un danger sérieux résultant, par exemple, d'une explosion ou d'une propagation de substances dangereuses. Il convient également d'éviter une défaillance des produits ou services mis à disposition, dans la mesure où il peut en résulter des dangers considérables, au sens de la définition des infrastructures critiques (KRITIS) mentionnée au début.

Objectif : réduire la vulnérabilité

L'exigence majeure du concept de protection de base est la protection de la vie humaine en réduisant la vulnérabilité des infrastructures critiques face aux événements naturels, à la défaillance technique ou à l'erreur humaine et face aux attentats terroristes ou actes criminels. Le concept de protection de base

doit prendre en considération les mesures de sécurité standard en matière de construction, d'organisation, de personnes et techniques.

Ce que le concept de protection de base **ne prend pas** en considération

Bien qu'également les risques aussi pour l'environnement puissent représenter une grave menace, dans l'intérêt d'une approche pragmatique le présent concept ne traitera pas spécifiquement des **conséquences** purement **environnementales.** Cependant il est possible d'appliquer analogiquement la même méthode. Les actes criminels dirigés contre les entreprises qui affectent surtout leur position concurrentielle, par exemple l'**espionnage industriel**, ne seront pas pris non plus en considération.

Et pour conclure, les **transports externes de matières dangereuses** également ne feront pas l'objet des considérations ci-dessous. Fondamentalement, il conviendra d'entamer des réflexions similaires concernant la sécurité des transports de marchandises dangereuses telles qu'elles ont été entamées ici pour les installations stationnaires. Les voies d'accès et de sortie, et en particulier leur protection, doivent être contrôlées et traitées au cas par cas pour y déceler la présence d'interfaces avec les transports. Il faut également amorcer des réflexions isolées concernant le vol de matières dangereuses ou l'abus intentionnel de celles-ci.

Les attaques par les réseaux électroniques des entreprises (les cyberattaques) ont une grande importance. Mais comme le concept de protection de base se concentre sur la prévention des risques physiques, nous renvoyons aux concepts existants de la **sécurité de l'information** tels que la norme ISO 17799 et le **manuel de protection de base de l'information** et aux recommandations supplémentaires de l'Agence fédérale de la sécurité des systèmes d'information (BSI).

Processus d'analyse et de planification

Il est fondamental de s'entendre sur le **niveau de protection** visé ou acceptable pour aboutir à des déclarations satisfaisantes et applicables. La méthode systématique suivante est donc indiquée pour développer le concept de protection:

I. La formation des catégories de risques, classées selon les différents domaines de catastrophes naturelles, défaillance technique et erreur humaine, terrorisme et actes criminels,

II. la fixation du niveau respectif de protection basée sur ces catégories,

III. la conception de scénarios de sinistre et de menace,

IV. l'analyse des points faibles,

V. la formulation des objectifs de protection et la fixation des mesures de protection et contre-mesures qui en découlent,

VI. la formulation du besoin d'action respectif (coordination entre mesures étatiques et privées),

VII. la mise en application du besoin d'action formulé et

VIII. le contrôle régulier de ce processus d'analyse et de planification dans le cadre de la gestion de la qualité.

Les exploitants sont les personnes compétentes et responsables de la mise en application des mesures permettant de réaliser le concept de base de protection. Dans ce contexte, il convient d'analyser entre autres les aspects suivants:[3]

- Appréciation de la **situation de danger** (situation générale en matière de sécurité, importance et composition des effectifs, qualité de l'organisation chargée de la sécurité, position sociale des membres de la direction de l'entreprise, type de relations de commercialisation et d'activités à l'étranger, criminalité relevée jusqu'à présent etc.).
- **Situation géographique** de la zone opérationnelle et des installations (vulnérabilité de l'extérieur et de l'intérieur, distance jusqu'à la clôture de l'usine, visibilité de l'extérieur, voieries intérieure et extérieure, proximité avec d'autres zones industrielles ou d'infrastructures critiques, conditions géologiques [par ex. risque de tremblement de terre] et géographiques [par ex. proximité de fleuves, topographie]).
- **Importance des installations** pour les processus de production situés en amont et en aval et les prestations de

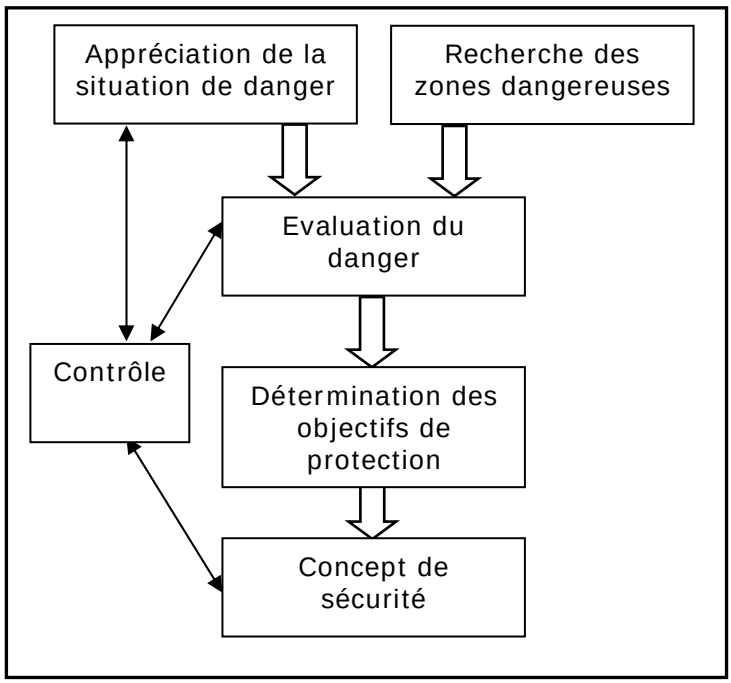
[3] Modifiés selon la Commission allemande des accidents, mesures contre toute intervention de personnes non autorisées, 2002.

service (par ex. les dommages économiques, les pertes de production et de livraison).

- **Caractère symbolique** de l'entreprise ou de l'installation (type de production et de stockage des matières, éventail de produits, importance économico-stratégique de l'entreprise).
- **Interdépendances**, à savoir les interactions avec d'autres infrastructures.
- Nature, topologie et relations de coopération des **structures** existantes **de gestion du risque** côté exploitant.
- Structures de la **coopération** entre les institutions publiques et les exploitants, aussi bien du point de vue du plan d'urgence et de gestion de crise que du point de vue de la prévention technique.

Pour l'analyse, il faut retenir non seulement les dommages primaires, mais aussi les **effets secondaires** (voir ici p 33).

Figure 2 : Etapes de l'analyse



Source Commission allemande des accidents, mesures contre toute intervention de personnes non autorisées, 2002, p. 20.

2.

Les risques et les domaines Menacés

2.1 Les risques

Effet domino / retard / diversion

Les risques auxquels doivent faire face les exploitants d'infrastructures critiques sont divisés en 3 : (1) les risques liés aux événements naturels, (2) les risques liés à une erreur humaine ou une défaillance technique et (3) les dangers liés au terrorisme ou aux actes criminels. Il faut observer que toute l'installation ou les parties de l'installation exigeant une protection peuvent être affectées également par des événements qui se produisent à l'extérieur de l'installation, dans les zones opérationnelles avoisinantes ou au niveau des infrastructures du trafic, soumis à un potentiel de risque particulier (effet domino). Les impacts possibles à cet égard comprennent, par exemple en cas d'incendie, la propagation du feu des équipements voisins, les débris qui volent à la suite d'une explosion des équipements voisins, la panne des installations des services publics à la suite de catastrophes hors de l'installation etc. Egalement les événements qui se répètent **dans un laps de temps très court**, par exemple une deuxième explosion différée ou plusieurs **accidents simultanés** en différents endroits, entraînent éventuellement un effet exponentiel en suspendant les mesures de sauvetage ou de réfection ou en rassemblant des ressources au mauvais endroit (**mesures de diversion**).

Figure 3 : Facteurs de risque

Facteurs de risque

L'aperçu suivant vise à rendre intelligible la complexité et l'hétérogénéité des facteurs de risque à prendre en considération, sans prétendre à l'exhaustivité:

L'homme comme facteur de risque

- *Conscience de sécurité inadéquate*
- *Personnel insuffisamment qualifié*
- *Erreur humaine*
- *Comportement criminel (sabotage, attentats terroristes)*

L'organisation comme facteur de risque

- *Concentration des ressources indispensables*
- *Externalisation des infrastructures critiques de l'entreprise*

La nature et l'environnement comme facteurs de risque

- *Catastrophes naturelles*
- *Calamités et épidémies*

L'informatique comme facteur de risque

- *Complexité des systèmes*
- *Accroissement de la dépendance informatique*
- *Vaste interconnexion mondiale des systèmes TI*
- *Courts cycles d'innovation de la technologie de l'information*
- *Standardisation de la technique et des composants*
- *Interconnexion des réseaux et interdépendances des infrastructures critiques*
- *Internet comme système névralgique des infrastructures (en relation avec la sécurité informatique)*

Source : Association fédérale des banques allemandes,
Gestion des infrastructures critiques, 2004, p 13

2.1.1 Les risques liés aux événements naturels

Situations météorologiques extrêmes

En Allemagne, selon les Assurances, les dommages éléments naturels résultent pour une grande part des événements atmosphériques extrêmes. Font partie de ces événements les crues (y compris l'augmentation du niveau de la nappe phréatique), les débordements, les inondations, les raz-de-marée, la

glace, la neige, les sécheresses et tempêtes. Des risques particuliers en cas de **crues** résultent de la force de l'eau qui affouille les chemins, les ponts, les digues etc. et des éléments flottants transportés par l'eau. Les substances nocives qui s'échappent et les ordures entraînées dans les eaux accroissent le danger d'une contamination des eaux potables et parallèlement des risques sanitaires considérables. L'augmentation du niveau de la nappe phréatique peut entraîner l'inondation des régions même isolées.

Les ouragans et la grêle peuvent être les conséquences d'orages violents et créer des dangers supplémentaires. On qualifie de **tempêtes** les mouvements de masse d'air à partir de 75 km/h et d'**ouragans** ceux supérieurs à 120 km/h. Outre les dommages directs qui résultent de la pression du vent et des rafales consécutives, les tempêtes et ouragans peuvent représenter des dangers supplémentaires dus aux débris et aux particules de saleté qui sont entraînés par le fort tourbillon d'un ouragan. Les tempêtes occupent une position de tête aussi bien au niveau de la fréquence qu'au niveau du pourcentage des dommages économiques.

Les **grêlons** peuvent atteindre au cas par cas une taille supérieure à 10 cm et un poids de plus d'un kilogramme. Outre les dégâts matériels et les dommages causés aux cultures agricoles, les grêlons peuvent entraîner également d'importantes blessures chez les êtres humains. Ils peuvent aussi boucher les écoulements d'eau et causer ainsi des débordements.

Les tremblements de terre

Le risque d'un tremblement de terre s'accroît obligatoirement parallèlement à l'intensité du tremblement. En fonction des paramètres géologiques tels que la nature du sol, même de faibles tremblements de terre peuvent provoquer des dégâts importants sur les bâtiments et les infrastructures. Il faut éventuellement prendre aussi en considération les dommages secondaires tels que les incendies et les raz-de-marée. La baie de Cologne, le fossé rhénan et la région de Vogtland notamment comptent parmi les régions allemandes exposées aux tremblements de terre.

Incendies de surface

Les incendies de surface peuvent se déclarer de façon naturelle par la foudre, l'ignition spontanée, intentionnellement ou par négligence, en combinaison avec une longue période de sécheresse. Les régions principalement menacées sont les régions forestières, les superficies agricoles exploitées et les surfaces plantées de landes.

Mouvements de masse

Les mouvements de masse sont causés par des événements géophysiques (tremblements de terre, intempéries), des influences météorologiques (fortes précipitations, inondations, fonte des neiges et des glaces) et des influences anthropogènes (mesures de construction, secousses, déboisements). Des exemples de mouvements de masse sont les avalanches, les laves torrentielles, les glissements de terrain et la liquéfaction.

Parallèlement aux dommages directs, les mouvements de masse peuvent entraîner également des menaces indirectes en générant des raz-de-marée dans les lacs ou les retenues d'eau ou en barrant les fleuves dont les digues se rompent ultérieurement.

Les épidémies

On entend par « épidémie » la survenance concentrée localement et temporellement d'une maladie contagieuse chez les êtres humains ou les animaux. Une augmentation du risque résulte du trafic global des marchandises et du tourisme, par exemple, de l'élevage intensif, des inondations et de la sécheresse. Une **pandémie** est une épidémie nationale, voire d'envergure internationale.

2.1.2 Les risques liés à une erreur humaine et une défaillance technique

Les incendies

L'incendie est un feu qui se propage de façon incontrôlée, dont la cause est une erreur humaine et une défaillance technique,

incendie criminel inclus (cf. 2.1.3), la foudre, le rejet de matières dangereuses ou la conséquence d'explosions. Les incendies sont classés, en fonction de leur ampleur, en petits incendies, en incendies moyens (incendies de bâtiment) et en incendies de grande ampleur (établissements industriels, grandes installations, entrepôts).

Le rejet de matières dangereuses

Font partie des matières dangereuses toutes les substances de type nucléaire, biologique, chimique et radiologique (NRBC/CBRN) ayant des conséquences préjudiciables sur l'environnement et sur l'homme et qui peuvent entraîner des explosions et des incendies. Les propriétés des matières dangereuses sont extrêmement différentes, elles peuvent être irritantes, légèrement inflammables, voire explosibles, polluantes, chroniquement nocives et toxiques. Les produits dangereux utilisés dans une entreprise peuvent être identifiés à l'aide d'un registre individuel des matières dangereuses.

Les explosions

Une explosion résulte d'une dilatation soudaine des gaz due à la libération d'énergie qui entraîne un souffle éventuellement accompagné d'un dégagement de chaleur. L'erreur humaine et la défaillance technique, y compris celles commises intentionnellement, la foudre ou le rejet de matières premières peuvent provoquer des explosions.

Autres impacts physiques de l'intérieur et de l'extérieur

Les impacts physiques de l'intérieur et de l'extérieur peuvent être causés par des accidents et des avaries tels que les accidents routiers ou professionnels ainsi que les accidents d'avion (cf. 2.1.3.). Outre la destruction de l'installation, les accidents et les avaries peuvent déclencher également des incendies et des explosions, entraîner un dégagement de matières dangereuses et autres dégâts.

2.1.3 Les risques liés au terrorisme et aux actes criminels

Catégories de risques

Les risques liés au terrorisme ou aux actes criminels, peuvent être attribués à des **catégories de risques** précises et **graduées** comme résultat de l'analyse relative à la situation générale des dangers d'une entreprise. Les degrés individuels donnent un aperçu des auteurs présumés du délit, de leur méthode éventuelle ou aussi typique, de leurs desseins et motifs ainsi que du degré d'énergie criminelle. Ces degrés permettent de représenter sous forme synoptique les risques qui sont à prendre en considération.

Les hypothèses émises dans une catégorie de risques reposent sur l'expérience criminalistique, en revanche, elles ne s'appliquent pas parfaitement à chaque cas. Evidemment, on ne peut en déduire avec certitude les auteurs présumés ni leur mode d'action. Cependant, sur la base des expériences acquises en matière de protection d'exploitation, il est possible de procéder à une classification grossière des **groupes d'acteurs**, leurs **motifs** typiques et les **comportements** éventuels dans un tableau (voir page 49) divisé par niveau de dangerosité (voir annexe). Les actes commis par négligence n'y sont pas indiqués, mais répertoriés sous le titre « Les risques liés à une erreur humaine et à une défaillance technique » (chapitre 2.1.2).

Dans quelle mesure les auteurs potentiels peuvent-ils effectivement causer un préjudice sérieux et où cela semble-t-il possible et vraisemblable ? Ces questions doivent faire l'objet de l'**évaluation des risques** et prendre en considération les zones dangereuses identifiées dans l'environnement de l'entreprise (cf. par exemple le paragraphe « Gestion du risque » de la liste de contrôle, annexe1). Les catégories de risques comprennent une série d'hypothèses qui doivent permettre d'assigner les risques à la situation de danger identifiée. Ces hypothèses englobent essentiellement

- les circonstances éventuelles de l'acte
- les motifs éventuels et les modes d'action typiques
- les ressources qui sont probablement utilisées

- l’énergie criminelle présumée.

Par ailleurs, on peut différencier l’acte criminel par moyens d’action, en établissant un lien entre les auteurs et respectivement leurs motivations et les options d’une infraction qu’offre la nature des infrastructures elles-mêmes. Les **moyens d’action** en principe envisageables sont par exemple:

Moyens d’action

La fausse manœuvre délibérée

On définit sous ce terme tous les actes prémédités susceptibles d’engendrer un incident en effectuant des manœuvres simples et sans avoir recours à des outils. On compte parmi ces actes: la mise en marche et l’arrêt des équipements, l’ouverture et la fermeture des obturateurs de tuyauterie (soupapes à tiroir), l’ouverture des volants à main et l’actionnement de leviers au cours du processus. Une erreur de manipulation exécutée avec préméditation peut être effectuée par le personnel interne ou externe à l’entreprise.

La manipulation

On entend par « manipulation » toute modification intentionnelle ou le déréglage des composants d’un système visant à induire une situation critique dans une installation. Les exemples pourraient être dans ce cas les suivants : la programmation erronée des commandes, le déréglage des instruments de mesure, le blocage des avis d’opération, d’incident technique, des alertes ou aussi la désactivation des systèmes de protection. Les premiers qui entrent en ligne de compte comme auteurs sont en priorité les « initiés » qui connaissent exactement l’installation.

L’accident de véhicule

Les accidents du trafic routier ou ferroviaire du domaine d’exploitation pourraient entraîner le dégagement des substances dangereuses ou endommager, voire détruire des éléments importants de l’installation. Par exemple : les fuites des fûts dues à un accident de chariot élévateur, le déraillement de wagons-citernes, la destruction d’installations par collision de poids lourds.

Les interventions usant de moyens simples

Il s'agit ici d'une intervention préméditée, en général spontanée, dans les parties importantes de l'installation qui est commise avec les moyens et outils disponibles dans toutes les exploitations. Les exemples comprennent ici : les brisures de pièces en verre de l'installation, blocage des pièces mobiles de l'installation ou aussi l'adjonction de substances non permises dans le processus. Ce sont en premier lieu les employés de l'entreprise qui entrent en considération en tant qu'auteurs.

Les interventions usant de moyens spéciaux

Ce moyen d'action correspond à la destruction violente et préparée des parties de l'installation. Les outils d'attaque qui entrent en ligne de compte sont, par exemple, les pieds-de-biche, les perceuses électriques, les chalumeaux de découpage, les coupe-boulons ou les masses. Exemples : fracturation des portes suivie de la destruction des installations, fracassement des dispositifs de mesure et de commande, ouverture par coups des réservoirs et tuyauteries dont les conséquences sont d'importantes fuites. Le vandalisme sous forme de vandalisme aveugle peut venir remplacer l'attentat ciblé, par exemple à la suite d'un cambriolage ayant échoué.

L'incendie criminel usant de moyens simples

On entend par « moyens simples » le fait d'allumer des sources inflammables avec des allumettes ou briquets ou bien de jeter des mégots de cigarettes. Ce moyen d'action n'est possible qu'en présence de matières combustibles et légèrement inflammables en quantités suffisantes. Les exemples comprennent ici : l'allumage de liquides inflammables issus du processus technologique, le fait d'incendier les dépôts avec pour conséquence la libération de substances dangereuses, le fait d'incendier les locaux périphériques ou les équipements ayant des incidences sur les éléments importants de l'installation.

L'incendie criminel usant de moyens comburants

Cette catégorie concerne les attaques incendiaires commises à l'aide de matières qui brûlent vite et de façon intense. Exemples d'attentats: le versement et l'allumage de liquides inflammables (par exemple de l'essence), le jet desdits cocktails Molotov (par

la fenêtre par exemple) ou l'application de compositions incendiaires professionnelles équipées de dispositifs d'allumage à retardement ou à distance. Les attaques incendiaires peuvent être exécutées également de l'extérieur (amplitude du jet) et présupposent une volonté criminelle délibérée.

L'utilisation d'explosifs

Les explosifs de fabrication artisanale, les explosifs industriels ou militaires peuvent être utilisés dans ce cas. Les exemples d'attaque possibles : le dépôt d'une « bombe faite à partir d'un extincteur » et de fabrication artisanale dans les composants sensibles de l'installation ou, plus probablement, à la périphérie du bâtiment, le fait de faire sauter les réservoirs et les tuyauteries, la destruction des composants porteurs avec pour conséquence le renversement des réservoirs, la destruction des éléments de l'installation. En règle générale, ce type d'attaque correspond à une action externe sur fond politique extrémiste.

Le bombardement

Dans le cas le plus simple, le bombardement s'effectue avec des armes à air comprimé ou des catapultes (balles d'acier) ; dans le cas le plus complexe, les auteurs d'actes terroristes font usage d'armes lourdes telles que les missiles antiaériens. Exemples de moyens d'action : le déclenchement de fuites dans les réservoirs exposés ou les tuyauteries, le déclenchement d'une explosion. Un tir est possible surtout en dehors de l'enclos extérieur d'une zone opérationnelle ou d'un parc industriel, mais les composants d'une installation montés à proximité de la clôture sont plus fortement menacés.

L'accident d'avion

Aussi bien l'énergie cinétique des appareils qui s'écrasent que l'explosion du carburant véhiculé ou, éventuellement, de l'explosif qui se trouve à bord demandent à être pris en considération ici. De surcroît, un avion peut être utilisé comme moyen de transport des substances NRBC. Les agressions entraînant la chute d'un avion peuvent venir de l'extérieur, par exemple en tirant des missiles, par la mise à feu d'explosifs à distance, la manipulation à distance de l'électronique de bord, l'arrêt ou l'abus des stations de contrôle du service de naviga-

tion aérienne, ou bien encore être exécutées de l'intérieur en reprenant le pilotage ou en le déréglant, en allumant un explosif (attentat-suicide).

L'utilisation d'armes NRBC

Selon la disponibilité des agents et des moyens, un large spectre d'applications est envisageable et demande à être développé séparément. Les applications possibles vont du déclenchement prémédité de maladies (envoi d'agents de l'anthrax) ou d'épidémies (par l'introduction d'agents extrêmement infectieux dans les systèmes d'alimentation ou via les voies respiratoires) jusqu'à l'emploi de gaz toxiques, par exemple aux points névralgiques du réseau routier, en passant par l'utilisation desdites "dirty bombs" (bombes radiologiques) visant à désorienter durablement la population.

Les effets combinés

Dans ce contexte également, on peut envisager un large spectre de possibilités: des bombes radiologiques citées précédemment comme combinaison explosion-contamination radioactive, en passant par la destruction d'une installation de production et la propagation d'agents nocifs jusqu'aux actions individuelles ayant une influence médiatique et de nombreuses conséquences pour les activités de l'entreprise ou l'approvisionnement de la population.

2.2 Les zones menacées dans les entreprises

Les risques liés aux événements naturels, à l'erreur humaine ou à la défaillance technique ainsi que ceux liés au terrorisme ou aux actes criminels touchent, dans des proportions différentes, les infrastructures critiques, mais aussi les zones individuelles de production et de service dans une installation. Du point de vue de l'entreprise, la **suppression du personnel, la centralisation et l'automatisation** des processus de réglementation et de surveillance, le transfert des compétences dû à

l'**externalisation** ou aux déficits d'exécution à la suite d'une pression des coûts peuvent comporter des risques additionnels.

2.2.1 Les zones particulièrement menacées par les événements naturels

Les zones particulièrement exposées aux situations météorologiques extrêmes

Les inondations et les crues soudaines peuvent détruire la totalité des bâtiments et des installations. Outre les réseaux, les bâtiments, les installations de production, d'extraction et de transformation notamment, ainsi que les masses d'informations électroniques font partie des domaines particulièrement menacés. Les eaux des crues qui s'évacuent lentement endommagent principalement les zones basses du bâtiment (sous-sol et rez-de-chaussée). Les technologies d'information et de communication, l'alimentation électrique (interne à l'entreprise), ainsi que les réseaux d'alimentation et autres réseaux de ligne sont particulièrement exposés étant donné que les dommages dus à l'eau provoquent en général des pannes d'alimentation. L'augmentation du niveau de la nappe phréatique peut causer ces dégâts hors des zones inondées.

En principe, indépendamment de leur situation géographique, tous les bâtiments et les installations sont exposés aux tempêtes ; cependant, les bâtiments et les installations particulièrement affectés sont ceux situés dans un endroit exposé (montagnes, collines, crêtes, couloirs d'air) et qui donnent prise à la tempête.

Les tempêtes, mais aussi les sécheresses ou le gel extrême, peuvent entraîner en sus des difficultés d'approvisionnement qui compromettent le déroulement normal des opérations.

Les zones particulièrement exposées aux tremblements de terre

Les tremblements de terre peuvent détériorer ou détruire les bâtiments et l'ensemble des complexes d'installations et causer des défaillances dans tous les domaines. Des secousses même légères peuvent en outre entraîner des dommages au niveau de la technologie de l'information et dans les domaines

de production, d'extraction et de transformation sensibles aux chocs.

Les zones particulièrement exposées aux incendies de surface

Les incendies de surface peuvent détériorer tous les sites où sont construits bâtiments ou installations. De surcroît, ces incendies de surface peuvent bloquer l'ensemble des sites ou les infrastructures routières rendant les installations inaccessibles ou difficilement accessibles.

Les zones particulièrement exposées aux mouvements de masse

Les mouvements de masse peuvent affecter ou détruire globalement les bâtiments et installations ou bien bloquer l'accès à ceux-ci. De même, les mouvements de masse qui se produisent à l'extérieur d'une installation et qui ont des incidences sur les réseaux externes peuvent entraîner des blocages dans l'approvisionnement qui entravent le déroulement normal des opérations.

Les zones particulièrement exposées aux épidémies

Les épidémies peuvent entraîner l'indisponibilité ou des situations bloquées s'agissant du personnel requis pour le fonctionnement des installations. Notamment, l'entreprise de production et les domaines « centre de calcul » et « stations de contrôle » seraient particulièrement affectés par ces circonstances. De surcroît, les barrages de zones peuvent compromettre, voire rendre impossible l'accès aux installations pendant la période épidémique et épizootique.

2.2.2 Les zones particulièrement exposées à l'erreur humaine et à la défaillance technique

Les zones particulièrement exposées aux incendies

Les incendies peuvent avoir un impact de l'intérieur et de l'extérieur sur les installations et les bâtiments. Ils peuvent détruire ou affecter toutes les zones ou bien entraver tout usage

ultérieur par l'effet de la fumée. De même, les petits incendies qui se déclarent dans les éléments exposés de l'installation tels que la technologie de l'information, peuvent causer la panne de toute l'installation.

Les zones particulièrement exposées aux matières dangereuses

Outre le préjudice causé au personnel de l'entreprise et à l'environnement de l'installation concernée, qui est considéré comme risque principal, la libération de matières dangereuses peut aussi générer des explosions et des incendies. Les installations techniques contaminées, y compris les matériels informatiques, sont dans ce cas rendus en partie inutilisables ou utilisables uniquement de façon restreinte.

Les zones particulièrement exposées aux explosions

Les explosions peuvent avoir un impact de l'intérieur et de l'extérieur sur les installations et les bâtiments. Elles peuvent endommager ou détruire tous les domaines et entraîner des réactions en chaîne. L'effet du souffle provoque la destruction principale ; les incendies se déclarent fréquemment à la suite de l'explosion. Même de petites explosions dans les zones sensibles (systèmes informatiques, courant) peuvent causer la panne de toute l'installation.

Les zones particulièrement exposées aux autres influences physiques intérieures et extérieures

Les influences physiques intérieures et extérieures peuvent compromettre le fonctionnement de l'installation, affecter ou détruire les bâtiments et tous les complexes d'installation. Ces impacts peuvent entraîner une panne dans tous les domaines. Les influences physiques dans le domaine des réseaux externes peuvent conduire à des difficultés internes d'approvisionnement et à des pertes de production.

2.2.3 Les zones particulièrement exposées au terrorisme et aux actes criminels

Les catégories de risques hiérarchisées et leurs remarques relatives aux menaces généralement envisageables concernent d'abord toute l'entreprise. Au sein même de l'entreprise, les complexes industriels individuels se composent de zones, d'unités ou d'éléments d'installations qui se différencient par danger potentiel, type de construction, exploitation, conception technique et se distinguent avant tout par leur degré de vulnérabilité face aux pannes.

En règle générale, il existe également des zones de vulnérabilité particulière dans les composants des installations. Il convient de déterminer systématiquement ces zones au moyen d'une étude séparée. Par analogie avec le rapport de sécurité qui doit être établi conformément à l'article 9 de l'ordonnance sur les accidents majeurs (Störfallverordnung), non seulement les dangers potentiels mais aussi les équipements destinés à l'approvisionnement et la commande des installations ainsi que les systèmes de transport de matières etc. jouent aussi un rôle important dans la protection de l'objet.

Classification des zones de sécurité

Par conséquent, il s'avère généralement utile de répartir la zone opérationnelle en un nombre de sous-zones de catégories et de risques différents. Une analyse exhaustive de tous les points faibles potentiels, associée aux moyens d'action variés et envisageables, donnerait un nombre incontrôlable de variantes. Par conséquent, il paraît plus pertinent de regrouper d'une manière plus généralisante les zones ou les éléments des installations. Ainsi, il peut être utile de considérer un complexe continu comme un tout, c'est-à-dire sans examiner de façon plus approfondie quels composants et parties individuels sont vulnérables et quelle incidence exacte une éventuelle attaque a sur l'un ou l'autre composant de l'installation. Le complexe d'installations concerné est considéré comme protégé et sécurisé globalement de manière à couvrir aussi tous les composants individuels.

Dans le cas des systèmes d'approvisionnement utilisés dans l'ensemble de la zone opérationnelle, il faut constituer si possible des sous-zones pour les objets menacés et ne pas étendre inutilement l'étude aux vastes ensembles de réseaux. Il demeure néanmoins important **d'observer une vigilance toute particulière** au-delà des **périmètres de l'exploitation**, non seulement du point de vue des risques particuliers dans la chaîne de valeur en amont et en aval, mais aussi au niveau des **interactions géographiques** avec les zones dangereuses avoisinantes.

Constitution de sous-zones

Exemples de regroupements pertinents des zones dangereuses:

- Installations de production, d'extraction et de transformation
- Centrales directrices, installations informatiques
- Installations extérieures (non surveillées)
- Tuyauteries d'alimentation
- Installations d'approvisionnement en énergie de tout genre
- Agrégats de secours de tout genre.

3.

Recommandations générales sur la protection de base

Protection de base comme protection minimale

L'objectif est de présenter des recommandations de protection de base pour les différents risques, qui doivent être considérées comme protection minimale des installations stationnaires au niveau des infrastructures critiques. Pour cela, une **méthode multiétagée**, s'inspirant du procédé décrit au chapitre 1 (Objectifs et base méthodiques, p. 11 et 12) s'impose; elle comprend la définition des risques ainsi que la conception et l'application de mesures de protection.

3.1 Analyse du besoin de protection

3.1.1 Méthode d'analyse du besoin de protection

Appréciation des risques

Il faut d'abord procéder à un examen des **sites** des équipements KRITIS. Celui-ci comprend l'appréciation des risques liés aux événements naturels, à la défaillance technique et à l'erreur humaine, aux attaques terroristes et aux actes criminels. Les appréciations des risques face aux dangers liés aux événements naturels peuvent se faire à l'aide de plans (plans d'inondation, cartes de tremblement de terre, plans d'aménagement du territoire, cartes des risques) pouvant être demandés auprès des autorités compétentes (cf. chapitre 4).

En ce qui concerne les risques liés à une défaillance technique ou à une erreur humaine, il faut contrôler que les dispositions en la matière et les spécifications techniques (protection-incendie, ordonnance sur les matières dangereuses, sécurité du travail, formations) soient observées. En ce qui concerne les menaces terroristes, les exploitants d'infrastructures critiques peuvent

- contrôler systématiquement et en collaboration avec les autorités compétentes en matière de sécurité (cf. Chapitre 4), si les zones critiques de l'entreprise et les installations peuvent représenter généralement une excellente cible offrant la **possibilité** d'une détérioration ou d'une défaillance, voire une destruction de l'équipement (**analyse du risque**),
- étudier, en collaboration avec les autorités compétentes en matière de limitation des risques hors de l'entreprise (cf. chapitre 4), quels sont les effets concrets escomptés dus à une éventuelle détérioration ou défaillance et destruction de l'installation, et vérifier s'ils pourraient présenter **un danger sérieux** (**analyse des dangers**),
- élaborer les divergences et convergences entre les exigences d'une protection contre toute intervention de personnes non autorisées, contre les dangers naturels, l'erreur humaine et la défaillance technique.

Entente sur le niveau de protection

L'analyse des risques et des dangers est un élément équivalent de l'analyse du besoin en protection. Il faudra décider au cas par cas de l'étape par laquelle vous devez commencer. Dans le cadre de ce concept, nous proposons d'effectuer d'abord l'analyse générale du risque, puis de déterminer les incidences concrètes de ces risques sur l'entreprise, en procédant à une analyse des dangers, pour convenir, sur cette base, du niveau de protection et enfin le fixer.

L'analyse et les mesures qui en découlent devront être documentées (cf. chapitre 3.5.2.). Mais cette **documentation** exige une confidentialité toute particulière, elle ne doit en effet être accessible qu'à un groupe limité d'employés au sein de l'entreprise. Il doit émaner clairement des documents, qui sont globalement à la disposition du personnel et du public, que l'exploitant a pris les mesures nécessaires pour assurer la sécurité de l'entreprise et des installations.

Au-delà, l'analyse doit être **réitérée** à intervalles réguliers et intégrée dans le processus de gestion du risque de l'entreprise afin de déceler de nouveaux risques ou pouvoir procéder éventuellement à la **réévaluation** nécessaire, d'adapter en fonction le besoin de protection et d'assurer ainsi l'actualité de la protection de base.

3.1.2 Prise en considération des dépendances et interactions

Outre les risques directs liés aux événements naturels, à l'erreur humaine et à la défaillance technique ou au terrorisme et aux actes criminels, les infrastructures critiques sont exposées également à des risques indirects qui sont à prendre en considération lors de l'analyse étendue du besoin de protection.

Effets domino

D'une part, il faut déterminer lesdits effets domino qui se produisent lorsque des événements externes, par exemple dans les zones opérationnelles voisines, dans l'entourage ou la zone de circulation, ont une incidence sur l'installation. Ainsi, les événements naturels qui se produisent à une certaine distance tels que les crues, les mouvements de masse ou les tremblements de terre liés géographiquement à une retenue d'eau, à l'ensevelissement des voies d'accès et de livraison, peuvent avoir des répercussions sur le fonctionnement de l'installation. Les dysfonctionnements dans les installations environnantes, qui présentent notamment un risque de menace particulier, peuvent affecter l'installation à la suite de la propagation d'un feu ou de débris qui volent ou à la suite d'une explosion. De même, des événements catastrophiques qui se déroulent à l'extérieur de l'installation peuvent entraîner la défaillance des installations des services publics telles que les services d'alimentation en énergie et en eau ou des prestations fournies par les sous-traitants.

Les événements qui se succèdent dans un laps de temps très court tels que plusieurs accidents simultanés en différents endroits ou une **deuxième explosion différée** peuvent avoir éventuellement un effet exponentiel en suspendant les mesures de sauvetage ou de réfection, par exemple, ou en rassemblant des ressources au mauvais endroit (**mesures de diversion**).

Dommages secondaires

Parallèlement, des dommages additionnels (**dommages secondaires**) peuvent résulter de l'atteinte aux infrastructures critiques, et prendre par exemple la forme de blocages dans l'approvisionnement et la fourniture des matériels, liés à des dysfonctionnements des transports à la suite d'une panne de courant. Ces dommages secondaires doivent également être pris en considération lors de l'analyse du besoin de protection, afin de pouvoir évaluer équitablement les conséquences d'une panne complète ou seulement spécifique des infrastructures critiques à l'intérieur, mais aussi à l'extérieur de l'installation.

3.1.3 Prise en considération particulière du terrorisme et des actes criminels

Les analyses des risques et des dangers déjà effectuées et les concepts de sécurité doivent être contrôlés pour s'assurer qu'ils prennent en considération également les dangers, conformément à l'analyse du risque, qui résultent de **l'intervention de personnes non autorisées**, même lorsqu'ils ont été largement exclus comme défaillances, risques naturels ou accidents.

Si l'existence d'un risque sérieux pour les objets protégés a été constatée dans l'analyse des dangers, il convient de vérifier dans quelle mesure les installations semblent particulièrement « séduisantes » pour les attaques terroristes ou les actes criminels. Il faut effectuer à cet effet une analyse systématique qui prend en considération notamment les aspects suivants, déjà mentionnés au chapitre 1 (Objectif et base méthodiques, p. 11 et 12) :

Processus d'analyse et de planification

- Appréciation de la **situation de danger.**
- **Situation géographique** de la zone opérationnelle et des installations.
- **Importance des installations** pour les processus de production situés en amont et en aval et les services.
- **Caractère symbolique** de l'entreprise ou des installations.
- **Interdépendances**, à savoir les interactions avec d'autres infrastructures.
- Nature, topologie et relations de coopération des **structures** existantes **de gestion du risque** côté exploitant.

- Structures de la **collaboration** entre les institutions publiques et les exploitants.

Coopération avec les autorités chargées de la sécurité

Les exploitants doivent actuellement demander les informations requises auprès des autorités compétentes en matière de sécurité intérieure (cf. chapitre 4), que nous conseillons d'intégrer absolument dans cette étape.

La **situation sécuritaire générale** décrit les risques tels qu'ils sont généralement applicables dans les zones opérationnelles, éventuellement avec des différences régionales. Les **indicateurs** d'une criminalité importante sont, dans un premier temps, la statistique de la criminalité de la police et les publications des assureurs. La situation en matière de sécurité relative aux actes punissables motivés politiquement est déterminée par les acquis continus des autorités, en raison de leurs activités au niveau de la police criminelle et de la sécurité du territoire. Les **aspects régionaux** également peuvent donc être pris plus largement en considération.

L'étendue, la gravité et le type des **délits constatés jusqu'à présent** dans une zone opérationnelle peuvent fournir des indications sur le degré du risque. On peut fixer ici une période d'environ **cinq ans**. Les informations suivantes doivent y être incluses :

- Données forfaitaires relatives aux délits mineurs observés tels que le vol simple.
- Nombre d'effractions commises jusqu'à présent ou les vols qualifiés.
- Constatation d'une criminalité organisée dans la zone opérationnelle.
- Nombre d'actes de sabotage commis jusqu'à présent, y compris les dossiers non élucidés pour lesquels il existe une forte présomption de sabotage.
- Nombre de menaces à la bombe commises jusqu'à présent ou autres actes de menace.
- Nombre d'incendies criminels commis jusqu'à présent ou attentats à l'explosif, cas de présomption inclus.

3.2 Fixation des objectifs de protection

Afin de pouvoir définir et opérationnaliser les objectifs de protection et de les ancrer aussi durablement que possible dans la politique de l'entreprise, il est recommandé de les fixer dans le cadre d'un système de gestion de la sécurité. Ces systèmes ont fait leurs preuves dans le passé comme instrument efficace pour l'application et le contrôle systématique des processus d'entreprise, dans la mesure où ils ont su assurer une synthèse réussie entre l'approche top-down (centralisée et hiérarchique), bottom-up (discursive, décentralisée) et fonction tranversale (innovatrice, interconnectée). En particulier dans le contexte de la **sécurité d'entreprise**, **l'intégration systématique des divers processus relatifs à la sécurité** revêt une grande importance, aussi bien l'intégration des processus entre eux qu'avec les stratégies de valeur ajoutée. Un grand nombre de ces mesures sont déjà mises en pratique ou elles peuvent être, comparativement, lancées rapidement. Les exploitants doivent contrôler l'efficacité des mesures existantes, si ce n'est pas déjà fait et éventuellement réagir (cf. aussi chapitre 3.5.1.).

L'équipement qualitatif et qualitatif personnel et technique du **service de sécurité** interne et externe (sécurité des installations) acquiert une importance particulière, ces exigences résultent, entre autres, de la norme DIN 77200. Il faut accorder de surcroît une importance particulière à l'**interconnexion des réseaux** et l'**harmonisation des éléments** souvent largement autonomes de la **gestion de la sécurité** telles que la sécurité informatique, la protection de l'objet et la sécurité du personnel. Si la zone opérationnelle qui doit être analysée fait partie d'une entreprise de plus grande envergure (domaine de l'entreprise, filiale, participation multiple etc.), le niveau de risques et de dangers de toute l'entreprise doit être pris en plus en considération. Cela s'applique également aux actes criminels motivés politiquement. Par expérience, ce danger croît à l'image de l'envergure et de la signification (globale) de toute l'entreprise.

Dans ce contexte, il faut aussi constater l'existence ou non de **risques plus importants** liés à certaines **relations de commercialisation**. Cela pourrait être le cas pour les relations

d'affaires avec des pays politiquement instables. Etant donné que les zones opérationnelles axées sur l'exportation livrent, en général, leurs produits dans le monde entier, le risque s'accroît surtout en cas de relations particulièrement privilégiées avec de tels pays.

Objectifs clé de protection

Les objectifs essentiels visant une protection des installations et objets jugés comme devant être protégés peuvent être décrits comme suit :

- Il faut protéger les limites des zones opérationnelles, en prenant des mesures techniques et organisationnelles, de manière à empêcher l'intrusion de personnes non autorisées sans faire usage de la force et pour détecter, dans un temps approprié, une intrusion de force.
- Les personnes externes à l'entreprise doivent être identifiables.
- Il faut protéger les installations elles-mêmes de manière à rendre impossible toute intervention indue sans connaissances internes et/ou moyens techniques.
- Les ressources financières doivent être employées conformément aux listes de priorité (**gestion intégrative de la protection**).
- Les **parcs industriels** posent des exigences particulières aux mesures de protection, uniquement à cause du nombre d'exploitants indépendants sur le plan juridique et organisationnel. Seuls les objectifs de protection et les mesures prises en commun permettent de minimiser, en général, la vulnérabilité des installations dangereuses. Les mesures appropriées sont sélectionnées de façon adéquate conformément à une analyse systématique de protection.

3.3 Mesures destinées à mettre en œuvre les objectifs de protection

Mesures contre toute intervention de personnes non autorisées

Il convient de **fixer les objectifs** permettant d'assurer la sécurité des installations et les objets jugés comme devant être protégés. Depuis déjà de nombreuses années, les exploitants

d'installations soumis à l'ordonnance sur les accidents majeurs sont tenus de protéger leurs zones opérationnelles et installations contre toute intervention de personnes non autorisées. Face aux situations de menace spécifique (terrorisme), il convient de compromettre toute intrusion de personnes non autorisées, également dans les **aménagements non soumis à l'ordonnance sur les accidents majeurs des infrastructures critiques.** Il s'agit ici de mesures efficaces telles que les clôtures surveillées, l'organisation de contrôles des entrées, les rondes de surveillance, la surveillance vidéo etc. (cf. aussi la liste de contrôle, annexe 1).

Il faut considérer la mise en danger des zones opérationnelles et des installations liée aux attaques terroristes de façon différenciée en ce qui concerne leur probabilité et leurs conséquences potentielles. **Les mesures de protection déjà en usage** jusqu'alors offrent aujourd'hui comme hier une **protection considérable**. Elles doivent donc être appliquées de façon conséquente et tenir compte des recommandations émises dans le présent concept, si elles n'ont pas encore été mises en œuvre. Il convient de protéger en plus les installations ou les éléments qui les composent, particulièrement sensibles et donc menacés par des attentats terroristes.

Il faut prendre les mesures correspondantes pour mettre en oeuvre les objectifs de protection définis. Ces mesures se divisent en mesures de protection intérieure et extérieure (protection physique), en mesures de protection personnelle et organisationnelle et en mesures de management.

3.3.1 Protection intérieure et extérieure

Les mesures visant la mise en œuvre des objectifs de protection extérieure et intérieure comprennent les mesures suivantes :

- Les sites particulièrement vulnérables ne doivent pas être construits dans les **régions exposées aux crues et aux tremblements de terre.** S'ils existent déjà dans ces zones, il faut envisager leur transfert dans des régions non exposées; en tout cas, il faut prendre des mesures spéciales de

prévention contre les inondations et tremblements de terre (surélévation des technologies de l'information et des distributeurs de courant, équipement de suspension contre les secousses, endigage).

Blindage et sécurisation des accès

- Il convient de durcir par blindage toutes les installations ainsi que les composants particulièrement sensibles pour réduire ou parer aux conséquences des débordements et des inondations, des tremblements de terre, des influences physiques et des explosions. Il faut prévoir des réserves de résistance suffisantes aux étages inférieurs (compensation de la pression). De plus, les **domaines** particulièrement **sensibles** doivent se situer **dans l'enceinte des installations**.
- Une composante essentielle de la prévention d'attentats terroristes ou de sabotage consiste à créer une **distance géographique et temporelle** par rapport à l'objet à protéger. Des barrières et obstacles peuvent entraver et bloquer l'accès aux zones sensibles (zones d'accès, contrôles d'accès, service de surveillance, porte, clôtures, patrouilles, bittes, éléments en béton, élévations).
- Les zones non visibles peuvent être contrôlées par des systèmes de sécurité électroniques (surveillance vidéo, détecteur de mouvements, de bruits, caméras thermiques, matériel de détection nocturne).
- Au-delà des contrôles d'accès, les loges de portier acquièrent une importance particulière, supplémentaire en matière de sécurité. Dans ce contexte se pose donc la question **de la sécurité de la porte** même. Si la loge du portier, soit la porte principale par exemple, est la seule zone destinée à recevoir les alertes et les avis d'incident technique (souvent seulement après le service normal de l'entreprise), il doit être impossible d'interrompre la retransmission des messages aux services de secours en accédant aux installations de télécommunication ou en menaçant le personnel de surveillance dans la loge du portier. Cela doit être garanti en prenant les mesures de prévention appropriées. L'occupation permanente de la loge du portier et du central de sécurité joue aussi un rôle capital.
- Il convient de sensibiliser et d'impliquer le **personnel** en matière de protection de la zone opérationnelle, par exem-

ple sous forme de stages d'équipe, de séminaires, formations etc.

Protection de base – Protection spéciale

Dans la majorité des cas, les mesures visant à protéger l'ensemble du site ont une fonction de **protection de base**, elles constituent le premier seuil de défense contre les personnes non autorisées. Il faut assurer en plus la protection spéciale individuelle de toutes les zones dangereuses existantes. Les mesures « classiques » destinées à la sécurité des installations ou objets jouent ici un rôle essentiel.

La **protection des zones individuelles dangereuses** représente en général la mesure de défense la plus importante, car il est rare d'obtenir une protection suffisante par les mesures « extérieures » qui touchent toutes les zones opérationnelles.

Ainsi, les mesures de protection extérieure ne portent pas atteinte à un risque d'acte intentionnel commis par des employés. Il n'est quasiment pas possible non plus de contrôler infailliblement l'accès à la zone opérationnelle ou à l'objet (par ex. au début du travail posté ou aux heures de pointe). Contrairement à cette situation, il est tout à fait possible d'effectuer un **contrôle beaucoup plus efficace** dans des **zones opérationnelles individuelles**.

3.3.2 Le personnel

Par principe, non seulement les intrus externes, mais également **internes** peuvent commettre des attentats contre une entreprise. Tandis que les concepts de protection contre les attaques de l'extérieur existent en nombre non négligeable, il s'avère que, pour le domaine des dangers potentiels commis par les auteurs internes, il y a une nécessité accrue d'agir. On définit sous ce terme les employés de l'entreprise ou les personnes externes qui ont légalement accès à la zone d'installations dignes de protection, mais qui entreprennent des actions illégales. Ils peuvent détenir de bonnes connaissances des installations et les exploiter dans un dessein criminel.

Sensibilisation du personnel

L'Etat d'une part, garant de la sécurité intérieure, et les exploitants des installations d'infrastructures d'autre part, sont tenus d'appliquer des mesures de défense. Des mesures préventives sont requises de la part des exploitants en plus des mesures générales des autorités chargées de la sécurité. Ces mesures sont attribuées avant tout au domaine de la **gestion et de la surveillance du personnel** (création d'une identification avec l'entreprise, motivation, utilisation sensible de mesures relatives au personnel exigeantes, formation des cadres etc.). Par ailleurs, il s'agit de procéder à une sensibilisation générale de tous les employés à cet ensemble de problèmes. Une discussion menée par des spécialistes particulièrement qualifiés peut s'avérer éventuellement utile. De même, il faut user de la possibilité d'un **contrôle de sécurité** des employés dans les domaines extrêmement sensibles. Pour une première analyse, les informations qui doivent être disponibles concerne le nombre d'employés externes, leur engagement envers la zone opérationnelle (notamment la durée du contrat) et le nombre moyen de visiteurs. Les autorités compétentes, notamment les commissariats de police, les Offices régionaux de police criminelle, l'Office fédéral de police criminelle, les Offices régionaux et l'Office fédéral pour la protection de la constitution donnent des indications complémentaires sur les mesures préventives au niveau du personnel.

3.3.3 Organisation et management

L'organisation interne, notamment les **mesures touchant à l'organisation du travail**, et le management constituent un cadre important à l'intérieur duquel il s'agit d'ajuster et de contrôler régulièrement les différentes mesures afin de garantir le fonctionnement totalement efficace de tout le système de sécurité. Dans ce contexte, les points suivants doivent être traités :

Organisation du travail

- Le service de cartes d'identité de l'entreprise avec délivrance et restitution de la carte d'identité, codage (type et suivi), dépôt (sécurité d'accès), compétences (définies aussi analogiquement pour les mots de passe ou les droits d'accès électronique)

- La méthode de recrutement et de surveillance du personnel chargé de tâches de protection, avec autorisation d'accès aux zones et postes de travail menacés.
- L'apprentissage professionnel, l'instruction et la formation de personnes afin d'éviter, par exemple, les erreurs de manipulation
- Règles de surveillance et contrôles réguliers en cas de travaux effectués dans les zones devant être protégées
- Les détails du système de clés avec système de fermeture (type, domaine, âge), délivrance, restitution et enregistrement des clés ainsi que dépôts des clés et cylindres
- Le nettoyage des zones devant être protégées, effectué par des employés internes ou externes, heures de nettoyage, surveillance lors du nettoyage, contrôle du personnel (pour le personnel externe)
- La liste des instructions de service pour toutes les mesures qui touchent à la protection
- Les plans d'alarme pour incendies et explosions, fuites, dangers menaçant l'environnement, événements spécifiques aux installations, prise d'otages, chantage etc.
- Le contrôle et l'actualisation réguliers du concept de protection de base, notamment du besoin de protection, des objectifs de protection et du catalogue des mesures.

3.4 Gestion du risque

Cycle de la gestion du risque

Les systèmes de gestion du risque comme instruments destinés à renforcer la sécurité d'une entreprise ont été généralement instaurés, jusqu'à présent, sur une base facultative. A la suite de l'amendement de la loi sur les sociétés anonymes (article 9, 2^{e} alinéa), certaines entreprises sont désormais **tenues** d'instaurer un système de surveillance afin de déceler très tôt les évolutions qui mettent en danger l'existence continue de la société . Le fondement des systèmes de gestion du risque est de définir une politique des risques comme partie intégrante de la politique générale de l'entreprise, fixant les lignes directrices du traitement des risques. Les systèmes de gestion du risque sont établis, en règle générale, au moyen d'un modèle de phase « analyse des risques, contrôle et maîtrise des risques,

surveillance des risques et financement des risques » qui se fondent sur la politique de gestion du risque adoptée pour l'entreprise:

- Dans l'analyse des risques, il convient d'identifier, d'analyser et d'évaluer individuellement pour chaque entreprise l'**intégralité** des **risques significatifs** pour l'entreprise, y compris les risques décrits dans le concept de protection de base.
- La gestion des risques sert à **prévenir** ou à minimiser **les risques** ou bien à les répercuter sur autrui (clients, assurances etc.) ; il faut accepter un **risque résiduel**.
- Dans le cadre de la surveillance des risques, des **systèmes de préalerte et de contrôle opérationnel** doivent être instaurés et la **politique des risques** de l'entreprise éventuellement ajustée.
- La question du financement des risques revêt une grande importance pour les entreprises, où des **considérations à moyen et long terme** doivent figurer au premier plan afin de pouvoir apprécier de façon appropriée les avantages des investissements en matière de sécurité, de concurrence.

L'introduction des systèmes de gestion du risque peut être supportée institutionnellement par la nomination d'un **délégué aux risques** qui conçoit, de concert avec les responsables compétents chargés de la sécurité dans l'entreprise, mais aussi avec les organismes compétents (publics ou privés), un système de gestion du risque hors de l'entreprise et l'ajuste continuellement aux conditions générales.

3.4.1 Planification des mesures d'urgence

Les exploitants ont à prendre des mesures en cas de détérioration, défaillance ou destruction de l'équipement d'infrastructures afin d'en **minimiser les effets**. Pour pouvoir maîtriser les conséquences d'une panne ou d'une crise sur les infrastructures critiques, les informations concernant les installations et les mesures réalisées et planifiées doivent également être disponibles auprès des autorités chargées de la limitation des risques. A leur tour, ces autorités doivent transcrire les scénarios

dans des plans d'urgence et d'intervention propres et appropriés. Les recommandations suivantes s'appliquent aux mesures qui limitent les incidences:

Coopération avec les autorités chargées de la limitation des risques

- Il en est de même pour les exploitants des installations et des matériels, qui ne sont pas soumis aux obligations légales élargies telles que l'ordonnance sur les accidents majeurs, mais qui se sont révélés comme devant être protégés, et qui doivent se mettre, **dans leur propre intérêt**, immédiatement en relation avec les autorités chargées de la limitation des risques et communiquer les informations nécessaires pour établir les plans d'urgence et d'intervention. Les autorités chargées de la protection et du maintien de la sécurité doivent se concerter en vue d'identifier ces installations potentielles importantes.
- Les autorités compétentes en matière de maintien de la sécurité doivent dresser, sans délai, **les plans externes d'urgence et d'intervention** sur la base des informations fournies par les exploitants pour protéger la population.
- En cas de catastrophe, les **plans des mesures** doivent être dressés et régulièrement actualisés (par exemple, les listes téléphoniques, l'attribution des responsabilités, les plans de déroulement). Ces plans de mesure comprennent également les préparations assurant le fonctionnement et l'efficacité de la **communication de crise**.
- Un **centre de renseignements** doit être créé. Pour cela, le personnel désigné et mis à disposition se réunit en cas de crise. Des locaux appropriés sont donc requis, ils doivent être protégés contre les influences extérieures et équipés de moyens de communication opérationnels.

Par ailleurs, il est recommandé de créer, mettre en application et contrôler régulièrement les **programmes d'urgence** concernant une éventuelle **indisponibilité du personnel**.

3.4.2 Communication des risques et communication de crise

Une communication appropriée et le plus efficace possible acquiert une importance particulière, aussi bien avant la survenance d'éventuelles crises qu'après la survenance de dommages graves se rapportant aux infrastructures critiques. Un

concept de communication doit être disponible, qui comprend les éléments suivants :

Communication de crise

- Avant même une crise qui ne peut jamais être entièrement exclue, il faut trouver et favoriser les **formes de communication appropriées** pour informer les médias et la population en cas de panne et les sensibiliser.
- Etant donné qu'il n'est jamais possible de garantir une protection intégrale, on accordera au préalable une importance particulière aux mesures de **limitation externe des risques**. Les autorités compétentes en la matière doivent obtenir les informations requises de la part des exploitants et prendre les mesures relevant de leurs compétences. Les informations requises par les exploitants et les autorités en vue d'évaluer la situation de risque doivent être disponibles, pour une grande part, en vertu des dispositions relatives au rapport de sécurité (article 9, ordonnance allemande sur les accidents majeurs) et aux plans d'urgence et d'intervention (article 10, ordonnance allemande sur les accidents majeurs, loi régionale sur la protection contre l'incendie et la protection civile). Pour les installations d'infrastructures non soumises à l'ordonnance sur les accidents majeurs, il convient de relever les informations nécessaires et de les documenter comme partie intégrante essentielle d'une **gestion intégrative de la protection**.

Coordination des voies de communication

- En cas de crise, il est capital d'agir et de communiquer rapidement. Dans ce genre de situation, les secteurs public et privé doivent réagir de façon coordonnée et pragmatique. Il convient de définir au préalable comment communiquer vers l'intérieur et l'extérieur en cas de crise, en tenant particulièrement compte des médias électroniques (et **de leur éventuelle défaillance**). Il faut définir comment communiquer par courrier électronique, pages web, téléphonie classique et mobile et par radio, et fixer les flux d'informations et les voies de communication des avis. Une importance particulière est accordée également à l'analyse de la situation (globale) des médias, car dans de nombreux cas, l'**effet psychologique** en soi peut dramatiser des événements au demeurant mineurs.
- Il faut considérer les parties de l'entreprise (par exemple les installations) pour lesquelles **la vie humaine** est menacée dans la zone méritant particulièrement une protection ou dans lesquelles de graves **atteintes à la santé** des

êtres humains sont à craindre. Ces informations constituent, entre autres, la condition sine qua non d'une communication efficace avec les services étatiques et doivent aussi faire partie intégrante du concept de protection de base de l'entreprise.

- En ce qui concerne toute objection éventuelle relative à la publication de données sensibles, les intérêts en cause concernés demandent à être examinés soigneusement et au cas par cas. Il faut noter que **l'information** de tierces personnes relative aux risques qui les concernent constitue non seulement un droit, mais aussi un **élément de prévention**. Outre l'examen des intérêts en cause, la publication requiert par conséquent la conception de critères permettant d'estimer la perte potentielle de sécurité par rapport au gain possible de protection.

Communication du risque: publication d'informations sensibles

3.4.3 Plan de secours et Plan de Continuité d'Activités

Mesure préventive du plan de secours

Afin de pouvoir maintenir en cas de crise l'activité de l'entreprise ou, à tout le moins, mettre en place un **fonctionnement en secours** afin de restaurer le plus rapidement possible le fonctionnement normal, il convient de fixer très tôt les concepts d'un plan de secours et les mesures s'y rapportant dans le cadre de la continuité d'activités. Le plan de secours et de reprise des activités comme mesures de prévention va au-delà de la gestion directe des urgences pour maîtriser la crise vécue ; l'élaboration de ces instruments centraux de maîtrise de la crise demande à être **initiée** et **accompagnée** par la **direction de l'entreprise.** Les plans de secours doivent notamment incorporer des concepts alternatifs pour l'organisation des processus de travail centraux en cas de défaillance des secteurs critiques dans l'entreprise, des sous-traitants et des prestataires de services, mais envisager aussi la mise à disposition de **fournitures de remplacement** ainsi qu'un site de repli. Ces plans doivent recouvrir au moins les points suivants:

- Il faut préparer des systèmes de remplacement (par exemple l'alimentation électrique de secours, les lignes des données, la production à voies multiples) pour les domaines particulièrement sensibles. Pour des raisons de sécurité, ceux-ci doivent être situés dans des **zones séparées**.

- Une quantité suffisante de **carburant** (pour la production, l'alimentation électrique de secours et autres processus vitaux) doit être disponible pour assurer le fonctionnement des installations. Il faut veiller en particulier aux effets d'événements à grande échelle qui peuvent s'étendre sur plusieurs jours (voies inaccessibles, longues pannes de courant).
- Les aspects d'un **aménagement sécurisé** des équipements de travail, installations et processus (limitation des incidences) doivent être pris en considération non seulement lors de la planification, mais aussi lors du fonctionnement.
- Pour se prémunir de l'indisponibilité de personnel due aux épidémies, par exemple, il faut disposer d'**effectifs suffisants**, notamment dans les positions-clés. Il est recommandé d'établir, de mettre en application et de contrôler régulièrement les programmes d'urgence concernant une éventuelle indisponibilité de personnel.
- Il faut vérifier régulièrement les plans de secours et d'urgence et les adapter aux nouvelles évolutions.

3.5 Gestion de la qualité et documentation des mesures de protection

3.5.1 La gestion de la qualité des mesures de protection

Intégration dans un système existant de gestion de la qualité

Les concepts de protection doivent être soumis à une gestion de la qualité afin d'assurer que les mesures de protection, telles qu'elles sont proposées, par exemple, dans le concept de protection de base, sont réalisées conformément aux exigences et **optimisées dans un processus d'amélioration** continu. Il est recommandé d'intégrer le concept partiel « gestion de la qualité des mesures de protection » dans un système de gestion de la qualité interne à l'entreprise, de fixer les compétences et les responsabilités et de les documenter. La gestion de la qualité relative aux mesures de protection a donc également une place déterminée dans la **gestion de l'entreprise**, elle fait partie intégrante des **missions** de sa **direction.**

Les exigences doivent être formulées de façon claire et univoque pour assurer une mise en oeuvre satisfaisante des mesures de protection et un contrôle continu. Elles se conforment donc aux critères **s.m.a.r.t**:

s (spécifique): Quel est l'objectif et comment l'atteindre exactement ?

m (mesurable) : Existe-t-il des critères de mesure ou des références qui permettent de mesurer et contrôler la mise en oeuvre des objectifs ? Les listes de contrôle sont-elles conçues en conséquence?

a (attractif, accepté): L'objectif est-il ambitieux, sa réalisation peut-elle être activée grâce aux ressources disponibles?

r (réaliste, réalisable): L'objectif peut-il être réalisé compte tenu des circonstances et des ressources ?

t (terme) : Un délai est-il fixé à l'intérieur duquel l'objectif (ou les objectifs intermédiaires) doit être atteint ?

Cycle de contrôle de la gestion de la qualité

La gestion de la qualité n'est pas un processus statique, mais obéit à un cycle de contrôle qui comprend la planification, la mise en œuvre, l'analyse et la mise au point, générant un processus d'amélioration continue. Par conséquent, il s'agit de soumettre aussi régulièrement que possible les mesures de protection à un contrôle régulier et de faciliter toute possibilité de **mise au point précise** en cas de modifications (formations complémentaires du personnel chargé de la sécurité, ajustement des processus etc.).

3.5.2 Documentation des mesures de protection

Les mesures de protection de chaque zone exposée aux risques doivent être documentées dans un concept de protection de base de l'entreprise, un regroupement en zones, bâtiments, sections ou unités fonctionnelles pouvant s'avérer pertinent. Il va sans dire que cette information est de nature **particulièrement confidentielle**. Les aspects suivants doivent être pris en considération pour les zones exposées:

- Situation sur le site (plan-masse), situation au sein des bâtiments ou des zones (tracé).

- Entrées, accès, issues de secours
- Construction et réalisation mécanique des séparations des zones (murs, clôtures)
- Construction des bâtiments et des locaux à protéger (matériels, armure, épaisseur des murs)
- Sécurité mécanique des portes, fenêtres et passages.
- Mesures de surveillance électronique au niveau des portes, fenêtres, pièces etc.
- Suivi du contrôle d'accès aux zones concernées pendant et après le service pour le personnel et les externes
- Protection des éléments individuels de commande contre toute erreur de manipulation ou sabotage, par exemple via un verrouillage mécanique ou une surveillance électronique
- L'application de panneaux indicateurs et d'avertissement
- Mesures de protection particulières
- Durées de service et de travail posté des services compétents, différenciation des mesures de protection
- Patrouille de surveillance des matériels, effectuée par le service de surveillance (voies et heures des rondes de surveillance).

Table des catégories de risques

	Catégorie de risques 1	Catégorie de risques 2	Catégorie de risques 3
Mobile :	L'auteur (le contrevenant) a l'intention de causer un dommage limité. Il est conscient ,ou pas, de générer une situation de risques beaucoup plus importante (intention conditionnelle).	L'auteur (le contrevenant) veut déclencher un dommage plus important et donc engendrer une situation de risques générale, éventuellement aussi comme technique de diversion (intention directe).	L'auteur (le contrevenant) vise des attentats massifs (manière d'agir brutale et particulièrement dangereuse).
Motivation:	Vengeance, frustration, volonté de mettre en lumière les insuffisances, obtenir des effets politiques, attirer l'attention, racket.	Radicalisme politique , vengeance, obtention d'importants avantages pécuniaires, concurrentiels.	Anarchisme, volonté de provoquer par la force des changements dans la société , « punir » les entreprises (au titre de représentantes des Etats ou des gouvernements), mobiles liés à la croyance religieuse.
Actions de préparation :	Espionner, se procurer les outils et données	Reconnaissance des composants et des points faibles relatifs à la sécurité, voire exploitation ciblée des lacunes lors de la surveillance. Procuration d'accessoires spéciaux, éventuellement mise hors service des dispositifs de sécurité.	Préparations logistiques, espionnage, mise hors service des installations de sécurité.
Outils de l'acte punissable :	Outils simples ou spéciaux ; éventuellement compositions incendiaires simples.	Outils simples ou spéciaux, dispositifs explosifs et incendiaires peu usités d'ordinaire (fabrication artisanale).	Outils simples et spéciaux, dispositifs explosifs et incendiaires peu usités d'ordinaire, explosifs en grandes quantités, armes (NRBC), avec risque conscient de perdre la vie lors de l'attentat.

	Catégorie de risques 1	Catégorie de risques 2	Catégorie de risques 3
Cercle de personnes :	A l'extérieur: Groupes radicaux, agissant sur ordre de criminels actifs; auteurs isolés, enclins à la violence. A l'intérieur : Le personnel, les anciens salariés licenciés, membres des employés externes et visiteurs.	Auteurs isolés, groupes d'auteurs, éventuellement aussi dans le cadre de la « criminalité organisée », groupes politiques radicaux.	Auteurs isolés et groupes extrémistes et terroristes.
Commentaires/exemples :	Mise hors service des installations de sécurité, interventions dans les déroulements de la production, la non-signalisation des états critiques de l'installation, incendie criminel, vandalisme à la suite d'un cambriolage raté, incendie criminel pour d'autres motifs.	Incendie ou attentat à l'explosif, destruction des équipements opérationnels, atteinte aux installations de commande, y compris erreur de programmation des processeurs pilote.	Attaque à main armée, emploi d'explosifs dans des lieux animés, tir de missile, fait d'incendier des installations importantes, attaques du personnel de surveillance, attentats ciblés contre les domaines particulièrement sensibles, utilisation d'agents de combat biologico-chimiques, contamination radioactive à explosion (« dirty bomb »).

4.

Autorités et institutions à contacter

Parallèlement aux possibles améliorations techniques de sécurité et organisationnelles, la **collaboration efficace et étroite** entre les exploitants d'infrastructures critiques et les autorités chargées de la sécurité et du maintien de la sécurité publique joue un rôle particulièrement important.

Les autorités et les institutions compétentes doivent se concerter sur la protection de base, afin de l'intégrer efficacement pour exploiter les informations relatives aux risques et choisir les mesures appropriées. Quant aux risques liés aux événements naturels, à une erreur humaine ou une défaillance technique, il convient de contacter à temps, par exemple, les autorités et organismes d'aménagement du territoire, les instituts de géologie et d'informations météorologiques, les offices de prévention des catastrophes et des incendies, les services de régularisation, les services administratifs pour le maintien de l'ordre et les services de la construction, les autorités chargées de la protection contre les nuisances ainsi que les services de protection de l'environnement. Les interlocuteurs directs des entreprises et des exploitants d'infrastructures critiques sont d'abord les autorités municipales et les administrations régionales.

Au niveau national, l'**Office fédéral pour la protection des populations et la gestion de catastrophes (BBK)** assume des tâches relatives à la protection de la population et d'assistance en cas de catastrophe. Cet office fédéral, le BBK,

réunit, de façon interdisciplinaire, tous les domaines de la prévention de la sécurité civile en un système de protection efficace destiné à la population et à ses bases critiques. Comme «centres d'alimentation de réseau", le **centre de protection des infrastructures critiques** du BBK a pour mission, entre autres, d'informer de la signification des infrastructures critiques pour l'Etat et la société, de sensibiliser, d'établir des coopérations entre autorités et entreprises, de développer des concepts d'analyse et de protection et de proposer des mesures de protection des infrastructures critiques à court, moyen et long terme.

L'**Agence fédérale de Secours Technique (THW)** apporte son concours technique en matière de protection civile et de lutte contre les catastrophes, états d'urgence civils et sinistres de grande envergure. L'Agence THW opère, sur demande des services compétents, pour le maintien de la sécurité et remplit, entre autres, les tâches de prévention technique des risques dans les infrastructures, d'aide technique dans la protection de l'environnement et d'approvisionnement de la population en cas de catastrophe.

Dans la mesure où un soutien externe, de la police par exemple, est nécessaire pour assurer la **protection contre toute intervention de personnes non autorisées**, l'exploitant doit, préalablement à toute intervention éventuelle, prendre contact avec les autorités locales compétentes.

En Allemagne, ce sont les Länder qui sont compétents dans le champ du maintien de la sécurité, des mesures de prévention des risques et d'enquêtes et investigations. La **Police fédérale** (anciennement le Service fédéral de protection des frontières – BGS) est l'interlocuteur à contacter dans le domaine de protection des installations ferroviaires, des aéroports et des frontières. L'**Office fédéral de police criminelle** (BKA), par exemple, acquiert les compétences en matière d'enquêtes uniquement dans des cas d'exception, tels que dans les cas de cybercriminalité grave selon l'article § 303 b du Code pénal allemand, dans la mesure où les éléments de fait indiquent que l'acte est dirigé a) contre la sécurité intérieure et extérieure de la République fédérale d'Allemagne ou b) contre les zones sensibles où

se trouvent des équipements vitaux, dont la défaillance ou la destruction constituerait une menace considérable pour la santé et la vie humaine, ou bien encore contre des équipements indispensables au fonctionnement de la société.“ Dans des situations exceptionnelles, l’Office fédéral de police criminelle (BKA) intervient également dans certaines enquêtes, même si ce domaine ne relève pas de ses compétences, en vertu de l’article 4 de la loi sur l’Office fédéral de police criminelle et la collaboration de l’Etat fédéral et des Länder dans les affaires criminelles (Loi relative au Bundeskriminalamt et à la coopération entre la Fédération et les Länder en matière de police judiciaire - Bundeskriminalamtgesetz – BKAG) .

L’**Agence fédérale de la sécurité des systèmes d'information** (**BSI**) se charge spécialement des questions touchant la **sécurité informatique** dans la société d’information. En qualité de prestataire central de sécurité de l’information de l’Etat fédéral, le BSI fournit des renseignements sur les risques et dangers lors de l’application de la technologie de l’information, et développe, entre autres, des critères et méthodes permettant de contrôler et évaluer la sécurité des systèmes d’information ; elle peut par ailleursconseiller, outre les constructeurs et distributeurs, également les utilisateurs, en répondant à toutes les questions relatives à la sécurité dans la technologie de l’information.

Annexe 1

Catalogue de questions et modèle d'une liste de contrôle

Le concept de base de protection peut être mis en place uniquement lorsque les acquis théoriques des dangers, menaces et risques sont opérationnalisés au moyen des concepts de gestion correspondants. Les catalogues de questions ainsi que les listes de contrôle facile à traiter s'imposent de plus en plus à l'échelle mondiale comme outils d'opérationnalisation des concepts de sécurité.

Le catalogue de questions présenté ici et la liste de contrôle sont à considérer comme modèles pour mettre en application le concept de protection de base orienté vers les utilisateurs. Les questions doivent avant tout permettre d'amorcer un **processus de discussion interne à l'entreprise** sur le renforcement de sa sécurité et orienter ce dernier en l'adaptant au cas par cas. Les listes de contrôle doivent servir d'instrument d'assistance et de contrôle concret dans le cadre de la mise en application.

Catalogue de questions

Le catalogue de questions ne revêt pas un caractère définitif, mais il importe de le compléter et de le perfectionner au même titre que le modèle de la liste de contrôle dans le processus de coopération.

Structures et coopérations (organisation et management)

1. Comment est structurée et présentée la sécurité de l'entreprise ? Quelles sont les relations ou les structures de

coopération qui existent ou sont prévues entre la sécurité matérielle, informatique et personnelle ?

2. Comment collabore l'entreprise dans le domaine de la sécurité avec d'autres entreprises, y compris avec d'autres utilisateurs de l'infrastructure ou au sein d'associations régionales ? Comment collabore-t-elle avec les fournisseurs privés en charge de ses externalisations ?

3. Quelles sont les mesures de sécurité et les structures de coopération qui existent ou sont planifiées au niveau des composants situés en amont et en aval des chaînes de valeur? Quelles coopérations supplémentaires existe-t-il en cas de sinistre grave? Comment la collaboration avec les autorités intervenantes chargées de la sécurité et les organismes de secours et de protection civile est-elle réglée et comment est-elle évaluée?

4. Quelles organisations de l'entreprise, du secteur ou des autorités de contrôle ou organisations externes traitent de l'analyse des sinistres (reconstitution du sinistre et de sa cause, conclusions, mise en application, contrôle des résultats) et se penchent, sur cette base, sur le développement de la sécurité technique?

Etudes, concepts (analyse du besoin de protection)

5. Quelles conceptions spéciales en matière de sécurité existe-t-il pour les domaines particulièrement sensibles ? Sur quels critères ces domaines sont-ils identifiés et hiérarchisés ? Quel est le niveau de protection qui a été déterminé ? A quels résultats aboutissent des études comparées des concepts et développements internationaux ?

6. Quels études et concepts relatifs à la substitution de services existe-t-il en cas de situation de préjudice ?

7. Quelles sont les approches utilisées en matière de gestion de la qualité et de gestion du risque et quelles en sont les expériences ? Quelle importance revêt la gestion de la protection dans le processus d'optimisation de l'entreprise ?

8. Quelles sont les analyses de risques existantes? Qui en a délégué les grandes lignes et qui les a réalisées ? Existe-t-il des concepts s'agissant d'une analyse intensifiée et intersystèmes, d'un développement éventuel de mesures concernant les interdépendances ?

9. Est-ce que des analyses coûts-profits portant sur l'utilisation et l'instauration des mesures de sécurité seront effectuées ?

10. Quels incidents seront enregistrés ? Quelles sont les déclarations possibles portant sur les incidents non saisis ?

Mesures de prévention (protection intérieure, extérieure et personnelle)

11. Quelles conséquences exceptionnelles ont été tirées des incidents particulièrement graves liés au domaine d'activité principal de l'entreprise dans le passé, (voire aussi à l'échelle mondiale).

12. Quels sont les outils utilisés pour la surveillance technique, les enquêtes et la conservation de la preuve ? Comment les mesures sont-elles avérées ?

13. Par quelles mesures techniques et organisationnelles a) les produits et b) les processus et installations de production sont-ils protégés contre les abus ?

Gestion de crise en cas de situation de sinistre (plan de secours, plans d'urgence)

14. Comment est traité l'incident ? Comment apprécie-t-on les différentes étapes d'une situation qui s'aggrave, et notamment l'évaluation du risque, les pouvoirs de décision etc. Existe-t-il des approches spécifiques au secteur ou des instructions pour agir en vue de différencier les situations de sinistre et du traitement de l'incident ?

15. Quelle optimisation doit être apportée a) dans l'optique des autorités et b) aux autorités et organisations chargées de la sécurité (AOS) du point de vue de la capacité d'agir en cas de situation de sinistre ?

16. Quels exercices d'alerte ont été effectués jusqu'à présent ou sont prévus pour maîtriser le sinistre ?

Modèle d’une liste de contrôle "protection de base"

Tout comme le catalogue de questions, la liste de contrôle suivante doit servir également d’instrument d’aide à la mise en oeuvre du concept de protection de base.

Comme les particularités individuelles spécifiques et locales ne peuvent être cependant prises en considération, il faudra adapter les aspects requis ici aux besoins spécifiques respectifs et, le cas échéant, les compléter; il est indispensable aussi d’indiquer éventuellement des mesures de sécurité complétives. La liste de contrôle est uniquement un **modèle sans caractère définitif**.

La liste de contrôle comprend les mesures de protections des domaines suivants:

1. **Protection de l’objet**
2. **Personnel**
3. **Organisation**
4. **Gestion du risque**
5. **Plan d’urgence et plan de secours**

Protection de l'objet
(Situation de l'objet, construction, sécurisation du périmètre intérieur,[4] protection des bâtiments)

	Oui	Non	Planifié	Nécessité d'agir / mesures
Emplacement de l'objet				
Peut-on exclure une menace contre l'entreprise liée à des événements naturels graves ?				
Les crues				
Les grandes vagues liées aux tempêtes				
Les tremblements de terre				
Les coulées de boue et glissements de terrain				
Les avalanches				
Les tempêtes				
…				
La périphérie autour de l'entreprise est-elle bien visible et la distance par rapport aux bâtiments voisins suffisante pour pouvoir constater une intrusion indue (*construction ouverte*)?				
Si ce n'est pas le cas, l'entreprise est-elle protégée des bâtiments adjacents d'autrui de manière à rendre plus difficile l'accès non autorisé (par exemple s'introduire en empruntant les toits adjacents) (*construction fermée*)?				

[4] Le *périmètre intérieur* est la surface comprise entre la limite du terrain et du bâtiment.

	Oui	Non	Planifié	Nécessité d'agir / mesures
Construction				
Le site de l'entreprise est-il bien aménagé pour le transport et dispose-t-il d'une sortie principale et de sortie(s) de secours indépendante(s) ?				
Le site est-il protégé contre une intrusion indue, voire violente en matière de construction ? Bittes				
Eléments en béton				
Barrières				
…				
Existe-t-il des places de stationnement ouvertes à l'usage du public à l'extérieur du terrain (zone publique) ?				
Si oui, la distance par rapport aux bâtiments à protéger est-elle suffisante ?				
Existe-t-il des parties de bâtiments dignes de protection à l'extérieur des sites exposés et des zones particulièrement menacées ?				
Les façades des bâtiments sont-elles lisses et sans saillies ?				
Les paratonnerres et autres annexes sont-ils montés de manière à ne pas pouvoir les utiliser comme outils auxiliaires de montée ?				
Les tuyaux de descente d'eau pluviale sont-ils posés sous plâtres ou revêtus ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
Les conduites et les raccordements au réseau de distribution (courant, huile/gaz, eau, téléphone) sont-ils enterrés et protégés contre toute manipulation ?				
L'alimentation des prises de courant extérieures peut-elle être mise sous tension ?				
Protection du périmètre intérieur				
Le terrain de l'entreprise est-il enclos ?				
L'enceinte est-elle continue?				
La clôture est-elle posée en ligne droite ?				
L'enceinte est-elle relativement résistante à la rupture ?				
L'enceinte est-elle exempte d'outils permettant de monter ou de grimper par dessus (traverses, arbres riverains) ?				
La clôture a-t-elle une hauteur minimale suffisante ?				
La clôture est-elle équipée d'une protection anti-intrusion (porte-à-faux avec bande ou fils barbelés) ?				
Si l'enceinte se compose d'une clôture, existe-t-il une protection anti-intrusion par-dessous ?				
Si oui, cette protection est-elle installée de manière à ne pas pouvoir l'utiliser comme outil de montée (socle en béton ou bordures en béton) ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
Les portails et les portes situés à l'intérieur de l'enceinte (par ex. la clôture) correspondent-ils à la hauteur et à la résistance de l'enclos ?				
Existe-t-il des contrôles techniques des accès tels portes coulissantes/à vantaux équipées d'une protection anti-intrusion, éventuellement avec sas [double porte], lecteurs de cartes et/ou code sur clavier, technique vidéo, interphone) ?				
Une détection électronique automatique se déclenche-t-elle en cas de tentative d'intrusion par dessus la clôture/par les entrées et accès (détection par systèmes d'alarme sur les clôtures/les portes, technique vidéo avec technologie des capteurs, protections des couronnements de murs, système de détection radar, barrières lumineuses haute fréquence, détecteurs d'effraction) ?				
Existe-t-il un éclairage extérieur sans ombre portée ?				
Les appareils d'éclairage sont-ils protégés contre les détériorations (au moyen d'un vitrage anti-projectile ou corbeilles en fil métallique à mailles serrées) ?				
L'alimentation électrique de l'éclairage extérieur se fait-il par conducteur enterré ?				
La clôture est-elle surveillée par des caméras vidéo ?				
Si oui, l'entreprise dispose-t-elle d'un personnel de surveillance formé en conséquence et capable d'agir pour le contrôle des écrans vidéo ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
Si tel est le cas, le personnel de surveillance est-il chargé également des rondes de surveillance ?				
Est-ce que l'entreprise utilise des caméras thermiques et des appareils de détection nocturne ?				
Les zones névralgiques et les bâtiments (ou parties de bâtiments) sont-ils contrôlés par des rondes de surveillance ?				
Les plantations du terrain (notamment les arbres, arbustes hauts) sont-elles suffisamment éloignées des portes, des escaliers, du rez-de-chaussée et des fenêtres de cave ?				
Protection des bâtiments				
Les zones sensibles des bâtiments sont-elles protégées de l'extérieur des regards indiscrets ?				
L'entreprise renonce-t-elle aux balises des parties de bâtiment qui requièrent une protection (poteaux indicateurs, plaques de porte) ?				
Est-il nécessaire d'avoir des zones de sécurité indépendantes à l'intérieur du site ?				
Ces zones sont-elles suffisamment sécurisées mécaniquement et électroniquement ?				
Des autorisations d'accès distinctes ont-elles été élaborées pour ces zones (concept de fermeture/contrôle d'accès technique) ?				
L'accès et la sortie des zones sensibles sont-ils surveillés séparément ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
Les portes extérieures, les fenêtres accessibles et les soupiraux sont-ils intégrés dans une installation de détection d'effraction ?				
Les fenêtres de cave sont-elles équipées de grilles de sécurité agréées (classe de résistance minimale 5 conformément à la norme DIN 18106) ?				
Les soupiraux sont-ils dotés de grilles de défense stables et de dispositifs antirelevage verrouillables ou vissés à demeure ?				
Les ouvertures des puits d'alimentation et d'évacuation dont le diamètre est supérieur à 30 cm sont-ils munis de grilles ?				
Les lucarnes/lumidômes sont-ils sécurisés mécaniquement et électroniquement ?				
Les bâtiments sont-ils équipés de fenêtres anti-effraction contrôlées (selon la norme DIN ENV 1627) ?				
Les fenêtres des toilettes et des autres pièces dans lesquelles, par expérience, les fenêtres sont souvent en position inclinée sont-elles grillagées ?				
Les fenêtres sont-elles en verre de sécurité (vitrage A anti-projectile, vitrage B anti-effraction, vitrage C anti-balles, vitrage D anti-explosion) ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
Les fenêtres non grillagées (si techniquement possible) sont-elles équipées de ferrures anti-effraction d'une classe de résistance minimale CR 5, de verre de sécurité feuilleté anti-projectile (conformément à la norme DIN EN 356, classe de résistance P 6 A), de grilles de fenêtre verrouillables et de parcloses vissées ?				
Le nombre de portes qui mènent à l'extérieur est-il limité à un nombre raisonnable ?				
Les portes extérieures correspondent-elles au minimum à la classe de résistance CR 5 selon la norme DIN ENV 1627 ?				
La porte d'entrée principale dispose-t-elle – d'un lecteur de cartes ou de puces ?				
– de serrures munies d'un dispositif d'accouplement et d'autoverrouillage ?				
– de gâches de sécurité électriques d'une résistance minimale à l'écrasement 15000 N ?				
– de ferme-portes automatiques ?				
– d'un bouton à l'extérieur (en cas d'utilisation de gâches électriques)				
– d'un interphone vidéo ?				
Les portes de secours sont-elles équipées de serrures anti-paniques, autoverrouillantes, de ferme-portes automatiques et de contrôleurs de portes avec alarme locale ?				
L'entrée principale et les autres accès sont-ils toujours fermés également dans la journée et accessibles uniquement par les personnes autorisées ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
L'entrée principale est-elle équipée d'un dispositif d'accès à l'unité (tourniquet ou système de portes tournantes en métal ou de construction en verre) ou d'un sas ?				
L'entrée et la sortie sont-elles séparées ?				
La validation de l'accès des personnes autorisées s'effectue-t-elle par voie d'autorisations électroniques d'accès (cartes, transpondeur) ?				
Si tel est le cas, la génération, le dépôt, l'administration et la délivrance des autorisations d'accès électroniques sont-ils gérés centralement ?				
Est-ce qu'une simple attribution de la carte à l'entreprise est exclue ?				
Les clés [un grand nombre de clés] sont-elles remises exclusivement aux personnes autorisées ?				
La génération, le dépôt, l'administration et la délivrance des clés sont-elles gérées centralement ?				
Est-il possible d'obtenir un double des clés dans un magasin spécialisé uniquement sur présentation d'une carte de sécurité ?				
Les clés de réserve sont-elles gardées en lieu sûr ?				
Les autorisations électroniques d'accès ou les clés sont-elles remises uniquement contre quittance (et documentation) ?				

	Oui	Non	Planifié	Nécessité d'agir / mesures
En cas de modification des affectations liées à l'acquisition de nouvelles compétences ou de démission des employés, les autorisations de fermetures font-elles immédiatement l'objet d'un contrôle ?				
Prévention des incendies				
Existe-t-il un système paratonnerre (paratonnerre extérieur) conformément à la norme DIN VDE 0185 ?				
Les prescriptions existantes de prévention des incendies (DIN 4102) et les modalités du Service de contrôle des constructions de bâtiments sont-elles respectées ?				
Le corps des sapeurs-pompiers local a-t-il été consulté pour le plan de prévention des incendies ?				
Existe-t-il un système de détection de dangers dont les détections et l'alarme sont transmises à un poste occupé en permanence (accueil, loge du portier, service de gardiennage et de sécurité, sapeurs-pompiers etc.) ?				
Mesures de protection supplémentaires				

Personnel
(Employés, personnes externes[5])

	Oui	Non	Planifié	Nécessité d'agir / mesures
Personnel (interne et externe)				
L'entreprise effectue-t-elle un contrôle de sécurité lorsqu'elle recrute de nouvelles collaboratrices ou de nouveaux collaborateurs ?				
L'entreprise effectue-t-elle un audit de sécurité en cas d'emploi (temporaire) de personnels externes ?				
Les contrôles de sécurité sont-ils effectués pour la protection personnelle contre le sabotage selon la loi sur les audits de sécurité ?				
Le personnel s'engage-t-il à respecter les lois, dispositions en la matière et les réglementations internes (par ex. l'article 5 de la loi fédérales « informatique et libertés » relatif au « secret des données ») ?				
Le personnel est-il sensibilisé aux questions de sécurité (terrorisme, sabotage) ?				
Personnes externes[5]				
Les personnes externes doivent-elles se présenter à l'accueil, à l'entrée ou au service de surveillance ?				

[5] Personnes externes : telles que visiteurs, artisans, le personnel d'entretien et de nettoyage.

	Oui	**Non**	**Planifié**	**Nécessité d'agir / mesures**
Les personnes externes sont-elles identifiables rapidement et facilement (au moyen notamment de cartes visiteurs) ?				
Les personnes externes sont-elles accompagnées/contrôlées ?				
Les fournisseurs et les marchandises sont- ils contrôlés ?				
Mesures de protection supplémentaires				

Organisation (interne et externe à l'entreprise)				
	Oui	**Non**	**Planifié**	**Nécessité d'agir/mesures**
Organisation interne à l'entreprise				
Existe-t-il dans l'entreprise un délégué chargé de la sécurité formé en fonction ?				
L'objet protégé est-il suivi par un personnel chargé de la sécurité appartenant à l'entreprise ?				
Le personnel interne chargé de la sécurité connaît-il les dispositions juridiques et les devoirs et compétences spécifiques requises pour l'exercice de ses tâches, ainsi que leur application pratique (par information, par exemple, par analogie à l'article 34 a du Code de législation industrielle et du travail et à l'article 4 de l'ordonnance allemande relative à la surveillance) ?				
Les exigences et/ou normes légales relatives à la sécurité sont-elles claires ?				
Les exigences de sécurité (guides, lignes directrices) sont-elles réglées ?				
Le personnel est-il informé des exigences de sécurité de l'entreprise et régulièrement formé ?				
Les événements touchant à la sécurité sont-ils enregistrés ?				
Des conséquences ont-elles été tirées des incidents relatifs à la sécurité ?				

	Oui	Non	Planifié	Nécessité d'agir/mesures
Le personnel dispose-t-il des connaissances de base en matière de sécurité du travail, de prévention des accidents et des « premiers secours » ?				
Les dangers potentiels et les indicateurs de pré-alerte ont-ils été identifiés ?				
Existe-t-il un concept de hiérarchisation des sites sensibles et des processus de l'entreprise ?				
Existe-t-il un poste de sécurité dans les sites d'implantation classés comme étant sensibles?				
Existe-t-il un catalogue des matières dangereuses dans l'entreprise ?				
Existe-t-il des plans exacts de toutes les conduites d'alimentation et d'évacuation (courant, eau d'égouts, eau, gaz, téléphone, détection des dangers)?				
Existe-t-il des plans pour les mesures de sécurité hiérarchisées (qui dépendent de la situation de menace actuelle) ?				
Y a-t-il une stratégie de mise en place sur les incidents de sécurité et leur gravité, plus ou moins grande?				
Existe-t-il un plan d'alerte ?				
Existe-t-il des règles de conduite à tenir et des moyens de les communiquer en cas d'incidents de sécurité?				
Existe-t-il des briefings réguliers sur les issues de secours ?				

	Oui	Non	Planifié	Nécessité d'agir/mesures
Existe-t-il des exercices d'évacuation réguliers ?				
Existe-t-il des exercices réguliers de simulation d'incendie ?				
Les acquis des exercices sont-ils intégrés dans les concepts de formation ?				
Existe-t-il une communication de crise (information aux employés, interlocuteurs pour les autorités et médias) ?				
Est-ce qu'une assistance psychologique du personnel concerné est garantie en cas d'incident de sécurité ?				
Organisation externe à l'entreprise				
Existe-t-il une communication « catastrophe » (communication prioritaire pour la télécommunication) ?				
La gestion de la sécurité est-elle exclusivement entre les mains de l'entreprise ?				
Si tel n'est pas le cas, les cocontractants et les prestataires en matière de sécurité répondent-ils à la norme DIN 77200, niveau 3 ?				
Cela s'est-il avéré efficace pour la direction de l'entreprise ?				
Existe-t-il des accords entre l'entreprise et les prestataires en matière de sécurité (établissement du contrat, collaboration pratique, compétences en cas de crise) ?				

	Oui	Non	Plani-fié	Nécessité d'agir/mesures
Le personnel de sécurité suit-il un entraînement en rapport avec cette thématique et béneficie-t-il d'une formation continue dans ce domaine ?				
La criticité des services externalisés a-t-elle été évaluée par rapport au fonctionnement de l'entreprise?				
L'entreprise évite-t-elle les sources ouvertes qui pourraient constituer un risque pour elle (par ex. vues aériennes disponibles sur Internet, matières et quantités produites, voies de distribution etc) ?				
Mesures de protection supplémentaires				

Gestion du risque				
	Oui	**Non**	**Planifié**	**Nécessité d'agir / mesures**
Une politique de gestion du risque, impérative pour toute l'entreprise a-t-elle été définie ?				
Existe-t-il pour des secteurs partiels de l'entreprise une politique spécifique de gestion du risque ?				
Tous les risques possibles pour l'entreprise sont-ils saisis et évalués, y compris ▪ les risques liés aux événements naturels,				
▪ les risques liés à une défaillance humaine ou technique,				
▪ les risques liés au terrorisme ou aux abus criminels ?				
L'entreprise mène-t-elle une réflexion sur les dangers issus de son environnement (centrales électriques, lignes de chemin de fer etc) ?				
Les normes de sécurité prévues et le risque admis sont-ils définis globalement et par catégorie de risques ?				
Est-ce que tous les risques se situent dans le domaine des risques résiduels acceptables ?				
Existe-t-il des mesures de maîtrise des risques dans tous les secteurs partiels (événements naturels, défaillance humaine ou technique, terrorisme, abus criminels) et sont-elles concertées ?				

	Oui	**Non**	**Planifié**	**Nécessité d'agir / mesures**
Existe-t-il des instruments appropriés de surveillance des risques (systèmes de préalerte et de contrôle opérationnel) ?				
Les décisions relatives au financement des risques reposent-t-elles sur des analyses coût-profit à moyen et long terme?				

Plan d’urgence et plan de secours

	Oui	Non	Planifié	Nécessité d’agir / mesures
Existe-t-il un manuel d’intervention en cas de crise et d’urgence ?				
Existe-t-il une réglementation de la responsabilité en cas d’urgence ?				
Existe-t-il des plans de crise et d’urgence pour des événements dommageables bien déterminés ?				
Y-a-t-il des exercices réguliers d’urgence ?				
Des modes de communication et des dispositifs de prise de décision sont-ils organisés en cas de sinistre ?				
Existe-t-il, en cas de sinistre grave, des coopérations avec les autorités compétentes ?				
Existe-t-il des plans de crise et d’urgence concertés avec les autorités compétentes ?				
Existe-t-il une alimentation électrique de secours suffisante qui comprend également les équipements de sécurité ?				
Est-ce que des mesures techniques et organisationnelles de prévention des incendies sont prises ?				
Extincteurs				
Installations de détection d’incendie				
Formation du personnel				
Issues de secours				
Contrôle				
...				
Est-ce que des exercices sont effectués pour faire face aux situations de sinistre (intégrant les autorités compétentes) ?				

	Oui	**Non**	**Planifié**	**Nécessité d'agir / mesures**
Existe-t-il une protection technique et organisationnelle contre les défaillances dans le processus de production ?				
Existe-t-il des études et concepts relatifs à la défaillance dans la fourniture de prestations externes en cas de sinistre ?				
Existe-t-il des fournitures de rechange?				
Existe-t-il des concepts permettant le rétablissement des prestations et de la production à la suite de sinistres (Plan de Continuité des Activités – PCA) ?				
Mesures de protection supplémentaires				

Annexe 2

Indications dans la perspective de la police

Il existe trois publications que le Bureau spécialisé dans le domaine des « délits commis à l'aide d'explosif et par incendie » de l'Office fédéral de police criminelle (BKA) a établies pour les Offices régionaux de police criminelle et les entreprises concernées. Ces publications comportent des indications sur les premières mesures à prendre en cas de menaces à la bombe ou relatives à la conduite à tenir à la réception d'un courrier suspect ou des matières biologiques ou bien chimiques. Elles peuvent être demandées auprès des Offices régionaux de police criminelle compétents (voir adresses ci-après).

En raison de la menace considérable que représentent de tels courriers pour les personnes, il convient de prévoir déjà au préalable des mesures de réduction des dangers. Outre l'entraînement de base des employés, les exercices réguliers, la définition des responsabilités et, éventuellement aussi les transformations (mot-clé : services courrier isolés) font également partie de ces mesures.

Remarque :

Appelez toujours le numéro d'urgence de la police en cas d'alerte à la bombe !

En principe, il faut prendre toute menace à la bombe au sérieux, la police devra en effectuer l'évaluation définitive – sur la base des informations et impressions recueillies par le destinataire d' alerte à la bombe.

Office de Police criminelle de Bade-Wurtemberg
Taubenheimstraße 85
70372 Stuttgart

Office hessois de Police criminelle
Hölderlinstraße 5
65187 Wiesbaden

Office de Police criminelle de Saxe Sachsen
Neuländer Straße 60
01129 Dresden

Office bavarois de Police criminelle
Maillingerstraße 15
80636 München

Office de Police criminelle du Mecklenbourg-Poméranie-Occidentale
Retgendorfer Str. 2
19067 Rampe

Office de Police criminelle de la Saxe-Anhalt
Lübecker Straße 53-63
39124 Magdeburg

Office de Police criminelle de Berlin
Platz der Luftbrücke 6
12101 Berlin

Office de Police criminelle de Basse-Saxe
Schützenstraße 25
30161 Hannover

Office de Police criminelle du Schleswig-Holstein
Mühlenweg 166
24116 Kiel

Office de Police criminelle de Brandenbourg
Tramper Chaussee 1
16225 Eberswalde

Office de Police criminelle de la Rhénanie-du-Nord-Westphalie
Völklinger Straße 49
40221 Düsseldorf

Office de Police criminelle de la Thuringe
Am Schwemmbach
99099 Erfurt

Office de Police criminelle de Brême
In der Vahr 76
28329 Bremen

Office de Police criminelle de la Rhénanie-Palatinat
Valenciaplatz 1-7
55118 Mainz

Office de Police criminelle de Hambourg
Bruno-Georges-Platz 1
22297 Hamburg

Office de Police criminelle de la Sarre
Hellwigstraße 14
66121 Saarbrücken

Annexe 3

Extrait de :

Für den Notfall vorgesorgt
(« Se prémunir contre la situation d'urgence »

Une information de

l'Office fédéral pour la protection des populations et la gestion des catastrophes

Version : Août 2004

Brochure complète sous
http://www.bbk.bund.de *(Thèmes et conseils destinés à la population)*

Commentaire :
La brochure « Se prémunir contre le cas d'urgence » s'adresse notamment à la population et à chaque citoyen. Les informations relatives aux dangers liés aux événements naturels et aux accidents techniques, présentées dans la brochure et les indications afférentes aux mesures de prévention peuvent être exploitées sous une forme modifiée également pour les plans de prévention de l'entreprise.

Introduction

Des informations sur des accidents et catastrophes nous parviennent quotidiennement. Tous peuvent être touchés par de graves incendies, les crues, les accidents chimiques, une panne de courant (panne d'énergie) ou par d'autres dangers soudains.

Pour limiter les dangers dans une large mesure, un système d'opération de secours assiste le citoyen. Tandis que les sapeurs-pompiers et le service de sauvetage se tiennent prêts pour les opérations de secours quotidiennes, les pays entretiennent la protection civile afin d'être capables de parer aux catastrophes et aux risques de notre environnement technicisé. L'Etat fédéral allemand renforce et complète le système intégré d'opérations de secours des situations dangereuses à grande échelle et des crises en y ajoutant des véhicules, en mettant à disposition des aides exemptées du service militaire, des hélicoptères de sauvetage de la protection civile et en ayant recours au secours technique du THW. L'Etat fédéral, les Länder et les municipalités travaillent ainsi en partenariat en matière de protection de la population afin d'apporter aux citoyennes et citoyens l'assistance nécessaire en situation de détresse. Mais jusqu'à l'arrivée des secours, le temps continue de s'écouler – un temps précieux pendant lequel la vie des personnes ou le maintien des conditions matérielles peuvent se jouer. Quelques minutes durant lesquelles on ne peut peut-être compter que sur soi-même.

En présence d'une situation d'urgence, il est trop tard pour prendre de vastes mesures de prévention qui, face à cette situation, devraient encore faire leurs preuves. Nous ne pouvons plus apprendre la conduite à tenir en cas d'incendie ou d'accident, une fois un feu déclaré ou une personne blessée. Nous ne pouvons aider que dans le cas où nous nous sommes confrontés en amont à une situation dangereuse, en apprenant les gestes des premiers secours, en les répétant régulièrement et en nous confrontant aux mesures préventives de lutte contre les situations dangereuses ou les crises.

D'où l'importance de la prévention ! Le plus tôt sera le mieux, car aucun individu ne peut prévoir quand un danger pourra le concerner personnellement ! Créer un socle solide de connaissances face à d'éventuelles situations d'urgence demande très souvent peu d'investissement et de temps.

Risques d'intempéries

Les intempéries pouvant par définition survenir brutalement, un travail de préparation en amont peut s'avérer assez difficile à mettre en place. Suivez les bulletins météorologiques et leurs avertissements ! Cela permet de réduire les risques, de prévenir ou diminuer des sinistres. En cas d'intempéries, des branches disloquées, des arbres et des tuiles de toit peuvent toujours devenir un danger. En présence de fortes précipitations, les routes peuvent être également inondées. Les dégâts causés sur la chaussée ou sur les plaques d'égouts soulevées par la pression de l'eau peuvent devenir un danger pour les véhicules et les piétons. Contactez les pompiers lorsque des substances dangereuses telles que le mazout ont été répandues.

En cas d'intempéries vous devez en général avoir les choses suivantes à votre disposition :

- - une radio à ondes métriques très courtes autonome et des piles en nombre suffisant
- sources lumineuses autonomes telles que lampes de poche et bougies
- Valise d'urgence contenant les documents importants si vous devez quitter votre habitation.

Conseil :
Cette valise doit contenir une documentation de vos biens sous forme de photos ou tous autres documents. Si votre propriété devait être endommagée, ces papiers peuvent en effet s'avérer très utiles pour les compagnies assurances.

Les **orages** combinés à des décharges électriques entraînent la survenance de dangers supplémentaires. Respectez ce qui suit:

- Evitez les grands arbres, les mâts, les antennes et objets similaires. Faites en sorte de vous protéger dans un bâtiment.
- Restez dans le véhicule et ne touchez pas les parties métalliques à nu.
- Respectez une distance minimale de 50 mètres avec les lignes électriques haute-tension.
- Un éclair peut très bien générer des surtensions. Ne faites pas exclusivement confiance à l'installation paratonnerre de votre maison. Débranchez les appareils sensibles du réseau et utilisez la protection antisurtension correspondante.
- Un coup de foudre peut endommager considérablement la maçonnerie et causer des fissures ou cassures.

La **grêle** et les **cyclones** sont parfois les conséquences d'orages violents. Les grêlons ainsi que les débris et particules de saleté qui sont entraînés par le fort tourbillon d'un cyclone présentent des dangers supplémentaires. En cas de grêle et de cyclone, il convient de respecter ce qui suit :

- Fermez les volets roulants ou les volets simples, tenez-vous à distance des ouvertures non protégées.
- Rendez-vous dans une pièce en sous-sol, par exemple une cave ou un local intérieur ; un véhicule, une caravane et des bâtiments légers iront ne pourront probablement pas offrir suffisamment de protection.
- Evitez les locaux qui présentent une portée de plafond importante, comme les halls par exemple.
- Ne restez pas à l'extérieur! Rendez-vous plutôt dans un bâtiment solide ! Si nécessaire, allongez-vous, visage tourné vers le sol et protégez votre tête et votre nuque avec les mains !

Conduite à tenir suite aux intempéries

- Contrôlez l'absence de dommages dans votre environnement tels que l'envahissement d'eau ou les bris de verre etc.
- Mettez les appareils électriques en service uniquement lorsqu'ils ne sont pas entrés en contact avec l'humidité.
- Lorsque quelqu'un est blessé, apportez les premiers secours et déclenchez l'alarme.
- Si le bâtiment est endommagé, quittez-le et pénétrez-y de nouveau seulement lorsque les experts en ont autorisé l'accès.
- Lorsque le toit a été endommagé à la suite d'une tempête, tenez-vous à l'écart de la zone détériorée par la chute. Elle est d'un tiers de la hauteur du sol à la gouttière. Avertissez les pompiers.

Les crues

Ces dernières années, les inondations ont menacé de manière très significative les ressources critiques d'une partie des populations. Parallèlement aux efforts fournis par l'Allemagne, les Länder et les communes pour limiter les effets de tels faits dommageables, chacun doit vérifier aussi dans quelle mesure il peut éviter ou réduire les dommages par des activités de préparation et des mesures ciblées. Les remarques ci-après peuvent y contribuer. Vous devez au préalable éclaircir le repère de crue critique pour votre lieu de résidence par l une information demandée à votre commune.

N'oubliez pas que l'alimentation normale en courant, en denrées alimentaires et en eau potable peut être entravée ou interrompue en cas de crue. Cette situation peut durer encore un certain temps, même une fois la menace imminente de crue passée, en raison de l'endommagement de l'infrastructure.

Des risques particuliers en cas de crues résultent de la force de l'eau qui creuse et endommage les chemins, les ponts, les digues etc., mais aussi par les éléments flottants qu'elle peut entraîner. Les substances nocives qui s'écoulent telles que le mazout, les détergents et les produits phytosanitaires, tout comme les déchets d'origine humaine et les ordures entraînées dans les eaux, présentent un risque pour la santé. L'eau potable peut être contaminée.

Les mesures suivantes sont recommandées au titre de **mesures préparatoires** :

- Préparer des planches de blindage, des planches contreplaquées étanches et du silicone pour calfeutrer les pièces exposées au danger. Préparer également des sacs de sable.
- Transférer en temps utile les substances dangereuses et les produits chimiques.
- Sortir les meubles ou les appareils de valeur des pièces exposées.
- Utiliser des matériaux de construction résistants à l'eau et procéder aux colmatages dans les pièces exposées au danger.
- Sécuriser la citerne à mazout contre le flottement (ancrage arrière vertical / ballastage, par exemple en recouvrant de terre en cas de danger imminent). Utiliser si possible des citernes qui conviennent au cas de charge « pression d'eau de l'extérieur ». Préparer des possibilités de fermeture des conduites.

A prendre en considération pour la sécurité :

- Planifiez les soins des personnes handicapées ou malades. Organisez des possibilités d'« évacuation » chez des parents ou amis hors de la zone en danger.
- Dans une situation dangereuse, les téléphones fixe et mobile peuvent tomber en panne; par conséquent, convenez avec vos voisins et les pompiers de signaux de détresse et de danger.
- Informez chaque membre de la famille des précautions prises en prévision d'un danger, de la bonne conduite à tenir et des composants importants de la prévoyance personnelle. Discutez de la « répartition des rôles » en cas de sinistre (commande de l'interrupteur principal et des robinets d'arrêt, sauvegarde des documents etc.).

En cas de crue menaçante :

- Suivez les bulletins météorologiques actuels et les avertissements de crues via les radiodiffuseurs et les télétextes des programmes télévisés régionaux. Informez éventuellement en plus vos colocataires.
- Vérifiez et complétez les mesures de prévention prises.
- Evacuez les pièces exposées au danger.
- Assurez l'étanchéité des portes et fenêtres exposées, des orifices d'évacuation etc.
- Sécurisez les équipements de chauffage et les appareils électriques dans les pièces menacées ou débranchez-les. L'eau de condensation constitue déjà un risque de décharge électrique ! Ne pas oublier le congélateur!
- Vérifiez les installations domestiques de drainage des eaux et les clapets de retenue dans la cave.
- Sortez en temps utile les véhicules des garages menacés ou ôtez-les des places de stationnement en danger.
- Avertissez les pompiers en cas d'émission de matières nocives.

Remarque complémentaire relative aux véhicules automobiles :

- Ne roulez pas sur les routes inondées. De l'eau qui pénètre dans le compartiment moteur menace de causer un dommage considérable ; de surcroît, la température de service d'un catalyseur se situe à environ 700°C, dont le refroidissement subi peut entraîner l'éclatement de la tête en céramique.
- Lorsque le véhicule est immergé dans l'eau jusqu'à hauteur de la cuvette à huile ou des roues, ne pas le démarrez mais le faire remorquer et contrôler dans un garage.

Sauvez des vies :

- Le sauvetage de vies humaines prime sur la sauvegarde des biens matériels.
- Il n'y a pas de tentatives de sauvetage sans protection propre, appelez au secours !

- N’abordez pas les zones riveraines en raison du risque de destruction et d’éboulement ! Ceci s’applique également au fait d’emprunter des routes inondées ou partiellement inondées! Respectez les barrages et suivez les instructions de la commune et des équipes en intervention !
- Ne circulez pas sur les eaux de crue en empruntant un bateau personnel en raison de la formation de vagues et du danger lié aux obstacles sous l’eau.

Après la crue

- Evacuez l’eau stagnante et la boue, utilisez une pompe pour évacuer les eaux de crue des pièces concernées uniquement lorsque l’eau s’est évacuée et que le niveau de la nappe phréatique a suffisamment baissé. Prêtez une attention à l’information donnée par votre commune.
- Vous devez enlever ou ouvrir les couvertures de sol et les revêtements afin de les contrôler.
- Séchez le plus vite possible les zones touchées afin de lutter contre les dommages de construction, l’infestation de moisissure ou autre infestation. Les appareils de chauffage peuvent favoriser le séchage.
- Faites contrôler l’état du gros œuvre endommagé (statique).
- Remettez les appareils électriques et les installations en service uniquement après les avoir faits contrôler par un électricien.
- Faites vérifier que les citernes à mazout n’ont pas été endommagées.
- Avertissez les pompiers en cas de rejet de substances nocives telles que produits phytosanitaires, peintures, vernis, détergents ou mazout. Leur élimination doit être effectuée le cas échéant par des sociétés spécialisées.
- En cas de rejet d’huiles, utilisez des produits liants uniquement en accord avec les pompiers.
- Il convient de toujours bien aérer les pièces dans lesquelles vous travaillez. Ne pas fumer et éviter tout feu nu en présence de substances nocives dégagées.
- Eliminez les meubles et les denrées alimentaires contaminés.

- Avertissez l'administration compétente sur votre secteur ou l'Office de l'agriculture lorsque les jardins ou les champs sont couverts d'épaisses couches de boue ou d'huile.

Vous obtiendrez les informations, indications et éventuellement les adresses des entreprises spécialisées par le biais des autorités compétentes de votre commune et des pompiers.

Conseil :
Vous obtiendrez les informations concernant la conduite à tenir en cas de crue et en présence d'autres dangers via le système allemand d'information de prévention des risques deNIS : **www.denis.bund.de**.

Panne d'énergie

Tous les citoyens des nations industrielles sont tributaires aujourd'hui des différentes sources d'énergie. Elles comprennent l'électricité, le gaz, l'huile et la chaleur à distance qui sont fournis à domicile par des réseaux de distribution. Les conséquences d'une panne d'électricité montrent combien nous sommes tributaires de ce réseau d'alimentation. Tous les appareils fonctionnant sur secteur tombent en panne. En font partie ici :

- le chauffe-eau
- la radio
- la lumière
- le distributeur automatique de billets
- le téléphone
- l'ordinateur
- les mécanismes de portes dépendant du courant et autres mécanismes

- et bien d'autres choses.

Même les systèmes de chauffage sont tributaires de multiples façons de l'électricité. Il en va de même pour le chauffage au mazout étant donné que son transport via les tuyauteries ascendantes, l'injection et l'allumage fonctionnent à l'électricité. Ces fonctionnements peuvent être commandés manuellement, et encore uniquement en engageant des transformations importantes et coûteuses.

Conseils concernant les stocks en matières énergétiques :

En cas de panne d'alimentation en mazout, chaleur à distance ou de panne d'électricité, tous les ménages doivent disposer d'alternatives pour parer à cette urgence. L'absence de chauffage peut être remplacée en général, dans nos régions, par des vêtements chauds pendant un certain temps. Celui qui a une possibilité de chauffer, en utilisant du charbon, des briquettes ou du bois, doit s'approvisionner en combustibles pour le cas d'urgence.

En cas de panne de lumière, on peut recourir aux bougies, aux lampes de poche ou à pétrole. Dans ce cas, il faut contrôler aussi les réserves de bougies, combustibles, d'ampoules de rechange, des piles et moyens d'allumage tels que les allumettes ou briquets. Les piles rechargeables conviennent moins à une réserve de secours, car elles ne conservent pas le courant stocké suffisamment longtemps lorsqu'elles sont rechargées. En cas de panne d'électricité, ceux-ci devraient être complètement rechargés. Dans des conditions très défavorables, n'oubliez pas qu'une panne d'énergie peut très bien durer plusieurs semaines.

Autoprotection au domicile

Même s'il n'existe pas de protection absolue contre tous les sinistres, il est possible toutefois de prévenir la majorité des risques ou d'en réduire les conséquences néfastes en agissant

efficacement. Aussi est-il particulièrement important de s'informer très tôt sur les dangers éventuellement menaçants son lieu de résidence et les mesures de prévention qui y sont prises.

Dans une habitation également, des mesures préventives de protection-incendie, par exemple l'utilisation de matériaux de construction difficilement inflammables, de portes anti-feu dans les chaufferies, l'application de détecteurs de fumée et d'appareils prêts pour lutter contre le feu, permettent de réduire les dangers pour les personnes et les biens matériels.

Possibilités de protection contre l'incendie

Les incendies à eux seuls sont la cause de la mort d'environ 600 personnes par an en Allemagne et de plus de 5000 blessés ! Rien que dans les maisons des particuliers, les biens matériels qui prennent feu chaque année s'élève à un montant supérieur à 10 milliards d'euros. Les catastrophes peuvent déboucher sur des incendies de grande ampleur. La protection contre les incendies fait par voie de conséquence partie des mesures de prévention indispensables. Si un incendie se déclare hors contexte de précaution voire si de nombreux foyers d'incendie se créent à la suite d'une catastrophe, les pompiers ne peuvent intervenir partout au même moment. Il est donc vital que les personnes concernées agissent rapidement et correctement afin d'éteindre les incendies, si possible dès leur naissance. A cet effet, vous aurez besoin de quelques appareils simples tels qu'extincteur ou tuyau de jardin qui doivent être conservés dans un endroit bien accessible.

Avant l'incendie:

Peu importe si vous séjournez dans votre habitation ou dans un autre bâtiment, vous devez vous informer sur ce qui suit avant que l'incendie ne se déclare :

- comment accéder à la cage d'escalier la plus proche en cas de danger, (ces cages d'escalier sont des issues et itinéraires de secours menant à l'extérieur, les ascenseurs ne doivent surtout pas être employés en cas d'incendie !),
- quelles mesures préparatoires ont été prises pour l'évacuation des personnes handicapées,

- quelles possibilités existe-t-il pour effectuer l'appel d'urgence,
- où se trouvent les extincteurs et comment les utiliser.

Veillez

- à ce que les couloirs et cages d'escalier ne soient pas encombrés, voire bloqués par des objets, il faut pouvoir utiliser l'issue de secours sans restriction,
- à ce que les portes sur les itinéraires de secours soient fermées, mais jamais verrouillées, afin d'empêcher l'extension du feu ou la propagation de la fumée dans l'issue de secours,
- à ce que les bouches d'incendie ou l'accès des pompiers ne soient pas bloqués,
- à ce que les équipements de sécurité de la maison ne soient pas endommagés et si tel est le cas, à le déclarer immédiatement .
- à ce que la lumière nue telle que bougies ou feu soit toujours utilisée sous surveillance,
- à ce que les installations et équipements électriques soient en parfait état et ne soient pas manipulés,
- à ce que les documents et les papiers les plus importants soient à portée de main à la maison en cas d'évacuation inattendue.

Conseils de prévention contre l'incendie :

- Dans la cave : Retirer le matériel superflu légèrement inflammable !
- Dans le grenier : Vider le grenier, dégager notamment le matériel inflammable logé dans tous les coins ou sous les pentes des combles !
- Préparer des matériels d'extinction pour l'urgence, par exemple extincteur, tuyau d'eau, couverture anti-feu etc.!
- Effectuer régulièrement l'entretien des extincteurs et les faire contrôler !
- Apprendre à se servir des appareils d'extinction et à employer correctement les matériels d'extinction disponibles !

- Ne jamais laisser un feu nu ou sources de danger similaires sans surveillance !

Pendant l'incendie :

Pour faciliter son propre sauvetage ou celui d'autres personnes dans un incendie, vous devez avoir des connaissances sur la bonne conduite à tenir en matière d'autoprotection. La sécurité des personnes a la priorité absolue. Si vous découvrez un incendie, vous devez respecter l'ordre suivant:

Si l'incendie est en train de se déclarer, entreprenez immédiatement les premières tentatives d'extinction pour le tuer déjà « dans l'œuf ».

- Tenter d'éteindre le feu uniquement s'il est possible de le faire en tout sécurité!
- N'éteindre en aucun cas avec de l'eau la graisse brûlante ou autres combustibles liquides !
- En présence d'un risque lié au courant électrique, couper celui-ci avant de commencer l'opération d'extinction dans la zone dangereuse.
- Eteindre un incendie de bas en haut et du côté vers le centre !
- Ne jamais pénétrer dans des pièces enfumées où se forment des gaz mortels. Fermez-en la porte et donner l'alarme auprès des pompiers.

Lorsqu'il n'est pas possible d'éteindre l'incendie : Fermer les fenêtres de la pièce si cela s'avère possible sans mettre sa vie en danger, fermer de même la porte de la pièce qui est en flammes. Cela peut asphyxier le feu.

Appeler les pompiers!

Avertir les personnes et les mettre en sécurité (éventuellement par d'autres)

Attendre les pompiers et leur rendre compte ou déléguer quelqu'un d'autre pour les informer.

Jusqu'à l'arrivée des sapeurs-pompiers, vous devez essayer d'endiguer l'extension du feu. Humidifier la porte qui mène à la pièce en flammes afin de repousser ou d'empêcher le feu de la traverser.

Si vous devez quitter le bâtiment ou l'appartement, l'étage etc., veillez à ce que personne ne demeure dans le bâtiment. Les portes des pièces qui ne sont pas en flammes ne doivent pas être verrouillées pour favoriser éventuellement des recherches rapides, les portes anti-feu et les portes de secteur coupe-feu sont naturellement fermées. Ne pas fermer les portes à clé! Préparer les clés des pièces ou fenêtres qui sont accessibles uniquement à l'aide de clés pour les équipes d'intervention.

Hors de la zone dangereuse, vérifiez si tous les habitants sont en sécurité, car si une personne était portée disparue, les pompiers doivent toujours partir du principe qu'elle se trouve éventuellement encore dans le bâtiment et est donc en danger.

Vous devez réagir également lors d'une simulation d'alarme (par exemple sur votre lieu de travail) comme pour un incendie réel. Si vous prenez un jour une alarme incendie "réelle" pour une simulation et ne réagissez pas, cela peut vous mettre vous-même et les forces d'intervention en danger.

Les pompiers vous fourniront des informations complémentaires.

Matières dangereuses – Principes de protection

Les matières dangereuses peuvent être dégagées dans l'industrie, lors du transport de produits dangereux, voire partiellement dans les foyers des ménages. Ces scénarios vont de l'utilisation trop négligente des détergents ou d'un accident à

une situation de crise dans laquelle nous sommes peut-être menacés par des substances insalubres. Les matières radioactives et toxiques apparaissent sous forme de gaz, vapeur et particules de poussières. Lors de leur rejet, ces matières, selon le type et la quantité, peuvent devenir un danger pour les personnes.

Le citoyen ne peut en général pas reconnaître s'il a affaire à une situation dangereuse qui exige l'application de mesures particulières de protection. Prêtez attention aux communiqués et recommandations des autorités publiques qui sont diffusés par radio et installations de haut-parleurs. Quelques règles de conduite simples renforce la protection dans certaines situations dangereuses et peuvent contribuer à réduire considérablement le danger.

Conduite autoprotectrice en cas de risque de contamination radioactive :

1. A l'extérieur :

- Rendez-vous dans la maison habitée la plus proche.
- Tentez de vous déplacer perpendiculairement au sens du vent, respirez si possible à travers un masque de protection, ou au moins à travers un mouchoir.
- Si vous êtes entré en contact avec des substances radioactives, changez vos vêtements de dessus et vos chaussures en pénétrant dans la maison.
- Laissez les vêtements de dessus et les chaussures pollués hors de l'habitation.
- Lavez-vous abondamment le visage, les cheveux et les mains, ainsi que le nez et les oreilles.
- Suivez les instructions qui s'appliquent dans les bâtiments.

2. En voiture :

- Arrêtez l'aération et fermez les fenêtres.
- Ecoutez la radio (stations régionales) et suivez les instructions des autorités et des équipes d'intervention.
- Rendez-vous autrement dans le bâtiment habité le plus proche et respectez-y les indications du paragraphe 1.

3. A l'intérieur du bâtiment :

- Restez dans le bâtiment.
- Accueillez-y provisoirement les personnes s'y présentant en danger.
- Informez, si nécessaire, les autres habitants.
- Fermez portes et fenêtres.
- Arrêtez les ventilateurs et l'installation de climatisation, fermez la fente d'aération des châssis de fenêtre.
- Rendez-vous dans une pièce de la cave ou une pièce intérieure protégée de l'habitation, de préférence sans fenêtres donnant sur l'extérieur
- Evitez de consommer inutilement de l'oxygène par des bougies ou objet similaire.
- Pour votre information, réglez la radio sur une station-radio régionale ou allumez le poste de télévision.
- Prêtez attention aux messages des autorités et des forces d'intervention.
- Téléphonez uniquement dans des cas d'urgence.
- En cas de pénétration de particules radioactives, utilisez les équipements respiratoires disponibles, si nécessaire un masque protecteur, par exemple un masque de chirurgie ou en tissu.

Conduite autoprotectrice en cas de risques biologiques ou chimiques:

1. A l'extérieur :

- Rendez-vous dans la maison habitée la plus proche.
- Tentez de vous déplacer perpendiculairement au sens du vent, respirez si possible à travers un masque respiratoire, ou au moins à travers un mouchoir.
- Si vous êtes entré en contact avec des substances dangereuses, changez vos vêtements de dessus et vos chaussures en pénétrant dans la maison.
- Laissez les vêtements de dessus et les chaussures pollués hors de l'habitation.

- Lavez-vous abondamment le visage, les cheveux et les mains, ainsi que le nez et les oreilles.
- Suivez les instructions qui s'appliquent dans les bâtiments.

2. En voiture :

- Arrêtez l'aération et fermez les fenêtres.
- Ecoutez la radio (stations régionales) et suivez les instructions des autorités et des équipes d'intervention.
- Rendez-vous autrement dans le bâtiment habité le plus proche et respectez-y les indications données dans le paragraphe 1.

3. A l'intérieur du bâtiment :

- Restez dans le bâtiment.
- Accueillez-y provisoirement les personnes s'y présentant .
- Informez, si nécessaire, les autres habitants.
- Fermez portes et fenêtres.
- Arrêtez les ventilateurs et l'installation de climatisation, fermez la fente d'aération des châssis de fenêtre.
- Rendez-vous dans une pièce intérieure bien protégée de l'habitation, de préférence sans fenêtres extérieures.
- Evitez les caves ou autres pièces de faible élévation.
- Evitez de consommer inutilement de l'oxygène par des bougies ou objet similaire.
- Pour votre information, réglez la radio sur une radio régionale ou allumez le poste de télévision.
- Prêtez attention aux messages des autorités et équipes d'intervention.
- Téléphonez uniquement dans des cas d'urgence.
- En cas de pénétration de substances chimiques toxiques, utilisez les équipements respiratoires disponibles, si nécessaire un masque protecteur, par exemple un masque de chirurgie ou en tissu.

Chacun doit être en mesure d'aider autrui et lui-même jusqu'à l'arrivée des secours organisés. Les premiers secours sont une composante importante de l'autoprotection. Les organismes d'aide vous fourniront volontiers les renseignements concernant le lieu et l'heure des cours d'instruction.

Protection des populations et contre les catastrophes

Avec le BBK (l'Office fédéral pour la protection de la population et l'aide à la catastrophe), l'Etat fournit une contribution importante à la protection de la population qui rattache et fait s'accorder les potentiels de l'Etat et des communes en un système d'aide intégré. Des hélicoptères de la protection civile dans le sauvetage aérien, des véhicules de reconnaissance ABC, l'oeuvre de Secours Technique mais aussi les prestations de service du BBK font par exemple partie du potentiel de prestation de l'Etat.

Les communes sont responsables de leur propre protection. Elles sont assistées par le BBK dans la prise en charge de cette tâche. La capacité à la propre assistance de chacun est, dans ce sens, la base incontournable de l'aide organisée. Si vous avez des questions sur la protection des populations ou sur la propre protection, adressez-vous à l'

Office fédéral pour la protection civile (BBK),
Téléphone : (01888) 550-0,Téléfax : (0228) 5554-436
http://www.bbk.bund.de
info@bbk.bund.de

Pour le soutien des services de sauvetage et des pompiers en cas de sinistres particuliers ou majeurs tels que des accidents graves, des catastrophes techniques et naturelles qui exigent une coopération des forces d'intervention au-delà du niveau local, les Länder subviennent aux besoins de la protection contre les catastrophes. Les organisations qui s'y associent sont, à cet effet, entre autres :

- L'Union des salariés et des samaritains en Allemagne

- die Deutsche Lebens-Rettungs-Gesellschaft (la société allemande de sauvetage de la vie)
- la Croix-Rouge Allemande
- les sapeurs-pompiers
- die Johanniter-Unfall-Hilfe (les volontaires de St Jean)
- der Malteser-Hilfsdienst (le service d'aide maltais)
- l'Agence fédérale de Secours Technique (THW).

Dans une situation urgente comme dans le cas, par exemple, d'un accident, des personnes peuvent être blessées et être tributaires ainsi de l'aide d'une personne étrangère. Dans les cas les plus rares, le service de sauvetage ou les pompiers sont immédiatement sur place. Ils doivent être d'abord alertés grâce à l'appel d'urgence. La base de toute aide organisée est donc un système d'appel d'urgence et d'alerte connu qui fonctionne correctement. Partout en Allemagne vous pouvez joindre gratuitement la police, les pompiers ou le service de sauvetage grâce aux numéros de téléphone suivants :

Pompiers : 112 Police : 110

Veuillez vous informer, malgré tout, sur les numéros d'appel d'urgence locaux complémentaires. Au demeurant : avec votre téléphone portable, vous pouvez appeler à tout moment et même sans carte le numéro d'urgence 112!

Le temps qui s'écoule jusqu'au moment où le service de sauvetage ou les pompiers arrivent doit être limité au maximum grâce à la mise en place de premiers gestes d'assistance. Vous pouvez lire, avec ce qui suit, dans quel ordre vous devez les appliquer :

1. Protégez, si nécessaire, l'emplacement du dommage.

2. Exécutez les mesures immédiates pour sauver la vie.

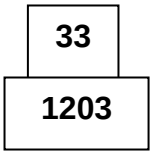
3. Appelez de l'aide au 112 ou l'un des autres numéros d'urgence.

4. Pour procéder à la déclaration, il faut répondre aux questions suivantes :

- Où cela s'est-il passé ?
- Que s'est-il passé ?
- Combien de personnes sont blessées ?
- De quel type sont les blessures ?
- Attendez les demandes de précisions des équipes de secours !

5. Procédez aux premiers secours jusqu'à ce que le service de sauvetage intervienne.

S'il s'agit d'un accident avec un transporteur de produits dangereux, veuillez alors indiquer les chiffres supérieurs sur la plaque signalisant la nature des produits à l'arrière du véhicule.



Numéros de téléphone importants

Police 110

Pompiers 112

Service de sauvetage

Service médical d'urgence

Urgence antipoison et intoxications

Service de garde de la pharmacie

Services communaux

Urgence	**Feu**
Où s'est-il passé quelque chose?	Où cela brûle-t-il?
Que s'est-il passé?	Qu’est-ce qui brûle?
Combien de blessés?	Quelle est l’ampleur du feu?
De quel type ?	Quels dangers ? (personnes en danger, bouteilles de gaz stockées ou similaire ?)
ATTENDRE les demandes de précisions !	ATTENDRE les demandes de précisions !

.

Annexe 4

Glossaire du concept de protection de base

Analyse des dangers	Méthode destinée à identifier et évaluer les répercussions d'éventuels événements sur les infrastructures, les objets ou la population pour pouvoir en déduire des conclusions pour la protection.
Analyse des menaces	Méthode destinée à identifier et évaluer les domaines, infrastructures et objets susceptibles d'être menacés par d'éventuels événements.
Analyse du risque	Saisie du potentiel de danger et de la vulnérabilité de la région/l'objet considéré(e) face aux impacts et détermination des conséquences qui en résultent (détermination des risques).
AOS	Autorités et organismes chargés de la sécurité (autorités de police et de protection civile fédérales et régionales, administration fédérale des douanes, pompiers, THW (agence fédérale de secours technique), organismes d'aide).
Autorités chargées du maintien de la sécurité	Les autorités compétentes pour la limitation des dangers (polices et autorités chargées de l'ordre public).
Catastrophe	Evénement dommageable (grave) d'origine naturelle (tremblement de terre, inondations, éruption volcanique etc.) ou lié à des activités humaines (accident chimique, accident d'avion, attentat etc.) susceptible de créer un danger pour la vie ou la santé d'un grand nombre de personnes, pour l'environnement ou autres biens protégés importants et que les autorités compétentes dans le domaine ne peuvent maîtriser adéquatement avec ses propres forces et moyens.
Catégories de risques	Systématisation des risques individuels à l'aide des événements qui les déclenchent.

Cible	Description d'un résultat théorique auquel il faut aboutir. Les objectifs de protection découlent des résultats de l'analyse des menaces et de l'évaluation des risques.
Communication de crise	Toutes les activités communicatives qui sont menées dans le contexte d'une crise. En pratique, la communication de crise signifie l'attribution claire des compétences et responsabilités et une ligne de communication claire pour assurer un contenu et une argumentation homogènes. Dans ce contexte, il est nécessaire de conclure un accord définissant comment intégrer les médias au moment d'assumer la crise.
Crise	Une situation subite ou insidieuse, divergeant de l'état normal et caractérisée par un potentiel de risque qui recèle des dangers et préjudices pour la vie et l'intégrité corporelle des personnes, les biens matériels majeurs, des menaces du système politique, social et économique et qui requiert une décision, prise souvent dans des conditions d'incertitude et sur la base d'informations incomplètes.
Criticité	Evaluation de l'ampleur et de la probabilité de la défaillance d'un secteur / processus d'infrastructures critiques.
Danger	Incidences (concrètes) des dangers ou menaces (événements naturels, défaillance technique ou humaine, erreur humaine) sur les infrastructures critiques.
Dangers NRBC/CBRN	Dangers de nature nucléaire, biologique, chimique ou radioactive (chemical, biological radiological or nuclear).
DIN 18106	Exigences relatives aux grilles anti-effraction et procédure de contrôle de celles-ci.
DIN 4102	Comportement au feu des matériaux, composants et éléments spéciaux de construction.
DIN 77200	Exigences fondamentales relatives à l'organisation, à la gestion du personnel et au mode de travail des prestataires en matière de sécurité.
DIN ENV 1627	Exigences relatives aux portes et fenêtres anti-effraction et classification de celles-ci.
DIN ENV 356	Vitrage spécial de sécurité/procédure de contrôle et classification de la résistance à l'attaque manuelle.
DIN/VDE 0185	Paratonnerre/protection des installations de construction et des personnes.

dirty bomb	Explosif traditionnel déclenchant une explosion par laquelle se propagent des substances radioactives (« bombe sale »).
Dommage	Destruction et diminution des valeurs concrètes et abstraites. Il comprend l'atteinte à la santé, la perte des chances de vie et les altérations de la qualité de vie ainsi que la perte des biens monétaires. Cette catégorie inclut également les préjudices idéaux tels que la perte de confiance dans l'intégrité des décideurs politiques.
Dommages éléments naturels	Dommages causés par des événements naturels tels que le feu, la chaleur, la foudre, les crues, les inondations, le gel, les avalanches, la chute de pierres, le tremblement de terre.
Effet domino	Séquence d'événements dont chacun est en même temps la cause de l'événement suivant ; tous les événements sont à imputer à un seul et même événement initial.
Evaluation/appréciation des risques	Méthode de jugement rationnel d'un risque prenant en considération son acceptabilité pour la société dans son ensemble ou pour certains groupes ou individus. L'analyse scientifique des risques et la perception du risque que des études empiriques ont recensée font partie intégrante de l'évaluation du risque.
Gestion de la crise	Création de conditions conceptuelles, organisationnelles et méthodiques qui favorisent le processus de restauration de l'état normal après la survenance d'une situation exceptionnelle.
Gestion de la qualité	Toutes les mesures d'une entreprise qui permettent de créer, d'assurer et d'améliorer la qualité. L'étendue et les contenus de la gestion de la qualité sont fréquemment consignés dans un manuel de la gestion de la qualité qui doit se conformer aux normes ISO 9000. Un système de gestion de la qualité correspondant permet de mettre en application la gestion de la qualité dans l'entreprise.
Gestion du risque	Ensemble des mesures visant à minimiser la situation de risque par l'examen de solutions alternatives stratégiques (options d'action) en consultation avec les parties concernées et en tenant compte de l'évaluation des risques et autres facteurs méritant d'être pris en considération.

Infrastructures critiques	Organisations et équipements revêtant une importante signification pour la communauté dont la défaillance et la perturbation créeraient des goulots d'étranglement durables dans l'approvisionnement, des dysfonctionnements importants de la sécurité publique ou d'autres conséquences dramatiques.[6]
Interdépendances	Interactions ou influence mutuelle des différentes infrastructures critiques.
Limitation des dangers	Mesures permettant de maintenir ou rétablir la sécurité civile.
Mise en danger	Possibilité d'un événement (événements naturels, défaillance technique ou humaine, erreur humaine) susceptible de porter préjudice aux personnes, aux biens matériels et à l'environnement ou de causer des perturbations sociales et économiques.
Norme ISO 17799	Norme internationale relative à la sécurité de l'information; directives pour la mise en place et la gestion d'un système de gestion de la sécurité de l'information (SGSI).
Ordonnance sur les accidents majeurs Störfallverordnung	Ordonnance sur les accidents majeurs, mise en application de la directive dite « Seveso II » dans le droit allemand ; comprend les obligatoires pour les exploitants des zones opérationnelles au sens de l'article 3, alinéa 3 de la loi fédérale sur la protection contre les nuisances qui définit les mesures de prévention des accidents et la conduite à tenir à la suite d'accidents.
Perception des risques	Appréciation des risques qui repose, pour une large part, sur les expériences personnelles, les informations transmises et les estimations intuitives.
Plan de Continuité des Activités (PCA)	Le PCA concerne toutes les mesures organisationnelles, techniques et personnelles qui permettent de poursuivre l'activité centrale d'une entreprise dès la survenance d'une crise et de continuer l'exploitation de l'entreprise en cas de défaillances ou de dysfonctionnements de longue durée.
Plan de secours	Précaution visant à maintenir et rétablir les processus de l'entreprise en cas d'événements ou de défaillances imprévisibles.
Planification des mesures d'urgence	Toutes les préparations concrètes à prendre pour la situation de crise/de catastrophe afin de garantir sa maîtrise effective.

[6] Définition d'infrastructures critiques du groupe de travail K KRITIS du Ministère de l'Intérieur (BMI) du 17.11.2003.

Redondance

La présence multiple de ressources identiques dans le but d'accroître la sécurité après la défaillance d'un système.

Risque

Attente d'un danger sérieux qui

- menace la vie des personnes,
- porte préjudice à la santé d'un grand nombre de personnes,
- affecte les activités économiques, services publics et infrastructures techniques, qui est susceptible d'endommager l'environnement, notamment les animaux et les plantes, le sol, l'eau, l'atmosphère ainsi que les biens culturels et matériels.

La probabilité des risques est hiérarchisée et qualifiée de « très grande », « grande », « moyenne », « basse », « minime » et « très minime ». Elle dépend de la vulnérabilité de la région considérée face aux impacts délétères, par exemple naturels, physiques, techniques, économiques, et de la probabilité de la survenance d'une situation exceptionnelle.

En termes mathématiques, le risque *R* est le produit du montant du dommage *D* et de la probabilité de survenance *P*:
$R = D \times P$

Annexe 5

Autres références

Les indications suivantes relatives à la bibliographie, aux manuels et guides ainsi que les adresses Internet sont conçues comme aide initiale et représentent seulement une sélection de l'offre en matière d'information imprimée et électronique devenue depuis très vaste.

Nous intégrons volontiers toute recommandation bibliographique supplémentaire et autres remarques pour actualiser et compléter notamment la version d'Internet ; prière de faire parvenir ces informations à BBK-Zentrum-I@bbk.bund.de

1. Bibliographie

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch (Stand: November 2004)
http://www.bsi.bund.de/gshb/deutsch/index.htm

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (Hrsg.), Vollzugshilfe zur Störfall-Verordnung, März 2004
http://www.umweltministerium.de/files/broschueren/faltblaetter/application/pdf/vollzugshilfe_stoerfall_vo.pdf

Bundesministerium für Wirtschaft und Arbeit, Geheimschutzhandbuch – Handbuch für den Geheimschutz in der Wirtschaft, 2005
https://www.bmwa-sicherheitsforum.de/geheimschutz/ghb.php

Bundesministerium für Wirtschaft und Arbeit, Leitfaden zum vorbeugenden personellen Sabotageschutz im nichtöffentlichen Bereich, Stand: 14.01.2005
https://www.bmwa-sicherheitsforum.de/shb/ghb/archiv/leitfaden_14.01.05.pdf

Bundesverband deutscher Banken, Management von Kritischen Infrastrukturen, 2004
http://www.bankenverband.de/pic/artikelpic/052004/br0405_rb_infrastruktur.pdf

Casavant, David, Emergency Preparedness for facilities. A Guide to Safety Planning and Business Continuity, Maryland, USA 2003

Deloitte, Erfolg in der Secure Economy – Wachstum und Wohlstand in einer sicheren Wirtschaft. Executive Summary, 2004
http://www.deloitte.com/dtt/cda/doc/content/de_public_Secure_Economy_1204.pdf

Ehses, Herbert u.a. (Hrsg.), Unternehmensschutz. Praxishandbuch Werksicherheit, Loseblattausgabe, Stuttgart, Stand: Mai 2004

Störfallkommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Leitfaden – Maßnahmen gegen Eingriffe Unbefugter der ad hoc- Arbeitsgruppe „Eingriffe Unbefugter“, (SFK-GS-38), 23.10.2002
http://www.sfk-taa.de/berichte_reports/berichte_sfk/sfk_gs_38.pdf

Störfallkommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Leitfaden für die Darlegung eines Konzepts zur Verhinderung von Störfällen gem. § 8 in Verbindung mit Anhang III der Störfall-Verordnung 2000 für Betriebsbereiche, die den Grundpflichten der Störfall-

Verordnung 2000 unterliegen, bearbeitet vom Arbeitskreis MANAGEMENTSYSTEME der SFK (SFK-GS-23, Revision 1), 22.05.2002
http://www.sfk-taa.de/berichte_reports/berichte_sfk/sfk_gs_23_rev1.pdf

(Les remarques de la Commission allemande des accidents s'appliquent également de façon analogue aux entreprises qui ne sont pas soumises à l'ordonnance sur les accidents majeurs).

2. Adresses Internet

a) Autorités :

Bundesministerium des Innern: http://www.bmi.bund.de

Bundesministerium für Wirtschaft und Technologie: http://www.bmwi.bund.de

Bundesministerium für Verkehr, Bau und Stadtentwicklung: http://www.bmvbs.bund.de

Bundesministerium für Gesundheit: http://www.bmg.bund.de

Bundesministerium der Finanzen: http://www.bundesfinanzministerium.de

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): http://www.bbk.bund.de

Bundeskriminalamt (BKA): http://www.bka.de

Bundesamt für Sicherheit in der Informationstechnik (BSI): http://www.bsi.bund.de

Bundesanstalt Technisches Hilfswerk (THW): http://www.thw.bund.de

Deutscher Wetterdienst (DWD): http://www.dwd.de

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: http://bundesnetzagentur.de
(vormals Regulierungsbehörde für Telekommunikation und Post (RegTP))

b) Divers :

Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.:
http://www.asw-online.de

Deutsches Notfallvorsorge-Informationssystem – deNIS:
http://www.denis.bund.de

Kompetenzzentrum GeoRisikoForschung der Münchner Rückversicherungs-Gesellschaft:
http://www.munichre.org (*Topics und Solutions*)

Sicherheitsforum: https://www.bmwa-sicherheitsforum.de/

TSM – System zur Überprüfung der Organisations- und technischen Sicherheit: http://www.dvgw.de

Verband der Elektrizitätswirtschaft (VDEW):
http://www.strom.de

Verband der Netzbetreiber: http://www.vdn-berlin.de

Allgemeine Informationen zur Ernährungsvorsorge:
www.ernaehrungsvorsorge.de

Impression	Impressum

Edité par le	Herausgeber:
Ministère de l'Intérieur de la République Fédérale d'Allemagne Section P II 1	Bundesministerium des Innern Referat P II 1

Alt Moabit 101 D
10559 Berlin

poststelle@bmi.bund.de
http://www.bmi.bund.de

Rédaction:	Redaktion:
Office fédéral pour la protection des populations et la gestion des catastrophes Centre de protection des infrastructures critiques	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Zentrum Schutz Kritischer Infrastrukturen

Deutschherrenstraße 93-95
53177 Bonn

BBK-Zentrum-I@bbk.bund.de
http://www.bbk.bund.de

Office fédéral de police criminelle Section KI 21	Bundeskriminalamt Referat KI 21

65173 Wiesbaden

info@bka.bund.de
http://www.bka.de

Première Edition Janvier 2006	1. Auflage (Januar 2006)